UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

"TEOREMA DE RIEMANN - ROCH"

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

ABRAHAM MARTIN DEL CAMPO SANCHEZ

FACULTAD DE CIENCIAS
UNAM

DIRECTOR DE TESIS: DR. ENRIQUE JAVIER ELIZONDO HUERTA

2005

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

"Teorema de Riemann - Roch"

realizado por Abraham Martín del Campo Sánchez

con número de cuenta 09954262-3 , quien cubrió los créditos de la carrera de:

Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Enrique Javier Elizondo Huerta	
Propietario	Dr. Francisco Portillo Bobadilla	
Propietario	Dra. Adriana Ortiz Rodríguez	
Suplente	Lic. Eduardo Ocampo Alvarez	
Suplente	M. en C. Jesús Rogelio Pérez Buendía	

Consejo Departamental de Matemáticas

M. en C. Alejandro Bravo Mojica

Teorema de Riemann-Roch

Abraham Martín del Campo Sánchez

Febrero de 2004

A Mabel

"El álgebra es sólo geometría escrita,
la geometría sólo álgebra hecha figuras."
—Sophie Germain.

"Mejor que de nuestro juicio, debemos fiarnos del cálculo algebraico."
—Leonhard Euler.

Agradecimientos

Quiero agradecer enormemente a la U.N.A.M y al Instituto de Matemáticas por haber sido una segunda casa y brindarme el privilegio de estudiar en esta universidad.

A mi esposa, Mabel, por su infinito apoyo, las palabras siempre me serán insuficientes para agradecerlo. Por su inmenso amor y por compartir la promesa de seguir siempre juntos. Por darle magia a mi vida y compartirme, además de su vida, su exuberante sensibilidad por lo humano. Por ser siempre una fuente de inspiración y motivación para dar todo de mí y alcanzar todos mis sueños. Te amo con todo mi ser, y más.

A mi madre, por su amor, por su ejemplo de constancia y esfuerzo para salir siempre adelante, por su nobleza, su sencillez y su eterna disposición por ayudar a los demás.

A mi padre, al que tanto admiro, a quien debo mi espíritu científico, por sus infinitas enseñanzas que son siempre estimulantes, pues su pasión por aprender, y el gusto de saber, forman un ejemplo de la sed de conocimiento siempre insaciable que dejó en mí.

A Javier por aceptar dirigir esta tesis, por compartir su gusto por la geometría algebraica e inspirarmelo, también por su paciencia para corregir mis errores y escuchar mis necedades.

A mis sinodales: Francisco Portillo, Adriana Ortiz, Rogelio Pérez Buendía, y Eduardo Ocampo por su apoyo y sus valiosas correcciones.

A mis profesores: Herbert Kanarek, Javier Bracho, Luis Montejano, Alejandro Díaz Barriga, José Antonio Gómez. Les agradezco toda mi formación, su pasión y sus ganas. A Ana Irene Ramírez, por las conversaciones que tanto me orientaron y ayudaron, también por su gusto por la geometría, porque me enseñó a escribir formalmente matemáticas, y me dio las herramientas para aprenderlas y para enseñarlas.

A mis amigos de la prepa: Felipe, Manuel, Wako, María, Martina, Montse, Esteli, Caro, Fer, Nat y Juan Carlos (que no es precisamente de la prepa, pero como si lo fuera), con quienes compartí innumerables momentos divertidos, lloré tantas penas, y con quienes crecí tanto espiritual como intelectualmente.

A Rolando y Tito, con ellos exploré el gusto de la Geometría Algebraica. Es una gran experiencia trabajar con ellos.

A mis amigos de la facultad: Aldo, Rudiger, Ana, Aisha, Eugenia, Alfredito Hubard, Mariano, Mau, Claudia, Cristobal, Silvia, Sara, Alejandra, Karel, Marlosti, Vlad, Julian, Luis Pedro, Gaby, Francisco Barrios y Juanma; de todos ellos siempre aprendí mucho. A Victor Breña, por su amistad y apoyo cuando más lo necesité.

A los cuates del 7 y medio: Daniela, Preisser, Azael, Belén, Kenya, Victorcito, Carlos, Claudio y Orestes. Gracias por tanto apoyo.

A los amigos del Instituto: Selene, Paulina, Chávez, José, Esteban, Grecia y Yesenia por su amistad y toda su ayuda. A Daniel, por su gran ayuda y su inigualable interés por cualquier problema matemático. Muy especialmente a Pietra, por su invaluable amistad.

A mis amigos del Logos: Angel, Sergio, Jorge, Irene, Nalliely, Alejandro, Sergio a la Torre, Marisol, José y Rebe, por su apoyo y su aliento para terminar este trabajo de tesis.

A mi abuela, porque siempre se preocupa por mí. A mis hermanos y mis sobrinos, que todos ellos siempre están en mi corazón.

A los abuelos Jorge, Nacha y Arturo, porque siempre los vamos a extrañar.

A la familia Martínez–Cáceres, a Regina, Nona, María, Mabel mamá, Julián y Mamotrín, por aceptarme en su casa y en su corazón.

A las familias Beltrán del Río García, Riva Palacio Nieto, Peñalosa Nájera, y Cariño García; por su cariño y apoyo.

Índice general

Introducción

El objetivo de este trabajo es recopilar los preliminares necesarios para presentar el Teorema de Riemann-Roch para curvas algebraicas, y su prueba. La importancia de este teorema radica en la clasificación de dichas curvas, pues relaciona las propiedades de las curvas de naturaleza puramente algebraica, con las propiedades de naturaleza topológica.

El material que se expone en esta tesis está basado principalmente en el libro *Algebraic Curves, William Fulton* [4], en el que se estudian las curvas algebraicas como introducción a la geometría algebraica.

El lector de este trabajo de tesis necesita como prerrequisito, un conocimiento básico de geometría algebraica, de resultados importantes y fundamentales en ella, como son el Teorema de los Ceros de Hilbert, y el Teorema de Bézout sobre intersección de curvas algebraicas.

Durante el primer capítulo de esta tesis se desarrollan preliminares algebraicos, y de geometría algebraica en general. El segundo capítulo está dedicado al estudio de curvas algebraicas planas, en el que se asocian estructuras algebraicas a dichas curvas, y se relacionan estas estructuras con las propiedades geométricas de las curvas. Dado que el Teorema de Riemann-Roch se cumple para curvas con puntos no singulares, el tercer capítulo está dedicado a mostrar que se pueden tomar modelos no singulares de las curvas, sin perder la información algebraica que asociamos en el segundo capítulo. Por último, el cuarto capítulo es la presentación y demostración del Teorema de Riemann-Roch.

Capítulo 1

Preliminares

1.1. Anillos de Valuación Discreta

Definición 1.1.1. Sea B un dominio entero, K su campo de cocientes. Decimos que B es un *anillo de valuación* de K, si para cada $x \in K$ no nulo, se tiene que $x \in B$ o $x^{-1} \in B$ (o ambos).

Proposición 1.1.1. *Sea B un dominio entero, K su campo de cocientes. Si B es anillo de valuación de K, entonces B es un anillo local.*

Demostración. Sea $\mathfrak{m}$ el conjunto de los elementos que no son unidades de B, de manera que $x \in \mathfrak{m} \Leftrightarrow x = 0$ o $x^{-1} \notin B$. Si $a \in B$ y $x \in \mathfrak{m}$ se tiene que $ax \in \mathfrak{m}$, de lo contrario $(ax) \notin \mathfrak{m} \Rightarrow (ax)^{-1} \in B$, y por tanto $x^{-1} = a \cdot (ax)^{-1} \in B \Rightarrow x \notin \mathfrak{m}$. Ahora, si tomamos x, y elementos no nulos de $\mathfrak{m}$, entonces $xy^{-1} \in B$ o $x^{-1}y \in B$, por ser B anillo de valuación de K. Si $xy^{-1} \in B$ entonces $x + y = (1 + xy^{-1})y \in B\mathfrak{m} \subseteq \mathfrak{m}$, y análogamente si $x^{-1}y \in B$. Por lo tanto $\mathfrak{m}$ es un ideal y por consiguiente B es un anillo local pues fuera de $\mathfrak{m}$ sólo hay unidades de B. ■

Definición 1.1.2. Sea K un campo. Una *valuación discreta* en K es una aplicación suprayectiva $\nu : K^* \to \mathbb{Z}$ (donde $K^* = K - \{0\}$ es el grupo multiplicativo de K) tal que

1) $\nu(xy) = \nu(x) + \nu(y)$, es decir, ν es un homomorfismo de grupos.

2) $\nu(x + y) \geq \min[\nu(x), \nu(y)]$

El conjunto formado por el 0 y todas las $x \in K^*$ tales que $\nu(x) \geq 0$ es un anillo de valuación, llamado el *anillo de valuación de ν*. Éste es un subanillo del campo K. Algunas veces es conveniente extender ν a todo K poniendo $\nu(0) = +\infty$.

Definición 1.1.3. Un dominio entero A es un *anillo de valuación discreta* si existe una valuación discreta ν de su campo de cocientes K, tal que A es el anillo de valuación de ν.

Proposición 1.1.2. *Sea A un dominio entero, y K su campo de cocientes. Si A es un anillo de valuación discreta, entonces es un anillo local, y su ideal maximal $\mathfrak{m}$ es el conjunto $\{x \in K \mid \nu(x) > 0\}$*

Demostración. A es un anillo local en virtud de la Proposición 1.1.1. Ahora, observemos que $\nu(1) = 0$ y esto es porque $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \Rightarrow \nu(1) = 0$. Veamos que $\nu(x^{-1}) = -\nu(x)$, y esto sucede porque $0 = \nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1})$ lo cual implica que $\nu(x^{-1})$ es el inverso aditivo en $\mathbb{Z}$ de $\nu(x)$ por lo tanto $\nu(x^{-1}) = -\nu(x)$. Como A es anillo de valuación de ν, entonces los elementos de A cumplen $\nu(x) \geq 0$. Así, si $u \in A$ es una unidad de A, entonces $\nu(u)$ y $\nu(u^{-1})$ son mayores o iguales a cero. Dado que $\nu(u) = -\nu(u^{-1})$, y ambos son enteros positivos o iguales a cero, entonces, $\nu(u) = \nu(u^{-1}) = 0$. Esto es, todas las unidades de A van a dar al 0 bajo ν, y viceversa, todos los elementos que van al cero bajo ν son unidades de A. Esto se debe a que si $\nu(x) = 0$ con $x \in A$ entonces $0 = \nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1}) = 0 + \nu(x^{-1}) = \nu(x^{-1})$. Como A es anillo de valuación discreta, se tiene que $\nu(x^{-1}) = 0 \Rightarrow x^{-1} \in A$. Esto es, x es unidad en A. Si definimos $\mathfrak{m} = \{x \in K \mid \nu(x) > 0\}$ entonces en $A - \mathfrak{m}$ sólo hay unidades de A por lo que $\mathfrak{m}$ es el ideal maximal. ■

Haremos algunas caracterizaciones de los anillos de valuación discreta (AVD) en el siguiente lema.

Lema 1.1.1. *Sean A un dominio entero, $\mathfrak{m}$ su ideal maximal, y K su campo de cocientes. Si A es un AVD, entonces se cumplen las siguientes afirmaciones:*

i) Si dos elementos $x, y \in A$ tienen la misma valuación, entonces los ideales que generan son el mismo.

ii) Si $I \neq 0$ es un ideal de A, entonces existen $k \in \mathbb{N}$ y $x \in I$ tales que $\nu(x) = k$ y $\nu(y) \geq k \ \ \forall y \in I$.

iii) A es noetheriano.

iv) El ideal $\mathfrak{m}$ es principal.

v) Cada ideal no nulo de A es una potencia de $\mathfrak{m}$.

Demostración. La proposición (i) se debe a que, si $x, y \in A$ tales que $\nu(x) = \nu(y)$, entonces $\nu(xy^{-1}) = 0$, y esto implica que $u = xy^{-1}$ es una unidad de A, y por consiguientes $\langle x \rangle = \langle y \rangle$.

Para la proposición (ii) tomamos $I \neq 0$ un ideal de A, y sea $\Im(I)$ la imagen de I bajo ν; como $I \subset A$ entonces $\Im(I) \subset \mathbb{N}$, por lo que $\Im(I)$ tiene un primer elemento. Sea k ese elemento. Por ser $\nu : K^* \to \mathbb{Z}$ suprayectiva, entonces $\exists x \in I$ tal que $\nu(x) = k$. Por la condición de minimalidad de k tenemos que $\forall y \in I$, $\nu(y) \geq k$. Observemos que $\exists y \in I$ tal que $\nu(y) = k + 1$ pues, por ser ν suprayectiva, existe un elemento $z_0 \in A$ tal que $\nu(z_0) = 1$ y entonces tenemos que $y = xz_0 \in I$ y $\nu(xz_0) = \nu(x) + \nu(z_0) = k + 1$. Con esto, junto con el inciso (i), concluimos que los únicos ideales distintos de 0 en A son los ideales $\mathfrak{m}_k = \{y \in A | \nu(y) \geq k\}$, que forman una cadena única $\mathfrak{m} \supset \mathfrak{m}_2 \supset \mathfrak{m}_3 \supset \ldots$, y por tanto A es noetheriano, lo que prueba (iii).

Demostremos (iv): Nuevamente, como $\nu : K^* \to \mathbb{Z}$ es suprayectiva, $\exists t \in A$ tal que $\nu(t) = 1$. Como esta t no puede ser unidad de A, entonces $t \in \mathfrak{m}$, y $t^{-1} \notin A$ y $\nu(t^{-1}) = -1$. Sea $y \in \mathfrak{m}$ entonces $\nu(yt^{-1}) = \nu(y) - 1 \geq 0$, lo cual implica que $yt^{-1} \in A$. Así, $y = at$ para algún $a \in A$, y por lo tanto $y \in \langle t \rangle$, entonces $\mathfrak{m} \subset \langle t \rangle$. Como $t \in \mathfrak{m} \Rightarrow \langle t \rangle \subset \mathfrak{m}$, con lo que hemos mostrado que $\langle t \rangle = \mathfrak{m}$.

Por último, como todo ideal no nulo es de la forma $\mathfrak{m}_k$ $(k \geq 1)$, y $\mathfrak{m} = \langle t \rangle$ entonces, por inducción, supongamos que $\mathfrak{m}_{k-1} = \langle t^{k-1} \rangle$. Sea $y \in \mathfrak{m}_k$, entonces $\nu(y) \geq k > k - 1$. Con esto $y \in \mathfrak{m}_{k-1}$, lo cual implica que $y = at^{k-1}$ para algún $a \in A$. Tenemos que a no puede ser unidad de A. De lo contrario $\nu(y) = \nu(at^{k-1}) = \nu(t^{k-1}) = (k-1)\nu(t) = k - 1$, lo cual contradice que $\nu(y) > k - 1$. Por tanto $a \in \mathfrak{m}$ lo que nos dice que $a = a't$ con $a' \in A$. Esto es, $y = a't^k$, esto implica que $\mathfrak{m}_k = \langle t^k \rangle = \mathfrak{m}^k$. Con lo cual (v) queda demostrado. ■

Corolario 1.1.1. *Si A es un AVD, entonces A es un Dominio de Ideales Principales.*

Demostración. Por el Lema 1.1.1, sabemos que todo ideal no nulo de A es potencia del ideal $\mathfrak{m}$, y también que $\mathfrak{m}$ es principal, por tanto, si $\mathfrak{m} = \langle t \rangle$ con $t \in A$, entonces claramente $\langle t^n \rangle = \mathfrak{m}^n$. ■

Lema 1.1.2. *Si t es un elemento de A que va a dar al 1 bajo ν, entonces para cualquier elemento $z \in A$ no nulo, podemos escribir de modo único $z = ut^n$ con $n \geq 0$ y u una unidad en A.*

Demostración. Supongamos que z es unidad en A, entonces hacemos $z = zt^0$. Supongamos ahora que z no es unidad, entonces $z = z_1 t$ para algún $z_1 \in A$. Si z_1 es unidad, aquí terminamos la prueba, si no, tenemos que $z_1 = z_2 t$ para cierto $z_2 \in A$. Continuando de esta manera, obtendremos una sucesión infinita $z_1, z_2, \ldots$ con $z_k = z_{k+1} t$. Como A es noetheriano, la cadena $\langle z_1 \rangle \subset \langle z_2 \rangle \subset \ldots$ se estaciona. Esto es, $\langle z_n \rangle = \langle z_{n+1} \rangle$ para un cierto n. Entonces $z_{n+1} = v z_n$ para algún $v \in A$, y por lo tanto $z_n = v t z_n \Rightarrow vt = 1$, pero t no es unidad, lo que nos hace concluir que no podemos formar dicha cadena y por tanto $z = ut^n$ con u unidad en A y $n > 0$.

Para mostrar la unicidad, supongamos que $ut^n = vt^m$ con u, v unidades en A, y sin pérdida de generalidad supongamos que $n \geq m$. Entonces $ut^{n-m} = v$ es unidad, pero como t^k no es unidad para ninguna potencia $k > 0$, entonces $n = m$. ■

Definición 1.1.4. Un elemento t como en el Lema 1.1.2 se denomina *parámetro de uniformización* de A.

Sean t y t' parámetros de uniformización, entonces $\langle t' \rangle = \mathfrak{m} = \langle t \rangle$. En virtud del Lema 1.1.2 tenemos $t' = ut^n$ con u unidad en A y n entero no negativo, por lo tanto $\langle t' \rangle = \langle t^n \rangle = \mathfrak{m}_n$. Pero $\langle t' \rangle = \mathfrak{m}$ por lo que $n = 1$ y entonces $t' = ut$. Con esto tenemos la siguiente observación.

Observación 1.1.1. *Cualesquiera dos parámetros de uniformización de A son asociados.*

Lema 1.1.3. *Sean A un AVD, K su campo de cocientes, y t un parámetro de uniformización fijo. Entonces todo elemento no nulo $z \in K$ se puede escribir de manera única en la forma $z = ut^n$, donde u es unidad en A y $n \in \mathbb{Z}$.*

Demostración. Por el Corolario 1.1.1 sabemos que A es un Dominio de Ideales Principales, entonces A es un Dominio de Factorización Única (DFU). Sea $z \in K$ un elemento no nulo, entonces $z = ab^{-1}$ con $a, b \in A$ sin factores comunes. Supongamos que también se tiene $z = cd^{-1}$ con $c, d \in A$ también sin factores comunes, entonces debe pasar que $ad = bc$. Por un lado esto nos dice que $b \mid ad$ pero $b \nmid a$, y esto implica que $b \mid d$. Esto es $b = de$ con $e \in A$. Por otro lado tenemos también que $a \mid bc$. Como $a \nmid b$, debe tenerse que $c \mid a$. Esto es, $a = cf$ con $f \in A$. Tenemos entonces que, $cd^{-1} = z = ab^{-1} = (cf)(de)^{-1} = (cd^{-1})(fe^{-1})$. Dado que A es DFU entonces, $cd^{-1} = (cd^{-1})(fe^{-1})$. Esto es, $fe^{-1} = u$ con u unidad en A. Por el Lema 1.1.2 sabemos que todo elemento no nulo de A lo podemos escribir como una potencia del parámetro de uniformización multiplicado por una unidad, entonces $z = ab^{-1} = (ut^l)(vt^m)^{-1} = wt^{l-m}$, donde u, v, w son unidades en A, $w = uv^{-1}$ y $n = l - m \in \mathbb{Z}$. ■

Definición 1.1.5. Sean A un AVD, K su campo de cocientes, t un parámetro de uniformización fijo y $z \in K$ un elemento no nulo. Al exponente n del Lema 1.1.3 se le llama *orden* de z y lo denotamos $n = ord(z)$. Definimos también $ord(0) = \infty$.

Observación 1.1.2. *Con el orden definido en la Definición 1.1.5, tenemos que $A = \{z \in K \mid ord(z) \geq 0\}$ y $\mathfrak{m} = \{z \in K \mid ord(z) > 0\}$.*

Con todo lo estudiado hasta el momento, hemos llegado a una forma sencilla de caracterizar a los Anillos de Valuación Discreta (AVD), como mostramos en la siguiente proposición.

Proposición 1.1.3. *Las siguientes afirmaciones son equivalentes:*

i) A es un Anillo de Valuación Discreta.

ii) A es un anillo local noetheriano, y su ideal maximal $\mathfrak{m}$ *es principal.*

iii) Existe un elemento irreducible $t \in A$ *tal que cada* $z \in A$ *no nulo se puede escribir de modo único en la forma* $z = ut^n$, *con u unidad en A, n un entero no negativo.*

Demostración. La Proposición 1.1.2, y el Lema 1.1.1 nos indican que $(i) \Rightarrow (ii)$; el Lema 1.1.2 nos demuestra $(ii) \Rightarrow (iii)$. Por último, si tomamos la función de orden como en la Definición 1.1.5, entonces $ord : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ nos da una una valuación discreta, lo que muestra que $(iii) \Rightarrow (i)$. ■

Ejemplo 1.1.1. Los dos ejemplos típicos de Anillos de Valuación Discreta son:

1) $K = \mathbb{Q}$. Tomando un primo fijo p, entonces cada $x \in \mathbb{Q}$ no nulo se puede escribir de manera única en la forma $p^a y$, donde $a \in \mathbb{Z}$ y tanto numerador como denominador de y son ambos primos relativos con p. Se define $\nu_p(x) = a$. El anillo de valuación de ν_p es el anillo local $\mathbb{Z}_{\langle p \rangle}$.

2) $K = k(X)$, donde k es un campo y X una indeterminada. Se toma un polinomio irreducible $f \in k[X]$ y se define ν_f como en 1). El anillo de valuación de ν_f es entonces el anillo local de $k[X]$ respecto al ideal primo $\langle f \rangle$.

Proposición 1.1.4. *Sea R un AVD con campo de cocientes K, y M el ideal maximal de R. Si S, es otro AVD, cuyo ideal maximal contiene a M, y* $R \subset S \subset K$, *entonces* $S = R$.

Demostración. Sea M_S el ideal maximal de S, entonces por hipótesis tenemos que $M \subset M_S$, sea $z \in S$ tal que $z \notin R$, como $z \notin R$ pero $z \in K$ entonces $z^{-1} \in M$ (porque R es anillo de valuación de K), y por tanto $z^{-1} \in M_S$, lo cual implica que $z \in K$ pero $z \notin S$ por ser S anillo de valuación de K, lo cual es una contradicción, por lo que $z \in R$ y por tanto $R = S$. ■

Proposición 1.1.5. *Sea R un AVD con campo de cocientes K, y se designa con ord, la función orden sobre K.*

(a) *Si* $ord(a) < ord(b)$, *entonces* $ord(a + b) = ord(a)$.

(b) *Si* $a_1, \ldots, a_n \in K$, *y para algún i,* $ord(a_i) < ord(a_j)$ *(todos los* $j \neq i$*), entonces* $a_1 + \ldots + a_n \neq 0$.

Demostración. Como $ord(a) < ord(b)$ entonces $ord(a) \neq \infty$, con lo cual $a \neq 0$, pues si $a = 0$ entonces $ord(a) = \infty$ y como no existe $z \in \mathbb{Z}$ tal que $\infty < z$, y dado que $ord : K^* \to \mathbb{Z}$ es sobre, entonces $b = 0$, por lo que $ord(a) = ord(b) = \infty$ y no se tendría $ord(a) < ord(b)$; por lo tanto $a \neq 0$. Ahora, dado que $a \neq 0$ entonces $a^{-1} \in K$; como $ord(a) < ord(b)$ se tiene que $0 < ord(b) - ord(a) \Rightarrow 0 < ord(ba^{-1})$ y por tanto $ba^{-1} \in R$ y no es unidad en R, por tanto $ab^{-1} \in K$.

Si $b = 0$, entonces $ord(a+b) = ord(a+0) = ord(a)$, y está demostrada la igualdad. En cambio, supongamos $b \neq 0$, entonces $ord(a+b) - ord(b) = ord((a+b)b^{-1}) = ord(ab^{-1}+1) = ord(ab^{-1}) + ord(1) = ord(ab^{-1}) = ord(a) - ord(b)$, esto se reduce a que $ord(a+b) - ord(b) = ord(a) - ord(b)$, por lo tanto $ord(a+b) = ord(a)$.

Para demostrar la segunda parte, tomemos como hipótesis un número finito de elementos $a_1, \ldots, a_n \in K$ tal que para alguna i se cumple que $ord(a_i) < ord(a_j)$ si $i \neq j$; entonces, al igual que en la primera parte de esta demostración, se tiene que $ord(a_i) \neq \infty \Rightarrow a_i \neq 0$, supongamos sin pérdida de generalidad que a_1 es tal que $ord(a_1) < ord(a_i)$ con $i = 2, \ldots, n$, y supongamos también que $a_1 + \ldots + a_n = 0$, entonces, al ser a_1 no nulo, y sea $b = a_2 + \ldots + a_n$ entonces $b = -a_1$, pero también se tiene que $ord(b) \geq \text{mín}\{ord(a_i)\} > ord(a_1)$, y por la primera parte de esta proposición, tenemos que $ord(a_1) = ord(a_1 + b) = ord(a_1 - a_1) = ord(0) = \infty$, con lo cual tenemos que $ord(a_1) = \infty$, que es una contradicción. Por lo tanto $a_1 + \ldots + a_n \neq 0$. ∎

Proposición 1.1.6. *Sea R un AVD cuyo ideal maximal es M, y campo de cocientes K. Supóngase que existe un campo k subanillo de R, tal que la composición $k \to R \to R/M$ es un isomorfismo de k con R/M. Entonces:*

(a) *Para todo $z \in R$, existe un único $\lambda \in k$, tal que $z - \lambda \in M$.*

(b) *Si t es un parámetro de uniformización para R, y $z \in R$. Entonces para cada $n \geq 0$ existen $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ y $z_n \in R$ únicos, tales que $z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \ldots + \lambda_n t^n + z_n t^{n+1}$.*

Demostración. (a): Sea $z \in R$ y tomemos su clase $z + M \in R/M$, como la inclusión seguida del paso al cociente es un isomorfismo entre k y R/M, entonces existe un único $\lambda \in k$ tal que $\lambda + M = z + M$, por lo tanto $z - \lambda \in M$.

(b): La demostración de la existencia será por inducción sobre n, entonces para $n = 0$, dado que $z \in R$, gracias al inciso (a) tenemos que existe un único $\lambda_0 \in k$ tal que $z - \lambda_0 \in M$, por ser t un parámetro de uniformización, entonces $z - \lambda_0 = z_0 t$ con $z_0 \in R$, entonces $z = \lambda_0 + z_0 t$. Supongamos ahora que la proposición es cierta para $n = s$, entonces existen $\lambda_0, \ldots, \lambda_s \in k$ y $z_s \in R$ tales que $z = \lambda_0 + \lambda_1 t + \ldots + \lambda_s t^s + z_s t^{s+1}$; como $z_s \in R$, por el inciso (a) existe un único $\lambda_{s+1} \in k$ tal que $z_s - \lambda_{s+1} \in M$, entonces

$z_s - \lambda_{s+1} = z_{s+1}t$ con cierta $z_{s+1} \in R$, entonces $z_s = \lambda_{s+1} + z_{s+1}t$, por lo tanto $z = \lambda_0 + \lambda_1 t + \ldots + \lambda_s t^s + (\lambda_{s+1} + z_{s+1}t)t^{s+1} = \lambda_0 + \lambda_1 t + \ldots + \lambda_s t^s + \lambda_{s+1}t^{s+1} + z_{s+1}t^{s+2}$, lo cual concluye el paso inductivo.

Para demostrar la unicidad: supongamos que existe n tal que $\lambda_0 + \lambda_1 t + \ldots + \lambda_n t^n + z_n t^{n+1} = z = \lambda'_0 + \lambda'_1 t + \ldots + \lambda'_n t^n + z'_n t^{n+1}$, sea $\gamma_i = \lambda_i - \lambda'_i$, y $w_n = z_n - z'_n$, por lo tanto $\gamma_0 + \gamma_1 t + \ldots + \gamma_n t^n + w_n t^{n+1} = 0$, donde cada $\gamma_i \in k$ y $w_n \in R$. Si $\gamma_i = 0$ para toda i, entonces $w_n t^{n+1} = 0$, por ser t parámetro de uniformización, entonces $w_n = 0$, con lo cual $z_n = z'_n$ y $\lambda_i = \lambda'_i$ para toda i, y terminamos.

Ahora haremos el caso en que $\gamma_i \neq 0$ para alguna i. Primero observemos que por estar $\gamma_i \in k$, y $k \cong R/M$, si $\gamma_i \neq 0$, entonces $ord(\gamma_i) = 0$, pues γ_i es unidad; ahora veamos que $ord(w_n t^{n+1}) = ord(w_n) + ord(t^{n+1}) = n + 1 + ord(w_n) \geq n + 1$, pues $ord(w_n) \geq 0$ porque $w_n \in R$. Supongamos que $\gamma_i \neq 0$ para algunas i, sea $A = \{\gamma_{i_1}, \ldots, \gamma_{i_r}\} \subset \{\gamma_0, \ldots, \gamma_n\}$ tal que $\gamma_{i_j} \neq 0$ para toda j, y $i_j < i_{j+1}$ con $j = 1, \ldots, r-1$, además $\gamma_i = 0$ si $\gamma_i \notin A$. Entonces $0 = \gamma_{i_1} t^{i_1} + \ldots + \gamma_{i_r} t^{i_r} + w_n t^{n+1}$, como $ord(\gamma_{i_1} t^{i_1}) = i_1 < i_j$ $(j = 2, \ldots, r)$, entonces $ord(\gamma_{i_1} t^{i_1}) < ord(\gamma_{i_j} t^{i_j})$ con $i_j \neq i_1$, y también $ord(\gamma_{i_1} t^{i_1}) \leq n < n + 1$, entonces $ord(\gamma_{i_1} t^{i_1}) < ord(w_n t^{n+1})$, por la Proposición 1.1.5 tenemos que $\gamma_{i_1} t^{i_1} + \ldots + \gamma_{i_r} t^{i_r} + w_n t^{n+1} \neq 0$, lo cual es una contradicción, por lo tanto $\gamma_i = 0$ para todo i. ■

1.2. Cambio de Coordenadas

Dado un conjunto cualquiera V (no vacío), y k un campo, indicaremos por $\Im(V,k)$ al conjunto de todas las funciones de V en k. El conjunto $\Im(V,k)$ tiene estructura de anillo con las operaciones usuales: si $f,g \in \Im(V,k)$, $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = f(x)\cdot g(x)$, para todo $x \in V$. Comúnmente se identifica k con el subanillo de $\Im(V,k)$ formado por todas las funciones constantes.

Denotemos con $\mathbb{A}^n$, al espacio afín de dimensión n. A lo largo de esta sección entenderemos por variedad, a una variedad algebraica afín.

Definición 1.2.1. Si $V \subset \mathbb{A}^n$ es una variedad, una función $f \in \Im(V,k)$ se denomina *función polinomial* si existe un polinomio $F \in k[X_1,\ldots,X_n]$ tal que $f(a_1,\ldots,a_n) = F(a_1,\ldots,a_n)\ \forall\ (a_1,\ldots,a_n) \in V$.

Las funciones polinomiales constituyen un subanillo de $\Im(V,k)$ que contiene a k. Dos polinomios F, G determinan una misma función si y sólo si $(F-G)(a_1,\ldots,a_n) = 0$ para todo $(a_1,\ldots,a_n) \in V$, es decir, $(F-G) \in I(V)$. Recordemos que el anillo coordenado para un conjunto algebraico $V \subset \mathbb{A}^n$ se define como $\Gamma(V) = k[X_1,\ldots,X_n]/I(V)$. Entonces podemos identificar a $\Gamma(V)$ con el subanillo de $\Im(V,k)$ formado por todas las funciones polinomiales de V.

Definición 1.2.2. Sean $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades. Una función $\varphi : V \longrightarrow W$ se denomina *aplicación polinomial* si existen polinomios $T_1,\ldots,T_m \in k[X_1,\ldots,X_n]$ tales que $\varphi(a_1,\ldots,a_n) = (T_1(a_1,\ldots,a_n),\ldots,T_m(a_1,\ldots,a_n))$ para todo $(a_1,\ldots,a_n) \in V$.

Una función $\varphi : V \longrightarrow W$ induce un homomorfismo $\widetilde{\varphi} : \Im(W,k) \longrightarrow \Im(V,k)$, donde $\widetilde{\varphi}(f) = f \circ \varphi$. Si φ es una aplicación polinomial, entonces $\widetilde{\varphi}(\Gamma(W)) \subset \Gamma(V)$, por lo tanto $\widetilde{\varphi}$ se restringe a un homomorfismo (también designado por $\widetilde{\varphi}$) de $\Gamma(W)$ a $\Gamma(V)$; y si $f \in \Gamma(W)$ es la $I(W)-$clase residual de un polinomio F, entonces $\widetilde{\varphi}(f) = f \circ \varphi$ es la $I(V)-$clase residual del polinomio $F(T_1,\ldots,T_m)$.

Proposición 1.2.1. *Sean $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades afines. Existe una correspondencia natural uno a uno entre las aplicaciones polinomiales $\varphi : V \longrightarrow W$ y los homomorfismos $\widetilde{\varphi} : \Gamma(W) \longrightarrow \Gamma(V)$. Una tal aplicación φ es la restricción de una aplicación polinomial de $\mathbb{A}^n$ en $\mathbb{A}^m$.*

Demostración. Supóngase que $\alpha : \Gamma(W) \longrightarrow \Gamma(V)$ es un homomorfismo. Elijamos $T_i \in k[X_1,\ldots,X_n]$ tales que $\alpha(\overline{X_i}) = \overline{T_i}$, $i = 1,\ldots,m$ y donde $\overline{X_i}$ denota a la $I(W)-$clase de X_i, y $\overline{T_i}$ denota a la $I(V)-$clase de T_i. Entonces $T = (T_1,\ldots,T_m)$ es una aplicación

polinomial de $\mathbb{A}^n$ en $\mathbb{A}^m$, que induce $\widetilde{T} : \Gamma(\mathbb{A}^m) \longrightarrow \Gamma(\mathbb{A}^n)$, es decir $\widetilde{T} : k[X_1, \ldots, X_m] \longrightarrow k[X_1, \ldots, X_n]$. Por lo que tenemos $\widetilde{T}(I(W)) \subset I(V)$, y por lo tanto que $T(V) \subset W$, luego T se restringe a una aplicación polinomial $\varphi : V \longrightarrow W$. Y por la construcción tenemos que $\widetilde{\varphi} = \alpha$. Dado que conocemos la manera de construir $\widetilde{\varphi}$ a partir de φ, la demostración queda terminada. ■

Si $T = (T_1, \ldots, T_m)$ es una aplicación polinomial de $\mathbb{A}^n$ en $\mathbb{A}^m$, y $F \in k[X_1, \ldots, X_m]$, escribiremos $F^T = F(T_1, \ldots, T_m)$. Para ideales I y conjuntos algebraicos V de $\mathbb{A}^m$, designaremos por I^T al ideal de $k[X_1, \ldots, X_n]$ generado por $\{F^T \mid F \in I\}$ y por V^T al conjunto algebraico $T^{-1}(V) = V(I^T)$, donde $I = I(V)$.

Definición 1.2.3. Un *cambio de coordenadas afín* en $\mathbb{A}^n$ es una aplicación polinomial $T = (T_1, \ldots, T_n) : \mathbb{A}^n \longrightarrow \mathbb{A}^n$ tal que cada T_i es un polinomio de grado 1, y que T es inyectiva y sobre.

Con esta definición podemos escribir $T_i = \sum a_{ij} X_j + a_{i0}$, entonces podemos ver a T como una composición de una transformación lineal seguida de una traslación, es decir, $T = T'' \circ T'$, donde T' es de la forma $T_i' = \sum a_{ij} X_j$ y T'' es de la forma $T_i'' = X_i + a_{i0}$.

Como toda traslación posee una inversa (que es también una traslación), es claro que T es inyectiva y supra si y sólo si T' es invertible.

Sean $P = (a_1, \ldots, a_n)$ y $Q = (b_1, \ldots, b_n)$ dos puntos distintos de $\mathbb{A}^n$. La recta determinada por P y Q se define por

$$\{(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) \mid t \in k\}$$

Proposición 1.2.2. *Sean P, $P' \in \mathbb{A}^2$ y L_1, L_2 dos rectas distintas que pasan por P; L_1', L_2' dos rectas distintas que pasan por P'. Entonces existe un cambio de coordenadas afín T de $\mathbb{A}^2$ tal que $T(P) = P'$ y $T(L_i) = L_i'$ $(i = 1, 2)$.*

Demostración. Sean $Q_i \in L_i$ y $Q_i' \in L_i'$ $(i = 1, 2)$ puntos en cada recta distintos de P y P', entonces

$$L_1 = P + t_1(Q_1 - P) \quad \text{y} \quad L_2 = P + t_2(Q_2 - P)$$

con $t_i \in k$ $(i = 1, 2)$, análogamente podemos escribir

$$L_1' = P' + s_1(Q_1' - P') \quad \text{y} \quad L_2' = P' + s_2(Q_2' - P')$$

con $s_i \in k$ $(i = 1, 2)$.

Supongamos que las coordenadas de cada punto que elegimos son: $Q_1 = (b_1, b_2)$, $Q_2 = (c_1, c_2)$; $Q_1' = (\beta_1, \beta_2)$, $Q_2' = (\gamma_1, \gamma_2)$. Sea T_1 el cambio de coordenadas que manda a la

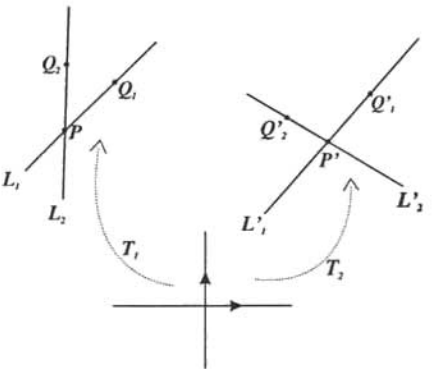


Figura 1.1: Cambios de coordenadas T_1 y T_2

terna canónica $\{(0,0), (1,0), (0,1)\}$, en la terna $\{P, Q_1, Q_2\}$, dicha T_1 la podemos pensar como $T_1 = Ax + P$, donde

$$A = \begin{pmatrix} b_1 - a_1 & c_1 - a_1 \\ b_2 - a_2 & c_2 - a_2 \end{pmatrix}$$

y $x = (X, Y)$ el vector de indeterminadas; análogamente, sea T_2 el cambio de coordenadas que manda a la terna canónica en la terna $\{P', Q'_1, Q'_2\}$, entonces también $T_2 = Bx + P'$, donde

$$B = \begin{pmatrix} \beta_1 - \alpha_1 & \gamma_1 - \alpha_1 \\ \beta_2 - \alpha_2 & \gamma_2 - \alpha_2 \end{pmatrix}$$

Como $L_1 \neq L_2$, entonces A es invertible, y también, dado que $L'_1 \neq L'_2$, también B resulta invertible, entonces el cambio de coordenadas T que buscamos, es la composición $T_2 \circ T_1^{-1}$, es decir, como $T_1^{-1} = A^{-1}x - A^{-1}(P)$, entonces $T = T_2 \circ T_1^{-1} = B(A^{-1}x - A^{-1}(P)) + P' = BA^{-1}x - BA^{-1}(P) + P'$.

Claramente $T(P) = P'$, como $T_1^{-1}(Q_1) = (1,0)$ y $T_1^{-1}(Q_2) = (0,1)$, entonces para cualquier punto $(P + t_1(Q_1 - P)) \in L_1$ tenemos que $T(P + t_1(Q_1 - P)) = T_2(T_1^{-1}(P + t_1(Q_1 - P))) = T_2(T_1^{-1}(P) + t_1 T_1^{-1}(Q_1) - t_1 T_1^{-1}(P)) = T_2((0,0) + t_1(1,0) - t_1(0,0)) = P' + t_1 Q'_1 - t_1 P' \in L'_1$, con lo cual $T(L_1) = L'_1$, y un argumento análogo muestra que $T(L_2) = L'_2$. ■

1.3. Funciones Racionales y Anillos Locales

En adelante, nos referiremos a una variedad algebraica afín irreducible, simplemente como variedad afín; por tanto, su anillo coordenado siempre lo tomaremos como un dominio entero.

Definición 1.3.1. Sea V una variedad afín, y $\Gamma(V)$ su anillo coordenado. Definimos el *campo de funciones racionales* de V como el campo de cocientes de $\Gamma(V)$, y lo denotamos con $k(V)$. Un elemento de $k(V)$ es una *función racional* de V.

Definición 1.3.2. Sea V una variedad afín, $P \in V$ y $f \in k(V)$, diremos que f está *definida* en P si para $a, b \in \Gamma(V)$, $f = a/b$, y $b(P) \neq 0$.

Notemos que puede haber distintas maneras de escribir f como cociente de polinomios; f estará definida en P si es posible hallar un "denominador" que no se anule en P.

Si $\Gamma(V)$ es un DFU, entonces la representación de f será única salvo unidades.

Definición 1.3.3. Sea $P \in V$. Definimos el *anillo local de V en P*, que denotamos con $\mathcal{O}_P(V)$, como el conjunto de todas las funciones racionales sobre V que están definidas en P

Observación 1.3.1. *Es claro que $\mathcal{O}_P(V)$ es un subanillo de $k(V)$ y que se tienen las siguientes contenciones:*

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

Definición 1.3.4. El conjunto de puntos $P \in V$ en los que la función racional f no está definida se llama *conjunto de polos* de f.

Proposición 1.3.1. (1) *El conjunto de polos de una función racional sobre V, es un subconjunto algebraico de V.*

(2) $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$

Demostración. (1): Supongamos $V \subset \mathbb{A}^n$. Para cada $G \in k[X_1, \ldots, X_n]$, designemos por $\overline{G}$ la clase de equivalencia de G en $\Gamma(V)$. Sea $f \in k(V)$ y consideramos $J_f = \{G \in k[X_1, \ldots, X_n] \mid \overline{G}f \in \Gamma(V)\}$. Lo primero que mostraremos es que J_f es un ideal de $k[X_1, \ldots, X_n]$ que contiene a $I(V)$.

Sean G_1 y G_2 en J_f, entonces $\overline{G_1}f$ y $\overline{G_2}f$ están en $\Gamma(V)$ y por tanto $\overline{(G_1 + G_2)}f = (\overline{G_1} + \overline{G_2})f = \overline{G_1}f + \overline{G_2}f$ que está en $\Gamma(V)$, lo cual implica que $G_1 + G_2 \in J_f$; ahora, sea $G \in J_f$ y $G' \in k[X_1, \ldots, X_n]$, entonces $\overline{G'} \in \Gamma(V)$, observemos que $\overline{(G'G)}f = (\overline{G'G})f = \overline{G'}(\overline{G}f) \in \Gamma(V)$, con lo cual $G'G \in J_f$. Que $I(V) \subset J_f$ es

inmediato pues en $\Gamma(V)$ tenemos $\overline{I(V)} = 0$ y evidentemente $\overline{I(V)}f = 0f = 0$ que está en $\Gamma(V)$.
Los puntos de $V(J_f)$ son exactamente los puntos en los que f no está definida, porque si pensamos a f como el cociente ab^{-1} con $a, b \in \Gamma(V)$, entonces la clase de los elementos de J_f en $\Gamma(V)$ son elementos de la forma bc con $c \in \Gamma(V)$, pero $b \in J_f$, por lo que, si $P \in V(J_f)$, entonces $\forall g \in J_f$ se tiene $g(P) = 0 \Rightarrow b(P)c(P) = 0$ como $\Gamma(V)$ es dominio entero, y $b \in J_f$ entonces $b(P) = 0$. Hemos mostrado que $V(J_f)$ es el conjunto de polos de f y por tanto hemos mostrado (1).

(2): Si $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$, entonces f está definida en todo V, por tanto $V(J_f) = \varnothing$, por el Teorema de los ceros (Nullstellensatz) de Hilbert débil[1], $1 \in J_f \Rightarrow \overline{1}f = f \in \Gamma(V) \Rightarrow \bigcap_{P \in V} \mathcal{O}_P(V) \subset \Gamma(V)$, y como ya habíamos observado, $\Gamma(V) \subset \mathcal{O}_P(V)$ para todo $P \in V$, por lo tanto, $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$.

■

La prueba del inciso (1) en la Proposición anterior nos motiva a la siguiente definición.

Definición 1.3.5. Sea $f \in \mathcal{O}_P(V)$, definimos el *valor de f en P*, que denotaremos $f(P)$, de la siguiente manera: escribimos $f = ab^{-1}$, con $a, b \in \Gamma(V)$ y $b(P) \neq 0$, sea $f(P) = a(P)b^{-1}(P)$.

Observación 1.3.2. El valor de f en P está bien definido, pues en $\Gamma(V)$ se tiene que $a \sim c \Leftrightarrow a-c \in I(V)$ y $b \sim d \Leftrightarrow b-d \in I(V)$, entonces $d(a-c)+(-c)(b-d) = ad-bc \in I(V)$.

Proposición 1.3.2. *El conjunto $\mathcal{O}_P(V)$ es un anillo local y $\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}$ es su ideal maximal, además, $\mathcal{O}_P(V)/\mathfrak{m}_P(V) \cong k$.*

Demostración. Si nos fijamos en el homomorfismo de valuación de $\mathcal{O}_P(V) \longrightarrow k$ que manda $f \mapsto f(P)$, entonces $\mathfrak{m}_P(V)$ es el núcleo de éste homomorfismo, por lo tanto $\mathcal{O}_P(V)/\mathfrak{m}_P(V) \cong k$.
Si tomamos un elemento $g \in \mathcal{O}_P(V) - \mathfrak{m}_P(V)$ entonces g está definida para todo $P \in V$, y además $g(P) \neq 0$ para todo $P \in V$ por lo que si escribimos a g como un ab^{-1}, entonces su inverso sería ba^{-1} que está bien definido en V. Por lo tanto $\mathcal{O}_P(V)$ es anillo local y su ideal maximal es $\mathfrak{m}_P(V)$. ■

Proposición 1.3.3. *$\mathcal{O}_P(V)$ es un dominio local noetheriano.*

[1] [4] Fulton W., *Algebraic Curves*, pág. 20.

Demostración. Gracias a la Proposición 1.3.2 bastará sólo con probar que todo ideal I de $\mathcal{O}_P(V)$ es finitamente generado. Por el Teorema de la Base de Hilbert[2], sabemos que $k[X_1,\ldots,X_n]$ es noetheriano, y el Nullstellensatz[3] nos dice que tenemos una correspondencia biyectiva entre ideales primos de $k[X_1,\ldots,X_n]$ y las variedades algebraicas irreducibles, por lo tanto, $\Gamma(V)$ es noetheriano. Escogemos generadores $f_1,\ldots,f_r$ para el ideal $I\cap\Gamma(V)$. Afirmamos que $f_1,\ldots,f_r$ generan a I como ideal de $\mathcal{O}_P(V)$, puesto que si $f\in I\subset\mathcal{O}_P(V)$, existe un $b\in\Gamma(V)$ con $b(P)\neq 0$ y $bf\in\Gamma(V)$; por lo tanto $bf\in\Gamma(V)\cap I$, entonces $bf=\sum a_if_i$, con $a_i\in\Gamma(V)$, y por tanto $f=\sum(a_i/b_i)f_i$, como se afirmaba. ∎

Este anillo local juega un papel importante en el estudio moderno de las variedades algebraicas. Todas las propiedades de V que dependen de una vecindad de P (las propiedades locales) se reflejan en el anillo $\mathcal{O}_P(V)$.

Proposición 1.3.4. *Sea $T:\ \mathbb{A}^n\longrightarrow\mathbb{A}^n$ un cambio de coordenadas afín, $T(P)=Q$, entonces $T:\ \mathcal{O}_Q(\mathbb{A}^n)\longrightarrow\mathcal{O}_P(\mathbb{A}^n)$ es un isomorfismo, y además, si $P\in V$ entonces T induce un isomorfismo de $\mathcal{O}_Q(V^T)$ a $\mathcal{O}_P(V)$.*

Demostración. Recordemos que $\mathcal{O}_Q(\mathbb{A}^2)=\{f'/g' \mid f',g'\in k[X,Y],\ g'(Q)\neq 0\}$, y $\mathcal{O}_P(\mathbb{A}^2)=\{f/g \mid f,g\in k[X,Y],\ g(P)\neq 0\}$; y que T es de la forma $T=(T_1,T_2)$, con T_i aplicaciones polinomiales. Entonces podemos considerar las composiciones $f'\circ T=f'(T_1,T_2)$ y $g'\circ T=g'(T_1,T_2)$. Así, dado $f'/g'\in\mathcal{O}_Q(\mathbb{A}^2)$, la composición con T nos define un nuevo cociente $\frac{f'\circ T}{g'\circ T}$, este cociente está en $\mathcal{O}_P(\mathbb{A}^2)$, pues $g'\circ T(P)=g'(Q)\neq 0$, entonces el cociente $\frac{f'\circ T}{g'\circ T}$ está definido en $\mathcal{O}_P(\mathbb{A}^2)$.

Para ver que es inyectivo, sea $f'/g',f''/g''\in\mathcal{O}_Q(\mathbb{A}^2)$ tales que $\frac{f'\circ T}{g'\circ T}=\frac{f''\circ T}{g''\circ T}$, entonces $(f'\circ T)(g''\circ T)=(f''\circ T)(g'\circ T)$, y por las propiedades de la composición tenemos $f'g''\circ T=f''g'\circ T$, como T es inyectiva y suprayectiva, entonces $f''g'=f'g''$, con lo cual $f'/g'=f''/g''$, y por tanto la composición con T es inyectiva. Para ver que es suprayectiva, tomamos $f/g\in\mathcal{O}_P(\mathbb{A}^2)$, como T es cambio de coordenadas, entonces T es invertible, por consiguiente $\frac{f\circ T^{-1}}{g\circ T^{-1}}\in\mathcal{O}_Q(\mathbb{A}^2)$, pues $g\circ T^{-1}(Q)=g(P)\neq 0$; y claramente $\frac{(f\circ T^{-1})\circ T}{(g\circ T^{-1})\circ T}=\frac{f}{g}$. ∎

Proposición 1.3.5. *Sea $\{P_1,\ldots,P_r\}$ un conjunto finito de puntos de $\mathbb{A}^n$. Existen entonces polinomios $F_1,\ldots,F_r\in k[X_1,\ldots,X_n]$ tales que $F_i(P_j)=0$ si $i\neq j$ y $F_i(P_i)=1$.*

Demostración. Sea $\{P_t=(a_{t1},\ldots,a_{tn})\}_{t=1}^r$ con $a_{ts}\in k$, un conjunto finito de puntos de $\mathbb{A}^n$. Sea $f=\sum_{j=1}^{n}\left(\prod_{t=1}^{r}(X_j-a_{tj})\right)$, y observemos que f se anula en todos los P_t, es decir,

[2] [4] Fulton W., *Algebraic Curves*, pág. 13.
[3] [4] Fulton W., *Algebraic Curves*, pág. 21.

$f(P_t) = 0$ para $t = 1, \ldots, r$, y basados en esto, definamos

$$f_i(X_1, \ldots, X_n) = \sum_{j=1}^{n} \left(\frac{\prod_{t=1}^{r} (X_j - a_{tj})}{(X_j - a_{ij})} \right)$$

y observemos que entonces $f_i(P_t) = 0$ si $i \neq t$, y $f_i(P_i) \neq 0$, sea $b_i = f_i(P_i)$, entonces definamos $F_i(X_1, \ldots, X_n) = b_i^{-1} f_i(X_1, \ldots, X_n)$. Notemos que con F_i así definida se tiene que $F_i(P_i) = b_i^{-1} f_i(P_i) = b_i^{-1} b_i = 1$ y si $i \neq t$ se tiene que $F_i(P_t) = b_i^{-1} f_i(P_t) = b_i^{-1} \cdot 0 = 0$. ■

Proposición 1.3.6. *Sean $I \subset J$ ideales de un anillo R, existe un homomorfismo canónico de anillos de R/I sobre R/J.*

Demostración. Sea $\varphi : R/I \longrightarrow R/J$ definida por $\varphi(x + I) = x + J$ para cada $x \in R$, esta φ que damos está bien definida porque si se tiene $x + I = y + I \Rightarrow x - y \in I$, como $I \subset J$ entonces $x - y \in J$, por lo tanto $x + J = y + J$. φ es suprayectiva porque si $x + J \in R/J$ entonces sea x' cualquier representante de $x + J$, entonces $\varphi(x' + I) = x' + J = x + J$. ■

Proposición 1.3.7. *Sea I un ideal de un anillo R, y R subanillo de otro anillo S; existe un homomorfismo natural de anillos de R/I en S/IS.*

Demostración. Como en la proposición anterior, sea $\varphi : R/I \longrightarrow S/IS$ definida por $\varphi(x + I) = x + IS$; sólo hay que ver que φ está bien definida. Si $x + I = y + I \Rightarrow x - y \in I$, como $I \subset IS$ entonces $x - y \in IS$, por lo tanto $x + IS = y + IS$. ■

Proposición 1.3.8. *Sean $P = (0, \ldots, 0) \in \mathbb{A}^n$, $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Sea I el ideal $\langle X_1, \ldots, X_n \rangle \subset k[X_1, \ldots, X_n]$. Entonces se tiene que $I\mathcal{O} = \mathfrak{m}$, y por lo tanto $I^r\mathcal{O} = \mathfrak{m}^r$, para toda $r \in \mathbb{Z}$.*

Demostración. Sea $f \in k[X_1, \ldots, X_n]$ tal que $f \in I$, si descomponemos a f como $f = f_0 + f_1 + \ldots + f_d$ donde los f_i son polinomios homogéneos de grado i, entonces $f \in I \Rightarrow f_0 = 0$, por lo tanto, si $F \in I\mathcal{O}$ entonces $F = f \cdot \frac{h}{g}$ con $f \in I$ y $h, g \in k[X_1, \ldots, X_n]$ y $g(P) = 0$, como $F(P) = f(P) \cdot \frac{h(P)}{g(P)} = 0 \cdot \frac{h(P)}{g(P)} = 0$, entonces $I\mathcal{O} \subset M$. Sea $\frac{h}{g} \in M$, entonces $h(P) = 0$ y $g(P) \neq 0$ con $h, g \in k[X_1, \ldots, X_n]$, por lo tanto $h \in I$, pues $h(P) = 0$, entonces $\frac{h}{g} = h \cdot \frac{1}{g}$ con $h \in I$ y $\frac{1}{g} \in \mathcal{O}$, por lo tanto $M \subset I\mathcal{O}$ y entonces $M = I\mathcal{O}$. Observemos que $M^r = (I\mathcal{O})^r = I^r\mathcal{O}^r$, como $\mathcal{O}$ es anillo conmutativo con 1, entonces claramente se tiene que $\mathcal{O}^r \subset \mathcal{O}$; sea $x \in \mathcal{O}$, entonces $x = 1^{r-1}x$, por lo tanto $x \in \mathcal{O}^r$ y entonces $\mathcal{O}^r = \mathcal{O}$. Por lo tanto $M^r = (I\mathcal{O})^r = I^r\mathcal{O}^r = I^r\mathcal{O}$. ■

Proposición 1.3.9. *Sean I, J ideales de un anillo R. Supóngase que I es de generación finita y que $I \subset Rad(J)$, entonces $I^n \subset J$ para un cierto n.*

Demostración. Sean $a_1, \ldots, a_m \in I$ los generadores de I, es decir, $I = \langle a_1, \ldots, a_m \rangle$. Como $I \subset Rad(J)$ entonces $\forall i \in \{1, \ldots, m\}$ existe $n_i \in \mathbb{N}$ tal que $a_i^{n_i} \in J$. Sea entonces $r = \max\{n_i\}$ y sea $n = mr$. Entonces I^n está generado por el conjunto $\{a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_m^{\alpha_m} \mid \sum_{i=1}^n \alpha_i = n\}$.

Sea $x = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_m^{\alpha_m}$ un generador de I^n, como $\sum_{i=1}^m \alpha_i = n = mr$, entonces algún α_i debe ser tal que $\alpha_i \geq r$, pues si todos los exponentes fueran menores que r, entonces $\sum_{i=1}^m \alpha_i < \sum_{i=1}^m r = mr$, lo que implica que $a_1^{\alpha_1} \cdot \ldots \cdot a_m^{\alpha_m}$ no sería generador de I^n. Por lo tanto $\alpha_{i_0} \geq r$, por lo tanto $a_{i_0}^{\alpha_{i_0}} = a_{i_0}^{r-n_{i_0}} \cdot a_{i_0}^{n_{i_0}}$, y como $a_{i_0}^{n_{i_0}} \in J$, entonces $a_{i_0}^{\alpha_{i_0}} \in J$, y por tanto $x \in J$. Como la demostración fue para cualquier generador de I^n, entonces $I^n \subset J$. ■

Lema 1.3.1. *Sean I, J ideales de un anillo R, entonces $Rad(I + J) = R$ si y sólo si $I + J = R$.*

Demostración. Si $I + J = R$, dado que $I \subset Rad(I)$ para cualquier ideal I, entonces $R \subset Rad(I+J) \subset R$, por lo que $Rad(I+J) = R$. Supongamos ahora que $Rad(I+J) = R$, esto es equivalente a que $Rad(I + J) = \langle 1 \rangle$, de la definición del radical tenemos que $1 = 1^n \in I + J$ para algún $n \geq 0$, por lo tanto $I + J = \langle 1 \rangle = R$. ■

Recordemos que dos ideales I, J de un anillo R, son comaximales si y sólo si $I + J = R$.

Proposición 1.3.10. *Sea k algebraicamente cerrado, y sean I, $J \subset k[X_1, \ldots, X_n]$ ideales. Entonces I, J son comaximales si y sólo si $V(I) \bigcap V(J) = \varnothing$.*

Demostración. Sea $R = k[X_1, \ldots, X_n]$. Supongamos que I, J son comaximales, entonces $V(I) \bigcap V(J) = V(I + J) = V(R) = \varnothing$.

Supongamos ahora que $V(I) \bigcap V(J) = \varnothing$, entonces $V(I + J) = \varnothing$, entonces $I(V(I + J)) = I(\varnothing) = R$, entonces $Rad(I + J) = R$, por el Lema 1.3.1 tenemos que $I + J = R$. ■

Lema 1.3.2. *Sean I, J ideales comaximales de un anillo R, entonces $I + J^n = R$. Más aún, I^n y J^m son comaximales para toda m, n.*

Demostración. Haremos la prueba por inducción, y para $n = 1$ entonces $I + J = R$ por hipótesis. Supongamos que se cumple $I + J^n = R$, y necesitamos probar que $I + J^{n+1} = R$. Como $I + J^n = R$ entonces $(I + J^n)J = JR = J$, entonces $IJ + J^{n+1} = J$, pero con esto se tiene que $I + J^{n+1} + IJ = J + I = R$, pero $I + J^{n+1} + IJ = I + J^{n+1}$ porque $IJ \subset I$, en particular $IJ \subset I + J^{n+1}$. Por lo tanto $I + J^{n+1} = I + J^{n+1} + IJ = R$, con lo que $I + J^n$

son comaximales. Que I^n, y J^m sean comaximales se sigue de usar esta primera parte, ya que I^n y J son comaximales, por tanto I^n y J^m son comaximales. ■

Proposición 1.3.11. *Sean $I_1, \ldots, I_N$ ideales de un anillo R, supóngase que I_i y $J_i = \bigcap_{i \neq j} I_j$ son comaximales para todo i. Entonces $I_1^n \bigcap \ldots \bigcap I_N^n = (I_1 \cdot \ldots \cdot I_N)^n = (I_1 \bigcap \ldots \bigcap I_N)^n$ para todo n.*

Demostración. Primero hay que observar que si I_i, J_i son comaximales, entonces I_i e I_j también son comaximales para toda $j \neq i$. Como $I_i + J_i = R$, entonces $(I_i + J_i) + I_j = I_i + (J_i + I_j) = R + I_j = R$ para toda $j \neq i$, pero en ese caso $J_i \subset I_j$ entonces $J_i + I_j = I_j$ para toda $j \neq i$, por lo tanto $I_i + I_j = I_i + (J_i + I_j) = R$ para toda $j \neq i$, por tanto I_i y I_j son también comaximales. Por lo tanto, $I_1 \bigcap \ldots \bigcap I_N = I_1 \cdot \ldots \cdot I_N$.

Ahora observemos que $(I_1 \bigcap \ldots \bigcap I_N)^n = (I_1 \cdot \ldots \cdot I_N)^n = I_1^n \cdot \ldots \cdot I_N^n$, por el Lema 1.3.2 tenemos que $I_1^n \cdot \ldots \cdot I_N^n = I_1^n \bigcap \ldots \bigcap I_N^n$. ■

Proposición 1.3.12. *Sea I un ideal de $k[X_1, \ldots, X_n]$, (k algebraicamente cerrado), y supóngase que $V(I) = \{P_1, \ldots, P_N\}$ es finito. Sea $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$. Entonces existe un isomorfismo natural de $k[X_1, \ldots, X_n]/I$ en $\overset{N}{\underset{i=1}{\times}} \mathcal{O}_i/I\mathcal{O}_i$.*

Demostración. Sean $I_i = I(\{P_i\}) \subset k[X_1, \ldots, X_n]$ ideales maximales distintos que contienen a I, y $R = k[X_1, \ldots, X_n]/I$, y $R_i = \mathcal{O}_i/I\mathcal{O}_i$. Por la Proposición 1.3.7, el homomorfismo canónico φ_i de R en R_i induce un homomorfismo φ de R en $\overset{N}{\underset{i=1}{\times}} R_i$.

Por el Nullstellenzats tenemos que

$$Rad(I) = I(\{P_1, \ldots, P_N\}) = \bigcap_{i=1}^{N} I_i,$$

por lo tanto, de la Proposición 1.3.9 tenemos que $(\bigcap I_i)^d \subset I$ para un cierto d. De la Proposición 1.3.10 sabemos que $\bigcap_{i \neq j} I_j$ e I_i son comaximales, entonces de la Proposición 1.3.11 se sigue que

$$\bigcap (I_j^d) = (I_1 \cdot \ldots \cdot I_N)^d = (\bigcap I_j)^d \subset I.$$

Por la Proposición 1.3.5 podemos escoger $F_i \in k[X_1, \ldots, X_n]$, tal que $F_i(P_j) = 0$ si $i \neq j$, $F_i(P_i) = 1$. Sea $E_i = 1 - (1 - F_i^d)^d$. Nótese que $E_i = F_i^d D_i$ para algún D_i, por lo tanto $E_i \in I_j^d$ si $i \neq j$, y

$$1 - \sum_i E_i = (1 - E_j) - \sum_{i \neq j} E_i \in \bigcap I_j^d \subset I.$$

Si llamamos e_i a la clase residual de E_i en R, tendremos que $e_i^2 = e_i$, $e_i e_j = 0$ si $i \neq j$, y $\sum e_i = 1$.

Afirmación 1. *Si $G \in k[X_1, \ldots, X_n]$, y $G(P_i) \neq 0$, existe un $t \in R$ tal que $tg = e_i$, donde g es la $I-$clase residual de G.*

Supuesta esta afirmación por el momento, mostraremos que φ es un isomorfismo:

φ es uno a uno: Si $\varphi(f) = 0$, entonces para cada i existe un G_i con $G_i(P_i) \neq 0$ y $G_i F \in I$ (donde f es la $I-$clase residual de F). Sea $t_i g_i = e_i$. Entonces $f = \sum e_i f = \sum t_i g_i f = 0$.

φ es suprayectiva: Como $E_i(P_i) = 1$, $\varphi(e_i)$ es unitario en R_i; además, ya que $\varphi_i(e_i)\varphi_i(e_j) = \varphi_i(e_i e_j) = 0$ si $i \neq j$, entonces $\varphi_i(e_j) = 0$ para $i \neq j$. Además $\varphi_i(e_i) = \varphi_i(\sum e_j) = \varphi_i(1) = 1$. Supongamos ahora $z = (a_1/s_1, \ldots, a_N/s_N) \in \times R_i$. En virtud de la Afirmación 1, podemos escribir $t_i s_i = e_i$; entonces $a_i/s_i = a_i t_i$ en R_i, por lo tanto $\varphi_i(\sum t_j a_j e_j) = \varphi_i(t_i a_i) = a_i/s_i$, y $\varphi(\sum t_j a_j e_j) = z$.

Para probar la Afirmación 1, supondremos que $G(P_i) = 1$. Sea $H = 1 - G$. Observemos que $(1-H)(E_i + HE_i + \ldots + H^{d-1}E_i) = E_i - H^d E_i$, entonces $H \in I_i$, por lo tanto $H^d E_i \in I$. Además $g(e_i + he_i + \ldots + h^{d-1}e_i) = e_i$, como deseábamos. ■

Corolario 1.3.1. $dim_k(k[X_1, \ldots, X_n]/I) = \sum_{i=1}^{N} dim_k(\mathcal{O}_i/I\mathcal{O}_i)$.

Corolario 1.3.2. *Si $V(I) = \{P\}$, entonces $k[X_1, \ldots, X_n]/I$ es isomorfo a $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$.*

Proposición 1.3.13. *Sea V una variedad de $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n]$, $P \in V$ y J un ideal de $k[X_1, \ldots, X_n]$ que contenga a I. Sea J' la imagen de J en $\Gamma(V)$. Existe un homomorfismo canónico $\varphi : \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \longrightarrow \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$. Además φ es un isomorfismo. En particular $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$ es isomorfo a $\mathcal{O}_P(V)$.*

Demostración. De la definición de $\mathcal{O}_P(\mathbb{A}^n)$ y la de $\mathcal{O}_P(V)$, tenemos el homomorfismo canónico ψ entre ellos, que está dado por el paso al cociente de $k[X_1, \ldots, X_n]$ en $\Gamma(V)$, la Proposición 1.3.7 nos asegura la existencia del homomorfismo canónico φ, el cual también sabemos que es suprayectivo. Es inyectivo, pues si $fg^{-1} + J\mathcal{O}_P(\mathbb{A}^n) \in Ker(\varphi)$, entonces $\varphi(fg^{-1} + J\mathcal{O}_P(\mathbb{A}^n)) = (f+I/g+I)+J'\mathcal{O}_P(V) \in J'\mathcal{O}_P(V)$, entonces $f+I/g+I \in J'\mathcal{O}_P(\mathbb{A}^n)$, como $J' = J + I \in \Gamma(V)$, entonces $f/g \in J\mathcal{O}_P(\mathbb{A}^n)$. ■

Proposición 1.3.14. *Si $\mathcal{O}$ es un anillo local con ideal maximal $\mathfrak{m}$, existe una sucesión exacta natural de $\mathcal{O}-$módulos*

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

Demostración. Sea $i : \mathfrak{m}^n/\mathfrak{m}^{n+1} \hookrightarrow \mathcal{O}/\mathfrak{m}^{n+1}$ la inclusión. Sea $\varphi : \mathcal{O}/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^n$ definida por $\varphi(x + \mathfrak{m}^{n+1}) = x + \mathfrak{m}^n$, que manda a cada representante de una clase en $\mathcal{O}/\mathfrak{m}^{n+1}$ a su respectiva clase en $\mathcal{O}/\mathfrak{m}^n$, claramente φ es supra, y también i es inyectiva, pues simplemente es la inclusión. Observemos que $Im\, i = Ker\, \varphi$, pues si $x + \mathfrak{m}^{n+1} \in Im\, i$, entonces $x \in \mathfrak{m}^n$, con lo que $\varphi(x + \mathfrak{m}^{n+1}) = 0$ y por lo tanto $Im\, i \subset Ker\, \varphi$. Ahora tomemos $x + \mathfrak{m}^{n+1} \in Ker\, \varphi$, entonces $x \in \mathfrak{m}^n$, y por tanto $x + \mathfrak{m}^{n+1} \in Im\, i$. Por lo tanto tenemos la siguiente sucesión exacta:

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \xrightarrow{i} \mathcal{O}/\mathfrak{m}^{n+1} \xrightarrow{\varphi} \mathcal{O}/\mathfrak{m}^n \longrightarrow 0.$$

■

Proposición 1.3.15. *Sea*

$$0 \longrightarrow V' \xrightarrow{\psi} V \xrightarrow{\varphi} V'' \longrightarrow 0$$

una sucesión exacta de espacios vectoriales de dimensión finita sobre un campo k. Entonces $dim\, V' + dim\, V'' = dim\, V$.

Demostración. Sabemos que $dim\, V = dim\,(Im(\varphi)) + dim\,(Ker(\varphi))$, como φ es suprayectiva, entonces $dim\,(Im(\varphi)) = dim\, V''$, y por la exactitud de la sucesión tenemos que $Ker(\varphi) = Im(\psi)$, por lo tanto $dim\, V = dim\, V'' + dim\,(Im(\psi))$. Notemos que $dim\,(Im(\psi)) = dim\, V' - dim\,(Ker(\psi))$, como ψ es inyectiva, entonces $Ker(\psi) = 0$, luego $dim\,(Im(\psi)) = dim\, V'$. Por lo tanto $dim\, V = dim\, V'' + dim\, V'$. ■

Proposición 1.3.16. *Sea $I = \langle X, Y \rangle \subset k[X, Y]$, entonces*

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

Demostración. La demostración la haremos por inducción. Para $n = 1$ tenemos que $k[X,Y]/I \cong k$, pues cualquier polinomio $f(X,Y) \in k[X,Y]$ lo podemos escribir como $f(X,Y) = f(X,Y) - f(0,0) + f(0,0)$, pero $f(X,Y) - f(0,0) \in I$, y $f(0,0) \in k$. Por lo tanto $k[X,Y]/I \cong k$, pues la función que manda a un polinomio a su término constante resulta ser el isomorfismo, y como $dim_k(k) = 1$, entonces hemos demostrado la base inductiva.

Ahora supongamos que $dim_k(k[X,Y]/I^{n-1}) = 1 + 2 + \ldots + (n-1)$, y tomemos la siguiente sucesión:

$$0 \longrightarrow I^{n-1}/I^n \xrightarrow{i} k[X,Y]/I^n \xrightarrow{\varphi} k[X,Y]/I^{n-1} \longrightarrow 0$$

donde i es la inclusión, y φ es el homomorfismo canónico que toma un representante de una clase en $k[X,Y]/I^n$ y lo manda a su respectiva clase en $k[X,Y]/I^{n-1}$, que está bien

definido dado que $I^n \subset I^{n-1}$. Esta sucesión es exacta, pues claramente la inclusión es inyectiva. Tenemos que φ es suprayectiva, pues si $f + I^{n-1} \in k[X,Y]/I^{n-1}$, entonces $\varphi(f + I^n) = f + I^{n-1}$. Si $f + I^n$ es tal que $\varphi(f + I^n) \in I^{n-1}$, entonces $f \in I^{n-1}$, por lo tanto $f + I^n \in I^{n-1}/I^n$, con lo cual $Im(i) \supset Ker(\varphi)$, y la otra inclusión es evidente.

Observemos que $dim_k(I^{n-1}/I^n) = n$, pues sea A el conjunto de monomios $A = \{X^iY^{n-1-i} \mid i = 0, 1, \ldots, n-1\}$, y A' el conjunto de I^n-clases de A, es decir, $A' = \{X^iY^{n-1-i} + I^n \mid i = 0, 1, \ldots, n-1\}$ que es una base de I^{n-1}/I^n, pues a un polinomio $f(X,Y) \in I^{n-1}$, por tener términos de grado al menos $n-1$, lo podemos pensar como $f(X,Y) = f_{n-1}(X,Y) + f_n(X,Y) + \ldots + f_m(X,Y)$, donde $f_i(X,Y)$ son polinomios homogéneos de grado i, y m es el grado de f; entonces la I^n-clase residual de $f(X,Y)$ es la clase de $f_{n-1}(X,Y)$, y como los elementos de A generan a $f_{n-1}(X,Y)$, y claramente son independientes, entonces A' es una base para I^{n-1}/I^n, y cuya cardinalidad es n.

Por la Proposición 1.3.15 tenemos que

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

lo que concluye el paso inductivo. ∎

Observación 1.3.3. *Sea R un anillo, y k un campo que es subanillo de R. Si M es un ideal de R, entonces M^n/M^{n+1} es un $R-$módulo, y por lo tanto, también es un $k-$módulo.*

La observación anterior justifica la siguiente proposición.

Proposición 1.3.17. *Sea R un Anillo de Valuación Discreta con ideal maximal M, y campo de cocientes K, y supongamos que existe un campo k subanillo de R, tal que la composición $k \to R \to R/M$ es un isomorfismo de k con R/M. Entonces*

(1) $dim_k(R/M^n) = n$ para todo $n > 0$.

(2) $dim_k(M^n/M^{n+1}) = 1$ para toda $n \geq 0$.

(3) Sea $z \in R$, si $\langle z \rangle = M^n$ entonces $ord(z) = n$, y por lo tanto $ord(z) = dim_k(R/\langle z \rangle)$.

Demostración. (1): Para $n = 1$ tenemos que $R/M \cong k$, por lo tanto $dim_k(R/M) = dim_k(k) = 1$.

Sean $t \in M$ un parámetro de uniformización de R, y $z \in R$. Por la Proposición 1.1.6, sabemos que existen únicos $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ y $z_n \in R$, tales que $z = \lambda_0 + \lambda_1 t + \ldots + \lambda_n t^n + z_n t^{n+1}$. Dado que $\lambda_n t^n + z_n t^{n+1} \in M^n$, entonces la clase de z en R/M^n es la clase de $\lambda_0 + \lambda_1 t + \ldots + \lambda_{n-1} t^{n-1}$, que es la suma de las clases de cada uno de los sumandos, pero por ser t parámetro de uniformización, entonces $M^n \subset M$, y cada $\lambda_i t^i$ con $0 \leq i \leq n-1$ no pertenecen a $M^n = \langle t^n \rangle$, por lo que la clase de $\lambda_i t^i$ es distinta de $\lambda_j t^j$ para $i \neq j$. Por

lo tanto $B = \{\overline{1}, \overline{t}, \ldots, \overline{t^{n-1}}\}$ es una base de R/M^n, donde la barra denota la M^n-clase residual. Como hay n elementos en B, entonces $dim_k(R/M^n) = n$.

(2): Por la Proposición 1.3.14, para cada n podemos considerar la sucesión exacta:

$$0 \longrightarrow M^n/M^{n+1} \longrightarrow R/M^{n+1} \longrightarrow R/M^n \longrightarrow 0.$$

Y entonces, de la Proposición 1.3.15, tenemos que

$$dim_k(R/M^{n+1}) = dim_k(R/M^n) + dim_k(M^n/M^{n+1}).$$

De la primera parte de esta demostración, tenemos que

$$dim_k(R/M^{n+1}) = n+1 \text{ y } dim_k(R/M^n) = n,$$

por lo tanto

$$n+1 = n + dim_k(M^n/M^{n+1}),$$

de lo que tenemos que $dim_k(M^n/M^{n+1}) = 1$.

(3): Sea $z \in R$ tal que $\langle z \rangle = M^n$, sea $t \in M$ un parámetro de uniformización, entonces $\langle z \rangle = \langle t^n \rangle = M^n$, por tanto $z = ut^n$, con $u \in R$ unidad, por la definición de $ord(z)$, tenemos que $ord(z) = n$. Por el inciso *(1)* tenemos que $ord(z) = n = dim_k(R/M^n) = dim_k(R/\langle z \rangle)$. ■

Proposición 1.3.18. *Sea V un espacio vectorial, W un subespacio, $T : V \to V$ una aplicación lineal uno a uno tal que $T(W) \subset W$, y supongamos que V/W y $W/T(W)$ son de dimensión finita. Entonces*

i) La aplicación T induce un isomorfismo de V/W en $T(V)/T(W)$.

ii) El cociente $T(V)/W \cap T(V)$ es isomorfo a $W + T(V)/W$, y el cociente $W/W \cap T(V)$ es isomorfo a $W + T(V)/T(V)$.

iii) $dim(V/(W + T(V))) = dim((W \cap T(V))/T(W))$.

iv) Finalmente, $dim(V/T(V)) = dim(W/T(W))$.

Demostración. i) Consideremos el siguiente diagrama

$$\begin{array}{ccccccccc}
0 & \longrightarrow & W & \longrightarrow & V & \longrightarrow & V/W & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} & & \vdots{\scriptstyle \varphi} & & \\
0 & \longrightarrow & T(W) & \longrightarrow & T(V) & \longrightarrow & T(V)/T(W) & \longrightarrow & 0
\end{array}$$

Donde los morfismos horizontales son las inclusiones y el paso al cociente en V/W y en $T(V)/T(W)$. Es claro que el primer cuadrado es conmutativo.

Definimos $\varphi : V/W \longrightarrow T(V)/T(W)$, de la siguiente manera. Sea $v+W \in V/W$, entonces $\varphi(v+W) = T(v)+T(W)$. Veamos que φ está bien definida. Sean $v_1, v_2 \in V$ tales que $v_1+W = v_2+W$, es decir, $v_1-v_2 \in W$, entonces $T(v_1-v_2) \in T(W)$, es decir, $T(v_1) - T(v_2) \in T(W)$, por lo tanto $\varphi(v_1+W) = T(v_1)+T(W) = T(v_2)+T(W) = \varphi(v_2+W)$.

Veamos ahora que φ es inyectiva. Sea $v+W \in V/W$ tal que $\varphi(v+W) = 0$, es decir, tal que $T(v) \in T(W)$. Entonces tenemos que existe $w_0 \in W$ tal que $T(w_0) = T(v)$. Como T es inyectiva, entonces $w_0 = v \in W$. Por lo tanto $v+W = W$, con lo que φ es inyectiva.

Mostremos la suprayectividad de φ. Sea $\overline{v} \in T(V)/T(W)$, entonces $\overline{v} = T(v_0)+T(W)$ para cierta $v_0 \in V$. Es claro entonces que $v_0+W \in V/W$ es tal que $\varphi(v_0+W) = T(v_0)+T(W) = \overline{v}$. Por lo tanto φ es suprayectiva. Con esto tenemos que φ es un isomorfismo, y está inducido por T. Por lo que $V/W \cong T(V)/T(W)$.

ii) Consideremos primero el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W \cap T(V) & \longrightarrow & T(V) & \longrightarrow & T(V)/W \cap T(V) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \vdots\, f & & \\ 0 & \longrightarrow & W & \longrightarrow & W+T(V) & \longrightarrow & W+T(V)/W & \longrightarrow & 0 \end{array}$$

Donde los morfismos están dados por las inclusiones, y por el paso al cociente en $T(V)/(W \cap T(V))$, y en $(W+T(V))/W$.

Sea $\overline{v} \in T(V)/(W \cap T(V))$, definimos f mediante $f(\overline{v}) = \widehat{v}$, donde $\overline{(\ )}$ denota a la clase residual en $T(V)/(W \cap T(V))$, y $\widehat{(\ )}$ denota la clase residual en $(W+T(V))/W$.

Notemos que f está bien definida. Supongamos que $v_1, v_2 \in T(V)$ son tales que $\overline{v_1} = \overline{v_2}$, entonces $v_1 - v_2 \in W \cap T(V)$ y $f(v_1 - v2) \in W$. Como $f(\overline{v_1 - v_2}) = 0$, es decir $\widehat{v_1 - v_2} = 0$, con lo que $\widehat{v_1} = \widehat{v_2}$. Por lo tanto, f está bien definida.

Sea $v \in T(V)$ tal que $\overline{v} \in Ker\ f$, entonces $\widehat{v} = 0$, lo que implica que $v+W \in W+T(V)/W$ es tal que $v \in W$. Como $v \in W$ y $v \in T(V)$, entonces $v \in W \cap T(V)$, y por tanto $\overline{v} = 0$. Con esto tenemos que $Ker\ f = \{0\}$ y concluimos que f es inyectiva.

Sea $v \in W+T(V)$, queremos ahora probar la suprayectividad de f. Tenemos que $v = w_1+v_1$ con $w_1 \in W$ y $v_1 \in T(V)$. Observemos que $\overline{v_1} = v_1+W \cap T(V)$, entonces

$f(\overline{v_1}) = \widehat{v_1}$. Demostrar que $\widehat{v_1} = \widehat{v}$, implica que f es suprayectiva; y esto es claro pues $v - v_1 = w_1 \in W$.

Con esto tenemos que f es una biyección, y entonces hemos probado que $(W + T(V))/W \cong T(V)/(W \cap T(V))$.

Ahora consideremos el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W \cap T(V) & \longrightarrow & W & \longrightarrow & W/W \cap T(V) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \vdots\ g & & \\ 0 & \longrightarrow & T(V) & \longrightarrow & W + T(V) & \longrightarrow & W + T(V)/T(V) & \longrightarrow & 0 \end{array}$$

Podemos definir el morfismo g de una manera análoga a la definición del morfismo f, y los argumentos que utilizamos para ver que f es un isomorfismo nos sirven para ver, de manera análoga, que g es también isomorfismo. Por lo tanto $W/W \cap T(V) \cong W + T(V)/T(V)$.

iii) Del álgebra lineal sabemos que, si $U' \subset W' \subset V'$ son espacios vectoriales, con V'/U' de dimensión finita, entonces $dim(V'/U') = dim(V'/W') + dim(W'/U')$. Del inciso i) tenemos que $V/W \cong T(V)/T(W)$, por tanto $dim(V/W) = dim(T(V)/T(W))$. Como V/W es de dimensión finita, y también se tiene que $W \subset W + T(V) \subset V$, entonces $dim(V/W) = dim(V/(W + T(V))) + dim((W + T(V))/W)$. Análogamente tenemos que $dim(T(V)/T(W)) = dim(T(V)/(W \cap T(V))) + dim((W \cap T(V))/T(W))$. Escribiendo la igualdad se tiene que

$$dim(V/(W + T(V))) + dim((W + T(V))/W) = dim(V/W) =$$

$$= dim(T(V)/T(W)) = dim(T(V)/(W \cap T(V))) + dim((W \cap T(V))/T(W)).$$

Pero del inciso ii) tenemos que $dim(W + T(V)/W) = dim(T(V)/(W \cap T(V)))$, entonces $dim(V/(W + T(V))) = dim((W \cap T(V))/T(W))$.

iv) Dado que $W/T(W)$ es de dimensión finita, entonces, por los incisos ii) y iii) tenemos

$$dim(W/T(W)) = dim(W/(W \cap T(V))) + dim((W \cap T(V))/T(W)) =$$

$$= dim((W + T(V))/T(V)) + dim(V/(W + T(V))) = dim(V/T(V)).$$

Por lo tanto $dim(W/T(W)) = dim(V/T(V))$.

■

Capítulo 2

Intersección de Curvas

2.1. Curvas planas

Definición 2.1.1. Diremos que dos polinomios $F, G \in k[X,Y]$ *están relacionados* si y sólo si $F = \lambda G$ para algún $\lambda \in k$ no nulo.

Proposición 2.1.1. *La relación de la definición de arriba es de equivalencia.*

Demostración. Que la relación es reflexiva es inmediato, pues $1 \in k$ y $F = 1 \cdot F$. La simetría también es inmediata porque, si $F = \lambda G$ con $\lambda \in k$, entonces $G = \lambda^{-1} F$ donde $\lambda^{-1} \in k$ pues $\lambda \neq 0$. Y para la transitividad supongamos que $F = \lambda_1 G$ y $G = \lambda_2 H$ con $F, G, H \in k[X,Y]$ y $\lambda_1, \lambda_2 \in k$ no nulos, entonces sustituyendo tenemos que $F = (\lambda_1 \lambda_2) H$ con lo que $F \sim H$ pues $\lambda_1 \lambda_2 \neq 0$ por ser producto de dos elementos no nulos en un campo. ∎

Definición 2.1.2. Definimos una *curva plana* C como una clase de equivalencia de los polinomios no constantes respecto a la relación definida en la Definición 2.1.1.

Pasaremos por alto la distinción de equivalencia, y diremos simplemente "curva plana". Denotaremos a las curvas planas por un representante de la clase de equivalencia que las define, o simplemente nos referiremos a una curva plana C entendiendo que hay un polinomio que la define.

Definición 2.1.3. El *grado* de una curva plana es el grado de cualquiera de los polinomios que la define.

Notación: Si F es un polinomio irreducible, $V(F)$ es una variedad en $\mathbb{A}^2$ o $\mathbb{P}^2$ dependiendo si el polinomio es o no homogéneo. Normalmente 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 2.1.4. Sea F una curva, $P = (a,b) \in F$. P se denomina *punto simple* de F, si alguna de las derivadas valuada en P es distinta de cero, es decir, si $F_X(P) \neq 0$ o $F_Y(P) \neq 0$.
En este caso, la recta $F_X(P)(X-a) + F_Y(P)(Y-b) = 0$ se denomina *recta tangente* a F en P.

Definición 2.1.5. Un punto que no es simple se denomina *múltiple* (o *singular*).

Definición 2.1.6. Sea F una curva plana que se anula en $P = (0,0)$. Consideremos la descomposición de F como suma de polinomios homogéneos, $F = F_m + F_{m+1} + \ldots + F_n$ con $gr(F_i) = i$, y $F_m \neq 0$; definimos la *multiplicidad* de F en $P = (0,0)$, que denotaremos $m_P(F)$, como $m = min\{gr(F_i)\}$.
Extendemos esta definición a cualquier punto $P = (a,b)$ en la curva, simplemente usando una traslación T que manda $(0,0) \mapsto P$, es decir, $T(x,y) = (x+a, y+b)$, entonces $F^T = F(X+a, Y+b)$. Definimos $m_P(F)$ como $m_{(0,0)}(F^T)$.

Proposición 2.1.2. *Sea F una curva, P es un punto simple de F si y sólo si $m_P(F) = 1$.*

Demostración. Supongamos que P es punto simple de F, entonces $F_X(P) \neq 0$ o $F_Y(P) \neq 0$, por la Definición 2.1.6 es claro que $F_X(P) = F_X^T(0,0)$ y análogamente $F_Y(P) = F_X^T(0,0)$. Sin pérdida de generalidad supongamos que $F_X^T(0,0) = F_X(P) \neq 0$, sean $F = F_m + F_{m+1} + \ldots + F_n$ y $F^T = G_m + G_{m+1} + \ldots + G_n$ las descomposiciones de F y F^T en polinomios homogéneos, entonces $m_P(F) = m_{(0,0)}(F^T) > 0$ pues si $P \in F \Rightarrow (0,0) \in F^T$ entonces $G_i(0,0) = 0$ con $i \geq 1$, puesto que son polinomios homogéneos de grado i, dado que $G_0 = \lambda$ con $\lambda \in k$, siempre se tiene que $G_0(0,0) = \lambda \in k$, pero como queremos que $F^T(0,0) = 0$ entonces $G_0(0,0) = 0$ lo cual lleva a que $m_{(0,0)}(F^T) > 0$. Supongamos que $m_P(F) \geq 2$ entonces $m_{(0,0)}(F^T) \geq 2$, como sabemos que la derivada baja el grado del polinomio entonces $F_X^T = G'_{m-1} + G'_m + \ldots + G'_{n-1}$ es la descomposición de la derivada en polinomios homogéneos, que valuada en $(0,0)$ siempre se anula, pues $gr(G'_i) \geq 1$ para todo i, lo cual contradice que la derivada de F^T respecto a X no se anula en $(0,0)$. Por lo tanto $m_P(F) = 1$, que muestra la primera parte de la proposición.

Supongamos que $m_P(F) = 1$, por la definición de $m_P(F)$ tenemos que $m_{(0,0)}(F^T) = 1$, sea $F^T = (\alpha X + \beta Y) + G_2 + \ldots + G_n$ la descomposición de F^T en polinomios homogéneos, dónde $\alpha, \beta \in k$; sabemos entonces que α y β no son ambas cero al mismo tiempo, sin pérdida de generalidad supongamos que $\alpha \neq 0$, entonces al derivar F^T con respecto a X, aparece como término de grado 0 justamente α, lo cual hace que $F_X^T(0,0) \neq 0$, con lo cual P es un punto simple de F. ∎

Es conveniente introducir una notación que nos será útil para el resto del capítulo:

Notación. Sea F una curva irreducible, para cualquier polinomio $G \in k[X,Y]$, denotamos por g a la clase de equivalencia de G en $\Gamma(F) = k[X,Y]/\langle F\rangle$.

Teorema 2.1.1. *P es un punto simple de F si y sólo si $\mathcal{O}_P(F)$ es un anillo de valuación discreta. En este caso, si $L = aX + bY + c$ es una recta que pasa por P y no es tangente a F en P, entonces la imagen ℓ de L en $\mathcal{O}_P(F)$ es un parámetro de uniformización de $\mathcal{O}_P(F)$.*

Demostración. Supongamos que P es un punto simple de F, y la recta L es una recta que pasa por P, no tangente a F en P. Por medio de un cambio de coordenadas adecuado, gracias a la Proposición 1.2.2 y la Proposición 1.3.4, podemos suponer que $P = (0,0)$, que Y es la recta tangente, y que $L = X$. En virtud de la Proposición 1.1.3, es suficiente probar que $\mathfrak{m}_P(F)$ está generado por x.

Ante todo observemos que las proposiciones 1.3.8 y 1.3.13, nos dicen que $\mathfrak{m}_P(F) = \langle x, y\rangle$, tanto si P es punto simple como si no lo es.

Una vez supuesto lo anterior, sea $F = Y + \textit{términos de grados superiores}$. Agrupando de momento estos términos con Y, podemos escribir $F = YG - X^2H$, donde $G = 1 + \textit{términos superiores}$, $H \in k[X]$. Entonces $yg = x^2h \in \Gamma(F)$, por lo tanto $y = x^2hg^{-1} \in \langle x\rangle$, ya que $g(P) \neq 0$. Por lo tanto $\mathfrak{m}_P(F) = \langle x, y\rangle = \langle x\rangle$, como se pretendía.

El recíproco se demostrará a partir del Teorema 2.1.2. ∎

Si suponemos que P es un punto simple sobre una curva irreducible F, sea ord_P^F la función orden sobre $k(F)$ definida por el anillo de valuación discreta $\mathcal{O}_P(F)$; cuando F esté fijo, podremos escribir simplemente ord_P. Si $G \in k[X_1, \ldots, X_n]$, y g es la imagen de G en $\Gamma(F)$, escribiremos $ord_P^F(G)$ en lugar de $ord_P^F(\mathrm{g})$.

Si P es un punto simple sobre una curva reducible F, escribiremos ord_P^F en vez de $ord_P^{F_i}$, donde F_i es la componente de F que contiene a P.

Supongamos que P es un punto simple de F, y L una recta que pasa por P. Entonces $ord_P^F(L) = 1$ si L no es tangente a F en P y $ord_P^F(L) > 1$ si L es tangente a F en P. Podemos suponer que las condiciones son las mismas que las de la demostración del Teorema 2.1.1; Y es la tangente, $y = x^2hg^{-1}$, y así, $ord_P(y) = ord_P(x^2) + ord_P(hg^{-1}) \geq 2$.

Teorema 2.1.2. *Sea P un punto de una curva irreducible F. Entonces se tiene la igualdad $m_P(F) = dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1})$ para todo n suficientemente grande. En particular, la multiplicidad de F en P depende sólo del anillo local $\mathcal{O}_P(F)$.*

Demostración. Para simplificar un poco la notación, escribamos $\mathcal{O}$, $\mathfrak{m}$ en vez de $\mathcal{O}_P(F)$, $\mathfrak{m}_P(F)$

respectivamente. De la sucesión exacta

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

se sigue que es suficiente probar que $dim_k(\mathcal{O}/\mathfrak{m}^n) = n\, m_P(F)+s$, para una cierta constante s, y para todo $n \geq m_P(F)$ (esto debido a la Proposición 1.3.14 y la Proposición 1.3.15).

Podemos suponer que $P = (0,0)$, por lo tanto $\mathfrak{m}^n = I^n\mathcal{O}$, donde $I = \langle X, Y\rangle \subset k[X,Y]$ (Proposición 1.3.8). Como $V(I^n) = \{P\}$, en virtud del Corolario 1.3.2 y la Proposición 1.3.13, tenemos que $k[X,Y]/\langle I^n, F\rangle \cong \mathcal{O}_P(\mathbb{A}^2)/\langle I^n, F\rangle\mathcal{O}_P(\mathbb{A}^2) \cong \mathcal{O}_P(F)/I^n\mathcal{O}_P(F) = \mathcal{O}/\mathfrak{m}^n$.

Por lo tanto, hemos reducido el problema a simplemente calcular la dimensión de $k[X,Y]/\langle I^n, F\rangle$. Sea $m = m_P(F)$. Entonces $FG \in I^n$ siempre que $G \in I^{n-m}$. Existe un homomorfismo natural $\varphi : k[X,Y]/I^n \longrightarrow k[X,Y]/\langle I^n, F\rangle$, y una aplicación $k-$lineal $\psi : k[X,Y]/I^{n-m} \longrightarrow k[X,Y]/I^n$ definida por $\psi(\overline{G}) = \overline{FG}$, donde las barras indican clases residuales. Es fácil ver que la sucesión

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

es exacta. Aplicando la Proposición 1.3.16 y de nuevo la Proposición 1.3.15, vemos que $dim_k(k[X,Y]/\langle I^n, F\rangle) = nm - \frac{m(m-1)}{2}$ para toda $n \geq m$, como queríamos demostrar. ■

Notemos que si $\mathcal{O}_P(F)$ es un anillo de valuación discreta, debido a la Proposición 1.3.17, el Teorema 2.1.2 implicaría que $m_P(F) = 1$, luego P es simple. Esto completa la demostración del Teorema 2.1.1. Motivados por esto, podemos dar una definición de punto simple, equivalente a la ya vista.

Definición 2.1.7. Un punto $P \in \mathcal{C}$ es *simple* si $\mathcal{O}_P(\mathcal{C})$ es un anillo de valuación discreta.

2.2. Números de Intersección

Por la Observación 1.3.1 de la sección de anillos locales, tenemos las siguientes contenciones:

$$k \subset \Gamma(\mathbb{A}^2) = k[X, Y] \subset \mathcal{O}_P(\mathbb{A}^2) \subset k(\mathbb{A}^2)$$

con lo cual $\mathcal{O}_P(\mathbb{A}^2)$ es una k-álgebra, pues contiene a k; y si $F \in k[X,Y]$ es un polinomio no constante, entonces $k \subset \mathcal{O}_P(\mathbb{A}^2)/\langle F\rangle$, lo cual también convierte a $\mathcal{O}_P(\mathbb{A}^2)/\langle F\rangle$ en una k-álgebra. Esto justifica la siguiente definición:

Definición 2.2.1. Sean F y G curvas planas, y $P \in \mathbb{A}^2$. Definimos el *número de intersección* de F y G en P, que denotaremos por $I_P(F \cap G)$, como:

$$I_P(F \cap G) := dim_k(\mathcal{O}_P(\mathbb{A}^2)/\langle F, G\rangle)$$

Antes de enunciar las propiedades que cumple el número de intersección, es conveniente hacer un par de definiciones respecto a la intersección de dos curvas en un punto:

Definición 2.2.2. Diremos que F y G *se cortan en sentido estricto en* P, si F y G no tienen ninguna componente común que pase por P.

Definición 2.2.3. Dos curvas F y G se *cortan transversalmente* en P, si P es un punto simple tanto de F como de G, y la recta tangente a F en P es distinta de la recta tangente a G en P.

Proposición 2.2.1. *Para todas las curvas planas F, G y todo punto $P \in \mathbb{A}^2$, el número de intersección $I_P(F \cap G)$ de la Definición 2.2.1 es el único número que satisface las siguientes propiedades:*

i) Si F y G se cortan en sentido estricto en P, entonces $I_P(F \cap G)$ es un entero no negativo; en caso contrario $I_P(F \cap G) = \infty$.

ii) $I_P(F \cap G) = 0$ si y sólo si $P \notin F \cap G$. Con lo que $I_P(F \cap G)$ depende sólo de las componentes de F y G que pasan por P.

iii) Si T es un cambio de coordenadas afín de $\mathbb{A}^2$, y $T(Q) = P$, entonces $I_Q(F^T \cap G^T) = I_P(F \cap G)$.

iv) $I_P(F \cap G) = I_P(G \cap F)$.

v) $I_P(F \cap G) \geq m_P(F)m_P(G)$, verificándose la igualdad si y sólo si F y G no poseen rectas tangentes comunes en P.

vi) *Si* $F = \prod F_i^{r_i}$, *y* $G = \prod G_j^{s_j}$, *entonces* $I_P(F \cap G) = \sum_{i,j} r_i s_j I_P(F_i \cap G_j)$.

vii) $I_P(F \cap G) = I_P(F \cap (G + AF))$ *para cualquier* $A \in k[X, Y]$.

Demostración. (Unicidad):

Es suficiente dar un procedimiento constructivo para calcular $I_P(F \cap G)$ utilizando sólo las propiedades *(i)-(vii)*. Gracias a la propiedad *(iii)*, podemos suponer que $P = (0, 0)$, y que $I_P(F \cap G)$ es finito por la propiedad *(i)*. El caso en el que $I_P(F \cap G) = 0$ ya se ha considerado en *(ii)*, por lo tanto podemos proceder por inducción; supongamos que $I_P(F \cap G) = n > 0$ y que $I_P(A \cap B)$ puede ser calculado siempre que $I_P(A \cap B) < n$. Sean $F(X, 0)$, $G(X, 0) \in k[X]$ de grados r, s respectivamente. Por *(iv)* podemos suponer que $r \leq s$.

Caso 1: $r = 0$. Entonces Y divide a F, por lo tanto $F = YH$ y por *(vi)* se tiene que $I_P(F \cap G) = I_P(Y \cap G) + I_P(H \cap G)$. Si $G(X, 0) = X^m(a_0 + a_1 X + \cdots)$, $a_0 \neq 0$, entonces (por *(vii)*, *(ii)*, *(vi)* y *(v)*) $I_P(Y \cap G) = I_P(Y \cap G(X, 0)) = I_P(Y \cap X^m) = m$. Como $P \in G$, $m > 0$, entonces $I_P(H \cap G) < n$, y la demostración por inducción está acabada.

Caso 2: $r > 0$. Podemos multiplicar F y G por constantes que conviertan a $F(X, 0)$ y a $G(X, 0)$ en mónicos. Sea $H = G - X^{s-r}F$. Entonces $I_P(F \cap G) = I_P(F \cap H)$, y $gr(H(X, 0)) = t < s$. Repitiendo este proceso (intercambiando el orden de F y el de H si $t < r$) un número finito de veces, obtenemos eventualmente un par de curvas A, B que caen en el caso 1, y que además verifican $I_P(F \cap G) = I_P(A \cap B)$. Esto acaba la demostración. ■

Demostración. (Existencia):

De la Definición 2.2.1 tenemos que $I_P(F \cap G) = dim_k(\mathcal{O}_P(\mathbb{A}^2)/\langle F, G\rangle)$. Debemos demostrar que satisface las propiedades *(i)-(vii)*. Como $I_P(F \cap G)$ depende sólo del ideal de $\mathcal{O}_P(\mathbb{A}^2)$ generado por F y G, esto dará pie a la demostración de *(ii)*, *(iv)* y *(vii)*.

(ii) Supongamos que $dim_k(\mathcal{O}_P(\mathbb{A}^2)/\langle F, G\rangle) = 0$, entonces $\mathcal{O}_P(\mathbb{A}^2) = \langle F, G\rangle$. Sea pues $\frac{f}{g} \in \mathcal{O}_P(\mathbb{A}^2)$ tal que $\frac{f(P)}{g(P)} \neq 0$, entonces existen $\frac{f_1}{g_1}$, $\frac{f_2}{g_2} \in \mathcal{O}_P(\mathbb{A}^2)$ tales que $\frac{f}{g} = \frac{f_1}{g_1}F + \frac{f_2}{g_2}G$, por lo tanto $\frac{f(P)}{g(P)} = \frac{f_1(P)}{g_1(P)}F(P) + \frac{f_2(P)}{g_2(P)}G(P) \neq 0$, con lo que tenemos que $F(P) \neq 0$ o $G(P) \neq 0$. Con esto tenemos que $P \notin F \cap G$.

Ahora supongamos que $P \notin F \cap G$, entonces $F(P) \neq 0$ o $G(P) \neq 0$. Sin pérdida de generalidad supongamos que $F(P) \neq 0$, entonces $F \notin \mathfrak{m}_P(\mathbb{A}^2)$. Debido a que

$\mathcal{O}_P(\mathbb{A}^2)$ es un anillo local, tenemos que F es una unidad. Por lo tanto, $\mathcal{O}_P(\mathbb{A}^2) = \langle F\rangle \subset \langle F, G\rangle$. Con lo que concluimos que $\mathcal{O}_P(\mathbb{A}^2) = \langle F, G\rangle$.

(iv) Es claro, puesto que $\langle F, G\rangle = \langle G, F\rangle$.

(vii) Queremos ver que $\langle F, G\rangle = \langle F, G + AF\rangle$ para cualquier $A \in k[X, Y]$. Es claro que $\langle F, G + AF\rangle \subset \langle F, G\rangle$. Sea $H \in \langle F, G\rangle$, es decir, $H = \frac{f_1}{g_1}F + \frac{f_2}{g_2}G$, para ciertos $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in \mathcal{O}_P(\mathbb{A}^2)$. Dado que $\frac{f_2}{g_2}AF - \frac{f_2}{g_2}AF = 0$, sea $\frac{f_3}{g_3} = \frac{f_1}{g_1} - \frac{f_2}{g_2}A$, como $g_1(P) \neq 0$, y $g_2(P) \neq 0$, entonces $g_3(P) \neq 0$, por lo que $\frac{f_3}{g_3} \in \mathcal{O}_P(\mathbb{A}^2)$. Observemos que $H = \frac{f_3}{g_3}F + \frac{f_2}{g_2}(G + AF)$, con lo que $H \in \langle F, G + AF\rangle$. Por lo tanto $\langle F, G\rangle = \langle F, G + AF\rangle$.

(iii) Por la Proposición 1.3.4 sabemos que un cambio de coordenadas afines induce un isomorfismo de anillos locales, de donde se concluye *(iii)*.

Con lo hasta ahora probado, podemos suponer que $P = (0, 0)$ y que todas las componentes de F y G pasan por P. En adelante denotaremos simplemente por $\mathcal{O}$ al anillo local $\mathcal{O}_P(\mathbb{A}^2)$.

(i) Si F y G no tienen componentes comunes, $I_P(F \cap G)$ es finito en virtud del Corolario 1.3.1 de la Proposición 1.3.12. Si F y G tienen una componente común H, entonces $\langle F, G\rangle \subset \langle H\rangle$, por lo tanto, como consecuencia de la Proposición 1.3.6, existe un homomorfismo de $\mathcal{O}/\langle F, G\rangle$ sobre $\mathcal{O}/H$, e $I_P(F \cap G) \geq dim_k(\mathcal{O}/\langle H\rangle)$. Pero $\mathcal{O}/\langle H\rangle$ es isomorfo a $\mathcal{O}_P(H)$ por la Proposición 1.3.13, y también tenemos que $\mathcal{O}_P(H) \supset \Gamma(H)$, y $dim_k\Gamma(H) = \infty$ gracias al Nullstellensatz[1], pues si $I \subset k[X_1, \ldots, X_n]$ es un ideal, entonces $V(I)$ es un conjunto finito $\Leftrightarrow$ $k[X_1, \ldots, X_n]/I$ es un $k-$espacio vectorial de dimensión finita, y además, el número de puntos de $V(I)$ es $\leq dim_k(k[X_1, \ldots, X_n]/I)$.

(vi) Para comprobar *(vi)*, es suficiente probar que $I_P(F \cap GH) = I_P(F \cap G) + I_P(F \cap H)$ para toda terna F, G, H. Podemos suponer que F y GH no poseen componentes comunes, ya que, de poseerlas, el resultado sería evidente. Sea $\varphi : \mathcal{O}/\langle F, GH\rangle \longrightarrow \mathcal{O}/\langle F, G\rangle$ el homomorfismo natural de la Proposición 1.3.6, y definamos una aplicación $k-$lineal $\psi : \mathcal{O}/\langle F, H\rangle \longrightarrow \mathcal{O}/\langle F, GH\rangle$ haciendo $\psi(\overline{z}) = \overline{G}\overline{z}$, donde $z \in \mathcal{O}$ y las barras indican las clases residuales. En virtud de la Proposición 1.3.15, es suficiente probar que la sucesión

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

es exacta.

Verificaremos que ψ es inyectiva: Si $\psi(\overline{z}) = 0$, entonces $Gz = uF + vGH$, con $u, v \in \mathcal{O}$.

[1] [4] Fulton W., *Algebraic Curves*, pág. 21.

Elijamos $S \in k[X, Y]$ tal que $S(P) \neq 0$, $Su = A$, $Sv = B$ y $Sz = C \in k[X, Y]$. Entonces $G(C - BH) = AF$ en $k[X, Y]$. Como F y G no tienen factores comunes, F debe dividir a $C - BH$, por lo tanto $C - BH = DF$. Como $Sz = C$ y $C = BH + DF$, entonces $z = (B/S)H + (D/S)F$, por lo tanto $\overline{z} = 0$, con lo que ψ es uno a uno. Sólo falta ver que φ es epiyectiva.

(v) Sean $m = m_P(F)$, $n = m_P(G)$. Sea I el ideal de $k[X, Y]$ generado por X y Y. Consideremos el siguiente diagrama de espacios vectoriales y transformaciones lineales:

$$\begin{array}{ccccccc} k[X,Y]/I^n \times k[X,Y]/I^m & \xrightarrow{\psi} & k[X,Y]/I^{m+n} & \xrightarrow{\varphi} & k[X,Y]/\langle I^{m+n}, F, G\rangle & \longrightarrow & 0 \\ & & & & \downarrow \alpha & & \\ & & \mathcal{O}/\langle F, G\rangle & \xrightarrow{\pi} & \mathcal{O}/\langle I^{m+n}, F, G\rangle & \longrightarrow & 0 \end{array}$$

donde φ, π y α son homomorfismos naturales de anillos, y ψ está definido por $\psi(\overline{A}, \overline{B}) = \overline{AF + BG}$.

Tenemos que φ y π son epiyectivas, pues si $f \in k[X, Y]$, y $[f]_{\langle I^{m+n}\rangle}$, $[f]_{\langle I^{m+n}, F, G\rangle}$ son sus clases residuales en $k[X, Y]/\langle I^{m+n}\rangle$ y $k[X, Y]/\langle I^{m+n}, F, G\rangle$ respectivamente, entonces se tiene que $\varphi([f]_{\langle I^{m+n}\rangle}) = [f]_{\langle I^{m+n}, F, G\rangle}$, con lo cual φ es claramente epiyectivo, y un argumento análogo demuestra que π también es epiyectivo. Y como $V(I^{m+n}, F, G) \subset \{P\}$, α es un isomorfismo en virtud del Corolario 1.3.2.

En el diagrama anterior, el primer renglón es exacto, pues ya vimos que φ es epiyectiva, y de la definición de ψ se tiene que $(\varphi \circ \psi)(\overline{A}, \overline{B}) = \varphi(\psi(\overline{A}, \overline{B})) = \varphi(\overline{AF + BG}) = 0 \in k[X, Y]/\langle I^{m+n}, F, G\rangle$. Esto prueba que

$$dim(k[X,Y]/I^n) + dim(k[X,Y]/I^m) \geq dim(Ker(\varphi)),$$

verificándose el igual si y sólo si ψ es uno a uno, y que

$$dim(k[X,Y]/\langle I^{m+n}, F, G\rangle) = dim(k[X,Y]/I^{m+n}) - dim(Ker(\varphi)).$$

Resumiendo todos estos resultados, obtenemos la siguiente lista de desigualdades:

$I_P(F \cap G) = dim(\mathcal{O}/\langle F, G\rangle) \geq dim(\mathcal{O}/\langle I^{m+n}, F, G\rangle) = dim(k[X,Y]/\langle I^{m+n}, F, G\rangle)$ $\geq dim(k[X,Y]/I^{m+n}) - dim(k[X,Y]/I^n) - dim(k[X,Y]/I^m)$ (por la Proposición 1.3.16).

Todo esto prueba que $I_P(F \cap G) \geq mn$, y que $I_P(F \cap G) = mn$ si y sólo si las dos desigualdades de la lista anterior son igualdades. La primera de dichas desigualdades es una igualdad si π es un isomorfismo, es decir, si $I^{m+n} \subset \langle F, G\rangle\mathcal{O}$. La segunda

es una igualdad si y sólo si ψ es uno a uno. La propiedad *(v)* es, por lo tanto, consecuencia del Lema 2.2.1, que enunciaremos y demostraremos enseguida.

■

Lema 2.2.1. (a) *Si F y G tienen tangentes distintas en P, entonces $I^t \subset \langle F, G\rangle \mathcal{O}$ para $t \geq m+n-1$.*

(b) *ψ es uno a uno si y sólo si F y G poseen tangentes distintas en P.*

Demostración. (a):
Sean $L_1, \ldots, L_m$ las tangentes a F en P, $M_1, \ldots, M_n$ las tangentes a G. Sea $L_i = L_m$ si $i > m$, $M_j = M_n$ si $j > n$, y sea $A_{ij} = L_1 \cdot \ldots \cdot L_i \cdot M_1 \cdot \ldots \cdot M_j$ para todo $i, j \geq 0$ ($A_{00} = 1$). $\{A_{ij} \mid i + j = t\}$ constituye una base del espacio vectorial de todos los polinomios homogéneos de grado t en $k[X, Y]$.
Por lo tanto, para demostrar *(a)*, es suficiente probar que $A_{ij} \in \langle F, G\rangle \mathcal{O}$ para todo $i + j \geq m + n - 1$. Pero $i + j \geq m + n - 1$ implica que $i \geq m$ o $j \geq n$. Si $i \geq m$, es $A_{ij} = A_{m0}B$, donde B es un polinomio homogéneo de grado $t = i + j - m$. $F = A_{m0} + F'$, donde los términos de F' son de grado mayor o igual que $m+1$. Entonces $A_{ij} = BF - BF'$, donde cada uno de los términos de BF' tienen grado mayor o igual que $i + j + 1$. Habremos terminado si podemos probar que $I^t \subset \langle F, G\rangle$ para toda t suficientemente grande. Este hecho es consecuencia del Teorema Nullstellentsatz: sea $V(F, G) = \{P, Q_1, \ldots, Q_s\}$, y elijamos un polinomio H tal que $H(Q_i) = 0$, pero $H(P) \neq 0$ (por la Proposición 1.3.5). $HX, HY \in I(V(F, G))$, por lo tanto $(HX)^N, (HY)^N \in \langle F, G\rangle \subset k[X, Y]$ para un cierto N. H^N es unidad en $\mathcal{O}$, luego $X^N, Y^N \in \langle F, G\rangle \mathcal{O}$ y por lo tanto $I^{2N} \subset \langle F, G\rangle \mathcal{O}$.

Demostración (b):
Supongamos que las tangentes son distintas y que $\psi(\overline{A}, \overline{B}) = \overline{AF + BG} = 0$, es decir, que $AF + BG$ consta exclusivamente de términos de grado mayor o igual a $m+n$. Escribamos $A = A_r +$ *términos de grado superior* y $B = B_s + \ldots$, luego $AF + BG = A_r F_m + B_s G_n + \ldots$. Entonces debe ser $r + m = s + n$ y $A_r F_m = -B_s G_n$. Pero F_m y G_n no tienen factores comunes, luego F_m divide a B_s, y G_n divide a A_r. Por lo tanto, $s \geq m$, $r \geq n$, y en consecuencia $(\overline{A}, \overline{B}) = (0, 0)$.

Recíprocamente, si L fuera una tangente común a F y a G en P, se tendría $F_m = LF'_{m-1}$, $G_n = LG'_{n-1}$. Pero entonces $\psi(G'_{n-1}, -F'_{m-1}) = 0$ y por lo tanto ψ no sería inyectiva. ■

Con el fin de simplificar los cálculos del número de intersección, observemos que se cumplen las siguientes propiedades que nos ayudaran más adelante.

Proposición 2.2.2. *Si P es un punto simple de F, entonces $I_P(F \cap G) = ord_P^F(G)$.*

Demostración. Podemos suponer que F es irreducible. Si g es la imagen de G en $\mathcal{O}_P(F)$, entonces $ord_P^F(G) = dim_k(\mathcal{O}_P(F)/\langle g \rangle)$ (por la tercera parte de la Proposición 1.3.17). Como $\mathcal{O}_P(F)/\langle g \rangle$ es isomorfo a $\mathcal{O}_P(\mathbb{A}^2)/\langle F, G \rangle$ (por la Proposición 1.3.13), esta dimensión es $I_P(F \cap G)$. ■

Proposición 2.2.3. *Si F y G no poseen componentes comunes, entonces*

$$\sum_P I_P(F \cap G) = dim_k(k[X,Y]/\langle F, G \rangle).$$

Demostración. Este resultado es una consecuencia inmediata del Corolario 1.3.1 ■

Para ilustrar cómo calcular el número de intersección hagamos el siguiente ejemplo:

Ejemplo 2.2.1. Calculemos $I_P(E \cap F)$, donde $E = (X^2 + Y^2)^2 + 3X^2Y - Y^3$, $F = (X^2+Y^2)^3 - 4X^2Y^2$, y $P = (0, 0)$. Podemos librarnos de la peor parte de F reemplazando F por $F - (X^2 + Y^2)E$ con lo que tenemos que $F - (X^2 + Y^2)E = Y((X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y) = YG$. Como no disponemos de ningún método obvio para calcular $I_P(E \cap F)$, apliquemos el proceso seguido en la demostración de la unicidad para ahorrarnos los términos en X. Reemplacemos G por $G + 3E = Y(5X^2 - 3Y^2 + 4Y^3 + 4X^2Y) = YH$. Entonces $I_P(E \cap F) = 2I_P(E \cap Y) + I_P(E \cap H)$. Pero $I_P(E \cap Y) = I_P(X^4 \cap Y) = 4$ (por las propiedades *(vii)* y *(vi)* del número de intersección), y $I_P(E \cap H) = m_P(E)m_P(H) = 6$ (por la propiedad *(v)*). Por lo tanto $I_P(E \cap F) = 14$.

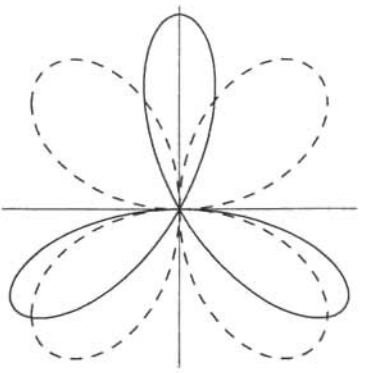


Figura 2.1: Gráfica de la curva E y en puntcado la curva F

2.3. Curvas Proyectivas Planas

Se puede extender el concepto de curva afín que aprendimos en la sección 2.1, a curvas proyectivas planas, simplemente tomando polinomios homogéneos en $k[X,Y,Z]$, en lugar de cualquier polinomio en $k[X,Y]$, pero haciendo la misma relación de equivalencia.

Una curva proyectiva plana es una hipersuperficie de $\mathbb{P}^2$, excepto que, como en el caso de las curvas afines, queremos admitir componentes múltiples.

Definición 2.3.1. Decimos que dos polinomios homogéneos $F, G \in k[X,Y,Z]$ son equivalentes si existe un $\lambda \in k$ no nulo, tal que $G = \lambda F$.

Proposición 2.3.1. *La relación arriba definida es de equivalencia.*

Demostración. La demostración es la misma que la de la Proposición 2.1.1, sólo hay que recalcar que multiplicar un polinomio por una constante λ no altera el grado ni la homogeneidad del polinomio. ■

Definición 2.3.2. Una *curva proyectiva* plana es una clase de equivalencia de polinomios homogéneos.

Definición 2.3.3. Definimos el *grado* de una curva, como el grado de uno de los polinomios homogéneos que la define.

Las notaciones y convenios de la Sección 2.1, referentes a las curvas afines se trasladan a las curvas proyectivas: de este modo se habla de componentes simples y múltiples, y se escribe $\mathcal{O}_P(F)$ en lugar de $\mathcal{O}_P(V(F))$ para un F irreducible, etcétera.

Definición 2.3.4. Un ideal $I \subset k[X_1, \ldots, X_{n+1}]$ se llama *homogéneo* si para todo $F \in I$, lo descomponemos como $F = \sum_{i=0}^{m} F_i$ donde las F_i son polinomios homogéneos de grado i, entonces tenemos que también $F_i \in I$.

Definición 2.3.5. Sea V una variedad proyectiva irreducible de $\mathbb{P}^n$, entonces $I(V)$ es un ideal primo, por lo tanto definimos el *anillo de coordenadas homogéneas* de V, que denotamos por $\Gamma_{hom}(V)$, como la anillo residual $\Gamma_{hom}(V) = k[X_1, \ldots, X_{n+1}]/I(V)$; este anillo por tanto es dominio entero.

Sea F un polinomio homogéneo en $k[X,Y,Z]$, denotamos con F_* a la deshomogeneización de F en la última coordenada, es decir, $F_*(X,Y) = F(X,Y,1)$. Observemos que estamos tomando la parte afín de F.

Podemos considerar a $\mathbb{A}^n$ como un subconjunto de $\mathbb{P}^n$ por medio de la aplicación $\varphi_{n+1} : \mathbb{A}^n \to U_{n+1} \subset \mathbb{P}^n$, donde $U_{n+1} = \{(x1, \ldots, x_{n+1}) \in \mathbb{P}^n \mid x_{n+1} \neq 0\}$, y entonces definimos φ de la haciendo $\varphi_{n+1}(a_1, \ldots, a_n) = (a_1, \ldots, a_n, 1)$.

Ahora tomemos V un conjunto algebraico de $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n]$. Sea I^* el ideal de $k[X_1, \ldots, X_{n+1}]$ generado por $\{F^* \mid F \in I\}$ dónde F^* es la homogeneización de F. I^* es un ideal homogéneo, y definimos V^* como $V(I^*) \subset \mathbb{P}^n$. A dicha V^* construida a partir de $V \subset \mathbb{A}^n$ se le denomina la *clausura proyectiva* de V.

Definición 2.3.6. Definimos el isomorfismo natural $\alpha : k(V^*) \to k(V)$ de la siguiente manera: $\alpha(f/g) = f_*/g_*$ donde f, g son polinomios homogéneos del mismo grado en $\Gamma_{hom}(V^*)$. Si $P \in V$, podemos considerar que $P \in V^*$ por medio de φ_{n+1}, y entonces α induce un isomorfismo de $\mathcal{O}_P(V^*)$ en $\mathcal{O}_P(V)$. Ordinariamente utilizaremos α para identificar $k(V)$ con $k(V^*)$, y $\mathcal{O}_P(V)$ con $\mathcal{O}_P(V^*)$.

Observemos que si $P = (x, y, 1)$, entonces $\mathcal{O}_P(F)$ es canónicamente isomorfo a $\mathcal{O}_{(x,y)}(F_*)$, donde F_* es la curva afín correspondiente.

Los resultados de las secciones anteriores de éste capítulo nos aseguran que la multiplicidad de un punto de una curva afín depende sólo del anillo local de la curva en dicho punto, por lo que podemos hacer la siguiente definición.

Definición 2.3.7. Si F es una curva proyectiva plana, $P \in U_i$ (i= 1, 2 ó 3), podemos deshomogeneizar F respecto a X_i, y definir la *multiplicidad* $m_P(F)$ de F en P, por $m_P(F_*)$.

Gracias al Teorema 2.1.2 tenemos que la multiplicidad es independiente de la elección de U_i, e invariante frente a cambios de coordenadas proyectivas.

La siguiente notación nos será útil. Si consideramos un conjunto finito de puntos $P_1, \ldots, P_n \in \mathbb{P}^2$, podemos encontrar siempre una recta L que no pase por ninguno de ellos. Si F es una curva de grado d, sea $F_* = F/L^d \in k(\mathbb{P}^2)$. Vemos que F_* depende de la elección de L, pero si L' fuera otra elección, entonces $F/L'^d = (L/L')^d F_*$, pero L/L' es una unidad en cada $\mathcal{O}_{P_i}(\mathbb{P}^2)$.

De la geometría proyectiva sabemos que siempre es posible encontrar un cambio de coordenadas proyectivo, tal que la recta L se transforme en la recta Z del infinito; entonces, por la identificación natural de $k(\mathbb{A}^2)$ con $k(\mathbb{P}^2)$ dada en la Definición 2.3.6, esta F_* es la misma que la anterior $F_* = F(X, Y, 1)$.

Si P es un punto simple de F, es decir, $m_P(F) = 1$, y F es irreducible, entonces $\mathcal{O}_P(F)$ es un Anillo de Valuación Discreta. Con ord_P^F designaremos la correspondiente función de orden sobre $k(F)$. Si G es un polinomio homogéneo de $k[X, Y, Z]$, $G_* \in \mathcal{O}_P(\mathbb{P}^2)$, denotamos por $\overline{G}_*$ a la clase residual de G en $\mathcal{O}_P(F)$, definimos $ord_P^F(G)$ por $ord_P^F(\overline{G}_*)$.

Sean F, G curvas proyectivas planas, $P \in \mathbb{P}^2$. Definimos $I_P(F \cap G)$, como antes, por $dim_k(\mathcal{O}_P(\mathbb{P}^2)/\langle F_*, G_* \rangle)$. Este número es independiente del camino seguido para formar F_* y G_*, y satisface las propiedades vistas en las Proposiciones 2.2.1, 2.2.2 y 2.2.3, pero haciendo ver que en la propiedad *(iii)*, T será un cambio de coordenadas proyectivo, y en *(vii)*, A será un polinomio homogéneo con $gr(A) = gr(G) - gr(F)$.

Definición 2.3.8. Decimos que la recta L es *tangente* a la curva F en P, si $I_P(F \cap L) > m_P(F)$. Y decimos que P es un *punto múltiple ordinario* de F, si F tiene $m_P(F)$ tangentes distintas en P.

Lema 2.3.1 (Teorema de Euler[2]). *Si F es un polinomio homogéneo de grado m en $k[X_1, \ldots, X_n]$. Entonces*

$$mF = \sum_{i=1}^{n} X_i F_{X_i}.$$

Proposición 2.3.2. *Sea F una curva irreducible de $\mathbb{P}^2$. Supongamos que $I_P(F \cap Z) = 1$, y $P \neq (1,0,0)$, entonces $F_X(P) \neq 0$.*

Demostración. Sea $F \in k[X,Y,Z]$ un polinomio homogéneo de grado m, tal que $I_P(F \cap Z) = 1$. Sea $P \in \mathbb{P}^2$ tal que $P = (a,b,c) \neq (1,0,0)$. Por el Lema 2.3.1 tenemos que

$$mF = XF_X + YF_Y + ZF_Z \tag{2.1}$$

y sabemos que la recta tangente a F en P tiene la siguiente ecuación

$$XF_X(P) + YF_Y(P) + ZF_Z(P) = 0. \tag{2.2}$$

Como $I_P(F \cap Z) = 1$, entonces $P \in F \cap Z$, además F y Z se cortan en sentido estricto, por lo que Z no puede ser tangente a F en P.

Que $P \in F$, implica que $F(P) = 0$, y al evaluarla la Ecuación 2.1 en P se obtiene:

$$aF_X(P) + bF_Y(P) + cF_Z(P) = 0. \tag{2.3}$$

Como $P \in Z$, entonces $P = (a,b,0)$ y en la Ecuación 2.3 se tiene simplemente

$$aF_X(P) + bF_Y(P) = 0. \tag{2.4}$$

Dado que $P \neq (1,0,0)$, se tiene entonces que $b \neq 0$. Por lo tanto, de la Ecuación 2.4 obtenemos

$$F_Y(P) = \frac{-a}{b} F_X(P). \tag{2.5}$$

Supongamos que $F_X(P) = 0$, entonces por la Ecuación 2.5 tenemos que $F_Y(P) = 0$. Por ser P un punto no singular de F, esto último implica que $F_Z(P) \neq 0$, con lo que la Ecuación 2.2 quedaría simplemente

$$ZF_Z(P) = 0.$$

Lo cual implica que, o bien Z es la recta tangente a F en P, lo que contradice el hecho de que Z y F se corten en sentido estricto; o bien, que $F_Z(P) = 0$, lo que contradice el hecho de que P es un punto no singular de F. Por lo tanto, $F_X(P) \neq 0$. ■

[2] [4] Fulton W., *Algebraic Curves*, pág. 6.

Definición 2.3.9. Dos curvas F y G se dice que son *proyectivamente equivalentes* si existe un cambio de coordenadas proyectivo T tal que $G = F^T$. Todo lo que se diga acerca de curvas será lo mismo para dos curvas proyectivamente equivalentes.

Ahora deseamos estudiar todas las curvas de un cierto grado $d \geq 1$.

Definición 2.3.10. Un conjunto $V \subset \mathbb{P}^n$ se denomina *subvariedad lineal* de $\mathbb{P}^n$ si $V = V(H_1, \ldots, H_r)$, donde cada H_i es un polinomio homogéneo de grado 1.

Lema 2.3.2. *El número de monomios de grado d en $R[X,Y,Z]$, para cualquier anillo R son $1 + 2 + \ldots + (d+1) = \frac{(d+1)(d+2)}{2}$.*

Demostración. Queremos contar de cuántas maneras podemos escoger enteros positivos $0 \leq \alpha, \beta, \gamma \leq d$, de tal manera que $\alpha + \beta + \gamma = d$, pues un monomio en $R[X,Y,Z]$ sería de la forma $X^\alpha Y^\beta Z^\gamma$. La condición $\alpha + \beta + \gamma = d$ puede traducirse a $\alpha + \beta = d - \gamma$ con $\gamma = 0, 1, \ldots, d$. En el caso $\gamma = 0$, queremos encontrar dos enteros positivos tales que $\alpha + \beta = d - 0 = d$, como α y β pueden variar entre 0 y d, si variamos α, entonces β queda determinada por $\beta = d - \alpha$, y por tanto tenemos $d+1$ posibilidades de escoger α y β para que $\alpha + \beta = d$. Ahora tomamos $\gamma = 1$, entonces nuestro problema se reduce a contar, de cuántas maneras podemos tomar dos enteros positivos $0 \leq \alpha, \beta \leq d - 1$ tales que $\alpha + \beta = d - 1$, de nuevo, al variar α, tenemos que β queda determinada por $\beta = d - 1 - \alpha$, con lo que tenemos d maneras de tomar dichos α y β. Continuando este proceso inductivamente, hasta el caso en que $\gamma = d$, entonces buscamos dos enteros positivos α y β tales que $\alpha + \beta = 0$, lo cual nos obliga a que $\alpha = 0 = \beta$, es decir, sólo tenemos una manera de elegir α y β, tales que $\alpha + \beta = 0$. Por lo tanto, el número de monomios de grado d que hay en $R[X,Y,Z]$ son: $1 + 2 + \ldots + (d+1) = \frac{(d+1)(d+2)}{2}$. ∎

Sean $M_1, \ldots, M_N$ una ordenación prefijada del conjunto de monomios en X, Y, Z de grado d, donde $N = \frac{(d+1)(d+2)}{2}$. Dada una curva F de grado d es siempre posible escoger $a_1, \ldots, a_N \in k$, no todos nulos, y escribir $F = \sum a_i M_i$, haciendo la salvedad de que $(a_1, \ldots, a_N)$ y $(\lambda a_1, \ldots, \lambda a_N)$ determinan la misma curva. En otras palabras, a cada curva F de grado d le corresponde un punto único de $\mathbb{P}^{N-1} = \mathbb{P}^{\frac{1}{2}d(d+3)}$, y cada punto de $\mathbb{P}^{\frac{1}{2}d(d+3)}$ representa una curva única. Por ejemplo, si $d = 2$, la cónica $aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2$ corresponde a $(a,b,c,d,e,f) \in \mathbb{P}^5$; si $d = 1$, a cada recta $aX + bY + cZ$ le corresponde el punto $(a,b,c) \in \mathbb{P}^2$, entonces las rectas de $\mathbb{P}^2$ constituyen un $\mathbb{P}^2$.

Lema 2.3.3. *Sea $P \in \mathbb{P}^2$ un punto fijo. Entonces el conjunto de curvas de grado d que contienen a P, forman un hiperplano de $\mathbb{P}^{\frac{1}{2}d(d+3)}$.*

Demostración. Si $P = (x, y, z)$, entonces la curva correspondiente a $(a_1, \ldots, a_N) \in \mathbb{P}^{\frac{1}{2}(d+3)d}$ pasa por P si y sólo si $\sum a_i M_i(x, y, z) = 0$. Como no todos los $M_i(x, y, z) = 0$, entonces los $(a_1, \ldots, a_N)$ constituyen un hiperplano. ■

Lema 2.3.4. *Si $T : \mathbb{P}^2 \to \mathbb{P}^2$ es un cambio de coordenadas proyectivo, entonces la aplicación $F \mapsto F^T$ del conjunto {curvas de grado d} en el conjunto {curvas de grado d} es un cambio de coordenadas proyectivo de $\mathbb{P}^{\frac{1}{2}d(d+3)}$.*

Demostración. La demostración de que $F \to F^T$ es lineal, es la misma que la del lema anterior; y sabemos que es invertible, ya que $F \to F^{T^{-1}}$ es su inversa. ■

Esto prueba que para todo conjunto de puntos, las curvas de grado d que los contienen forman una subvariedad lineal de $\mathbb{P}^{\frac{1}{2}d(d+3)}$. Como la intersección de n hiperplanos de $\mathbb{P}^n$ no es vacía, existe una curva de grado d que pasa por $\frac{1}{2}d(d+3)$ puntos dados.

Supongamos ahora que fijamos un punto P y un entero $r \leq d+1$. Afirmamos que las curvas F de grado d tales que $m_P(F) \geq r$ forman una subvariedad lineal de dimensión $\frac{d(d+3)}{2} - \frac{r(r+1)}{2}$. Por el Lema 2.3.4, podemos suponer $P = (0, 0, 1)$. Representamos F como suma, $F = \sum F_i(X, Y)Z^{d-i}$, donde F_i es un polinomio homogéneo de grado i. Entonces $m_P(F) \geq r$ si y sólo si $F_0 = F_1 = \ldots = F_{r-1} = 0$, es decir, los coeficientes de todos los monomios $X^iY^jZ^k$ con $i + j < r$, son ceros. Y hay $1 + 2 + \ldots + r = \frac{r(r+1)}{2}$ de tales coeficientes.

Definición 2.3.11. Sean $P_1, \ldots, P_n \in \mathbb{P}^2$, y $r_1, \ldots, r_n$ enteros no negativos. Indicamos con $V_d(r_1P_1, \ldots, r_nP_n) = \{\text{curvas } F \text{ de grado } d \text{ tales que } m_{P_i}(F) \geq r_i,\ i = 1, \ldots, n\}$

Teorema 2.3.1. (1): *$V_d(r_1P_1, \ldots, r_nP_n)$ es un subespacio lineal de $\mathbb{P}^{\frac{1}{2}d(d+3)}$ de dimensión $\geq \frac{d(d+3)}{2} - \sum \frac{r_i(r_i+1)}{2}$.*

(2): *Si $d \geq (\sum r_i) - 1$, entonces $\dim V_d(r_1P_1, \ldots, r_nP_n) = \frac{d(d+3)}{2} - \sum \frac{r_i(r_i+1)}{2}$.*

Demostración. La afirmación (1) se sigue de la discusión anterior. Podemos probar (2) por inducción respecto de $m = (\sum r_i) - 1$. Podemos suponer que $m > 1$ y $d > 1$, ya que en otro caso es trivial.

Caso 1: Cada $r_i = 1$. Sea $V_i = V_d(P_1, \ldots, P_i)$. Es suficiente probar por inducción que $V_n \neq V_{n-1}$. Escojamos rectas L_i que pasen por P_i pero no por P_j, $j \neq i$, y una L_0 que no pase por ningún P_i. Entonces $F = L_1 \cdot \ldots \cdot L_{n-1}L_0^{d-n+1} \in V_{n-1}$, pero $F \notin V_n$.

Caso 2: Algún $r_i > 1$. Llamemos $r = r_1 > 1$, y $P = P_1 = (0, 0, 1)$. Sea $V_0 = V_d((r-1)P, r_2P_2, \ldots, r_nP_n)$. Para $F \in V_0$ sea $F_* = \sum_{i=0}^{r-1} a_iX^iY^{r-1-i} + \textit{términos de grado}$

superiores. Sea $V_i = \{F \in V_0 \mid a_j = 0 \text{ para } j < i\}$. Entonces tenemos $V_0 \supset V_1 \supset \ldots \supset V_r = V_d(r_1P_1, r_2P_2, \ldots, r_nP_n)$, por lo tanto bastará probar que $V_i \neq V_{i+1}$, $i = 0, \ldots, r-1$.

Sea $W_0 = V_{d-1}((r-2)P, r_2P_2, \ldots, r_nP_n)$; para $F \in W_0$, sea $F_* = a_iX^iY^{r-2-i} + \cdots$; Sea $W_i = \{F \in W_0 \mid a_j = 0 \text{ para } j < i\}$. Por inducción $W_0 \supsetneq W_1 \supsetneq W_2 \supsetneq \cdots \supsetneq W_{r-1} = V_{d-1}((r-1)P, r_2P_2, \ldots, r_nP_n)$. Si $F_i \in W_i$, entonces $F_i \notin W_{i+1}$, y entonces $YF_i \in V_i$, con $YF_i \notin V_{i+1}$, y $XF_{r-2} \in V_{r-1}$, $XF_{r-2} \notin V_r$. Luego $V_i \neq V_{i+1}$ para $i = 0, \ldots, r-1$, lo que acaba la demostración. ■

2.4. Teorema fundamental de Max Noether

Definición 2.4.1. Un *cero-ciclo* de $\mathbb{P}^2$, es un elemento del grupo abeliano libre sobre el conjunto de puntos de $\mathbb{P}^2$, es decir, es una suma formal $\sum_{P\in\mathbb{P}^2} n_P P$, donde los n_P son enteros, todos cero salvo un número finito.

Definiendo así a los cero-ciclos, es natural entonces dar las siguientes definiciones.

Definición 2.4.2. Definimos el *grado* del cero-ciclo $\sum n_P P$ como la suma de sus coeficientes: $\sum n_P$.

Definición 2.4.3. Decimos que el cero-ciclo $\sum n_P P$ es *mayor que* el cero-ciclo $\sum m_P P$, y lo denotaremos $\sum n_P P \succ \sum m_P P$, si cada $n_P \geq m_P$.

Ahora, utilizaremos los conceptos vistos en la sección anterior para definir el ciclo intersección.

Definición 2.4.4. Sean F y G dos curvas proyectivas planas de grados m y n respectivamente, y sin componentes comunes. Definimos el *ciclo intersección* por

$$F \cdot G = \sum_{P\in\mathbb{P}^2} I_P(F \cap G)P.$$

El Teorema de Bézout[3] nos asegura que $F \cdot G$ es un cero-ciclo positivo de grado mn.

Varias propiedades de los números de intersección se traducen expresivamente a propiedades de los ciclos intersección. Por ejemplo: $F \cdot G = G \cdot F$; $F \cdot GH = F \cdot G + F \cdot H$, y $F \cdot (G + AF) = F \cdot G$ si A es un polinomio homogéneo de grado $gr(A) = gr(G) - gr(F)$.

El Teorema de Max Noether se ocupa del siguiente problema: supongamos que F, G y H son curvas, y $H \cdot F \succ G \cdot F$, es decir, H corta a F en un ciclo mayor que el ciclo en que G corta a F. ¿Cuándo existe una curva B tal que $B \cdot F = H \cdot F - G \cdot F$? Observemos que se necesita $gr(B) = gr(H) - gr(G)$.

Para encontrar una curva B, bastaría con encontrar polinomios homogéneos A y B tales que $H = AF + BG$, con lo que se tendría que $H \cdot F = BG \cdot F = B \cdot F + G \cdot F$.

Definición 2.4.5. Sean $P \in \mathbb{P}^2$, F y G curvas sin componentes comunes que pasen por P, y H otra curva. Diremos que *se satisfacen las condiciones de Noether en* P (respecto de F, G y H), si $H_* \in \langle F_*, G_* \rangle \subset \mathcal{O}_P(\mathbb{P}^2)$, es decir, si existen $a, b \in \mathcal{O}_P(\mathbb{P}^2)$ tales que $H_* = aF_* + bG_*$.

[3] [13] Silverman P., *Rational Points on Elliptic Curves*, Apéndice 4, pág. 242–251.

Proposición 2.4.1. *Sean F, G, H curvas planas, $P \in F \cap G$. Las condiciones de Noether se verifican en P si una de las siguientes afirmaciones es cierta:*

(1) *F y G se cortan transversalmente en P, y $P \in H$.*

(2) *P es un punto simple de F, y $I_P(H \cap F) \geq I_P(F \cap G)$.*

(3) *F y G poseen tangentes distintas en P, y $m_P(H) \geq m_P(F) + m_P(G) - 1$.*

Demostración. (2): $I_P(H \cap F) \geq I_P(F \cap G)$ implica que $ord_P^F(H) \geq ord_P^F(G)$, por lo tanto $\overline{H}_* \in \langle \overline{G}_* \rangle \subset \mathcal{O}_P(F)$. Como $\mathcal{O}_P(F)/\langle \overline{G}_* \rangle \cong \mathcal{O}_P(\mathbb{P}^2)/\langle F_*, G_* \rangle$ (gracias a la Proposición 1.3.13), la clase residual de H_* en $\mathcal{O}_P(\mathbb{P}^2)/\langle F_*, G_* \rangle$ es cero, como queríamos.

(3): Supongamos que $P = (0,0,1)$, y $m_P(H_*) \geq m_P(F_*) + m_P(G_*) - 1$. Usando el Lema 2.2.1 con su notación, tenemos que $H_* \in I^t$, $t \geq m+n-1$. Y en dicho lema probamos precisamente que $I^t \subset \langle F_*, G_* \rangle \subset \mathcal{O}_P(\mathbb{P}^2)$ si $t \geq m_P(F) + m_P(G) - 1$.

(1): Es un caso particular de (2) y (3). ∎

Lema 2.4.1. *Sean F, G, H curvas proyectivas planas; F y G sin componentes comunes. Sea $\Gamma = k[X,Y,Z]/\langle F, G \rangle$. La aplicación $\alpha : \Gamma \to \Gamma$ definida por $\alpha(\overline{H}) = \overline{ZH}$ (donde las barras designan las clases módulo $\langle F, G \rangle$) es uno a uno.*

Demostración. Tenemos que probar que si $ZH = AF + BG$, entonces $H = A'F + B'G$ para ciertos A', B'. Para todo $J \in k[X,Y,Z]$, designemos temporalmente a $J(X,Y,0)$ simplemente por J_0. Como F, G y Z no tienen ceros comunes, entonces F_0 y G_0 son primos relativos en $k[X,Y]$.

Si $ZH = AF + BG$, entonces $(ZH)_0 = 0 = (AF + BG)_0 = A_0F_0 + B_0G_0$, de donde $A_0F_0 = -B_0G_0$, y por lo tanto $B_0 = F_0C$ y $A_0 = G_0C$ para un cierto $C \in k[X,Y]$. Sean $A_1 = A + CG$, $B_1 = B - CF$. Como $(A_1)_0 = (B_1)_0 = 0$, tendremos que $A_1 = ZA'$ y $B_1 = ZB'$ para ciertos A', B'. Como $ZH = A_1F + B_1G$, hemos probado entonces que $H = A'F + B'G$. ∎

Ahora estamos provistos de herramientas para enunciar y probar el teorema de Noether, que relaciona las condiciones locales y las globales.

Teorema 2.4.1 (Fundamental de Max Noether). *Sean F, G, H curvas proyectivas planas. Se supone que F y G no tienen componentes comunes. Existe una ecuación $H = AF + BG$ (con A, B polinomios homogéneos de grados $gr(A) = gr(H) - gr(F)$ y $gr(B) = gr(H) - gr(G)$ respectivamente) si y sólo si las condiciones de Noether se satisfacen en cada punto $P \in F \cap G$.*

Demostración. Si $H = AF + BG$, entonces $H_* = A_*F_* + B_*G_*$ en todo P. Para probar el recíproco, podemos suponer, mediante un cambio de coordenadas proyectivo, si es necesario, que $V(F, G, Z) = \varnothing$. Las condiciones de Noether dicen que la clase residual de H_* en $\mathcal{O}_P(\mathbb{P}^2)/\langle G_*, F_*\rangle$ es cero en todo $P \in F \cap G$. Esto prueba, en virtud de la Proposición 1.3.12, que la clase residual H_* es cero en $k[X,Y]/\langle F_*, G_*\rangle$, es decir, $H_* = aF_* + bG_*$, con $a, b \in k[X,Y]$. Entonces al homogeneizar tenemos $Z^r H = AF + BG$ para ciertos A, B, r. Pero en el Lema 2.4.1 hemos visto que la multiplicación por Z es una aplicación uno a uno en $k[X,Y,Z]/\langle F, G\rangle$, por lo tanto $H = A'F + B'G$ para ciertos A', B'. Si $A' = \sum A'_i$, y $B' = \sum B'_i$, con A'_i, B'_i polinomios homogéneos de grado i, entonces $H = A'_s F + B'_t G$, $s = gr(H) - gr(F)$, $t = gr(H) - gr(G)$. ∎

Corolario 2.4.1. *Si se cumple alguna de las siguientes condiciones*

i) F y G se cortan en un número de puntos distintos igual a $gr(F) \cdot gr(G)$, y H pasa por estos puntos.

ii) Todos los puntos de $F \cap G$ son puntos simples de F, y $H \cdot F \succ G \cdot F$,

Entonces existe una curva B tal que $B \cdot F = H \cdot F - G \cdot F$.

Ahora veremos algunas consecuencias interesantes del Teorema de Max Noether. Como no nos serán necesarias en capítulos posteriores, las demostraciones serán breves.

Proposición 2.4.2. *Sean C, C' cúbicas, $C' \cdot C = \sum_{i=1}^{9} P_i$; supongamos que Q es una cónica, y que $Q \cdot C = \sum_{i=1}^{6} P_i$. Si $P_1, \ldots, P_6$ son puntos simples de C, entonces P_7, P_8, P_9 están alineados.*

Demostración. Se consideran $F = C$, $G = Q$, $H = C'$ en el Corolario 2.4.1. ∎

Corolario 2.4.2. (Pascal): *Si un hexágono está inscrito en una cónica irreducible, entonces los lados opuestos se cortan en puntos colineales.*

Demostración. Sean C tres lados, C' los tres lados opuestos. Q la cónica, y aplíquese la Proposición 2.4.2. ∎

Corolario 2.4.3. (Pappus): *Sean L_1, L_2 dos rectas; P_1, P_2, $P_3 \in L_1$, Q_1, Q_2, $Q_3 \in L_2$ (ninguno de estos puntos se encuentra sobre $L_1 \cap L_2$). Sea L_{ij} la recta que une P_i y Q_j. Para cada i, j, k con $\{i,j,k\} = \{1,2,3\}$, sea $R_k = L_{ij} \cdot L_{ji}$. Entonces R_1, R_2 y R_3 están alineados.*

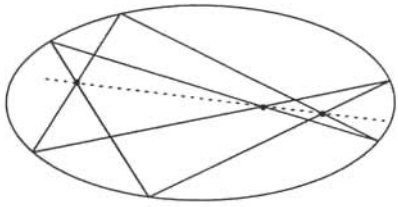


Figura 2.2: Teorema de Pascal

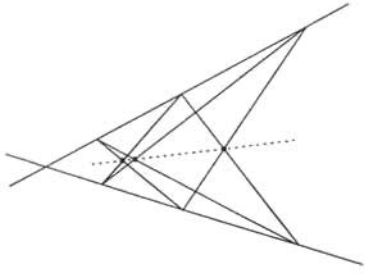


Figura 2.3: Teorema de Pappus

Demostración. Las dos rectas forman una cónica, y la demostración es idéntica a la del Corolario 2.4.2. ■

Capítulo 3

Modelos no singulares

3.1. Aplicaciones racionales

Definición 3.1.1. Sea V un conjunto algebraico irreducible de $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. Todo subconjunto abierto X de V se denomina *variedad*. X posee la topología de Zariski inducida por V.

Si U es un subconjunto abierto de X, entonces U es también abierto en V, por lo tanto U es también una variedad. Diremos que U es una *subvariedad abierta* de X.

Definición 3.1.2. Si Y es un subconjunto cerrado de X, diremos que Y es *irreducible* si Y no es unión de dos subconjuntos propios cerrados.

Una Y como la definida se denomina simplemente *subvariedad cerrada* de X.

Lema 3.1.1. *Sean cualesquiera subconjuntos abiertos U_1, U_2 no vacíos de una variedad V, entonces $U_1 \cap U_2 \neq \varnothing$.*

Demostración. Supongamos que $U_1 \cap U_2 = \varnothing$, entonces los cerrados $V - U_1$ y $V - U_2$ forman una descomposición de V en unión de dos subconjuntos propios cerrados, es decir, $(V - U_1) \cup (V - U_2) = V - (U_1 \cap U_2) = V$ lo cual contradice que V es irreducible. ■

Lema 3.1.2. *Todo subconjunto abierto no vacío U de una variedad V, es denso en V.*

Demostración. Sea $\overline{U}$ la cerradura topológica de U, es decir

$$\overline{U} = \bigcap_{U \subset W_\lambda} W_\lambda$$

donde los W_λ son subconjuntos cerrados de V. Entonces el abierto $V - \overline{U}$ no interseca a U, pero por el Lema 3.1.1, la intersección es no vacía, por lo que no puede haber dicho abierto $V - \overline{U}$, entonces $V - \overline{U} = \varnothing \Rightarrow \overline{U} = V$. ■

Definición 3.1.3. Sea X una variedad, U un subconjunto abierto no vacío de X. Designamos por $\Gamma(U, \mathcal{O}_X)$, o simplemente $\Gamma(U)$, al conjunto de funciones racionales sobre X que están definidas en cada uno de los puntos $P \in U$: $\Gamma(U) = \bigcap_{P \in U} \mathcal{O}_P(X)$.

Observemos que con esta definición, $\Gamma(U)$ es un subanillo de $k(X)$, y si $U' \subset U$, entonces $\Gamma(U) \subset \Gamma(U')$. Notemos que si $U = X$ es una variedad afín, entonces $\Gamma(X)$ es el anillo coordenado de X, por lo tanto nuestra notación es consistente.

Si $z \in \Gamma(U)$, z determina una función k-valuada sobre U: pues si $P \in U$, $z \in \mathcal{O}_P(X)$, y $z(P)$ está bien definido.
Sea $\Im(U, k)$ el anillo de todas las funciones k-valuadas sobre U. La aplicación que asocia una función a cada $z \in \Gamma(U)$ es un homomorfismo del anillo $\Gamma(U)$ en el anillo $\Im(U, k)$.

Lema 3.1.3. *Sea U un subconjunto abierto de una variedad X. Si $z \in \Gamma(U)$, y $z(P) = 0$ para todo $P \in U$, entonces $z = 0$.*

Demostración. Sea $z \in \Gamma(U)$ tal que $z(P) = 0$ para todo $P \in U$, entonces el conjunto $V(z) = \{P \in V \mid z(P) = 0\}$ es un conjunto cerrado en V pues es una subvariedad de V, con lo que tenemos que $U \subset V(z) \subset V$; y por el Lema 3.1.2 sabemos que U es un conjunto denso en V, entonces V es el cerrado más pequeño que contiene a U pues es su cerradura topológica, por lo tanto, $V(z) = V$, lo cual implica que $z = 0$. ∎

Si $\varphi : X \to Y$ es una función entre conjuntos, componiendo con φ se obtiene el homomorfismo de anillos $\widetilde{\varphi} : \Im(Y, k) \to \Im(X, k)$; es decir, $\widetilde{\varphi}(f) = f \circ \varphi$. Esto nos motiva a la siguiente definición.

Definición 3.1.4. Sean X, Y variedades. Un *morfismo* de X en Y es una función $\varphi : X \to Y$ tal que:

(1) φ es continua.

(2) Para todo conjunto abierto U de Y, si $f \in \Gamma(U, \mathcal{O}_Y)$, entonces $\widetilde{\varphi}(f) = f \circ \varphi \in \Gamma(\varphi^{-1}(U), \mathcal{O}_X)$.

Un *isomorfismo* entre X y Y es un morfismo φ uno a uno de X sobre Y, tal que φ^{-1} es un morfismo.

Una variedad isomorfa a una subvariedad cerrada de un cierto $\mathbb{A}^n$ (o bien $\mathbb{P}^n$) se denominará *variedad afín* (respectivamente *variedad proyectiva*). Cuando escribimos "$X \subset \mathbb{A}^n$ es una variedad afín", querremos indicar que X es una subvariedad cerrada de $\mathbb{A}^n$, mientras que si decimos solamente "X es una variedad afín"querremos significar que X es una variedad en el sentido general de la Definición 3.1.1, pero que existe un isomorfismo de X

a una subvariedad cerrada de un cierto $\mathbb{A}^n$. Una observación semejante es válida para las variedades proyectivas.

Proposición 3.1.1. *Sean X y Y variedades afines. Existe una correspondencia natural uno a uno, entre morfismos $\varphi : X \to Y$, y homomorfismos de anillos $\widetilde{\varphi} : \Gamma(Y) \to \Gamma(X)$. Si $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$, un morfismo de X en Y coincide con una aplicación polinómica.*

Demostración. Podemos suponer que $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ son subvariedades cerradas de un espacio afín. La proposición se sigue de las siguientes consideraciones: (i) una aplicación polinómica es un morfismo; (ii) un morfismo φ induce un homomorfismo $\widetilde{\varphi} : \Gamma(Y) \longrightarrow \Gamma(X)$; (iii) todo $\widetilde{\varphi} : \Gamma(Y) \longrightarrow \Gamma(X)$ está inducido por una aplicación polinómica única de X en Y gracias a la Proposición 1.2.1; (iv) y todas estas operaciones son compatibles. ■

Proposición 3.1.2. *Sea V una variedad afín, y $f \in \Gamma(V)$ con $f \neq 0$. Sea $V_f = \{P \in V \mid f(P) \neq 0\}$, una variedad abierta de V. Entonces*

(1) $\Gamma(V_f) = \Gamma(V)[1/f] = \{a/f^n \in k(V) \mid a \in \Gamma(V),\ n \in \mathbb{Z}\}$.

(2) *V_f es una variedad afín.*

Demostración. Podemos suponer que $V \subset \mathbb{A}^n$, sean $I = I(V)$, $\Gamma(V) = k[X_1, \ldots, X_n]/I$. Tomemos la $F \in k[X_1, \ldots, X_n]$ tal que su I–clase residual $\overline{F}$ sea f.

(1): Sea $z \in \Gamma(V_f)$: El conjunto de polos de z es $V(J)$, donde $J = \{G \in k[X_1, \ldots, X_n] \mid \overline{G}z \in \Gamma(V)\}$ (como en la demostración de la Proposición 1.3.1). Como $V(J) \subset V(F)$, $F^N \in J$ para un cierto N, por el teorema de Nullstellensatz. Luego $f^N z = a \in \Gamma(V)$, por lo tanto $z = a/f^n \in \Gamma(V)[1/f]$. La otra inclusión es obvia.

(2): Deseamos "empujar los ceros de F al infinito". Consideremos al ideal I' generado por I y por $X_{n+1}F - 1$ en $k[X_1, \ldots, X_{n+1}]$, sea $V' = V(I') \subset \mathbb{A}^{n+1}$.

Sea $\alpha : k[X_1, \ldots, X_{n+1}] \longrightarrow \Gamma(V_f)$ definida de la siguiente manera: $\alpha(X_i = \overline{X_i})$ si $i \leq n$, y $\alpha(X_{n+1}) = 1/f$. Según la parte (1) tenemos que α es exhaustiva, y es claro que $Ker(\alpha) = I'$. En particular I' es primo, por lo tanto V' es una variedad, y α induce un isomorfismo $\overline{\alpha} : \Gamma(V') \longrightarrow \Gamma(V_f)$.

La proyección $(X_1, \ldots, X_{n+1}) \mapsto (X_1, \ldots, X_n)$ de $\mathbb{A}^{n+1}$ en $\mathbb{A}^n$ induce un morfismo $\varphi : V' \longrightarrow V_f$. El morfismo φ es uno a uno y exhaustivo, y $\widetilde{\varphi} = (\overline{\alpha})^{-1}$. Si $W = V(G_\alpha(X_1, \ldots, X_{n+1})) \cap V'$ es cerrado en V', entonces tenemos que el conjunto $\varphi(W) = V(F^N G_\alpha(X_1, \ldots, X_n, 1/F)) \cap V_f$, es cerrado en V_f, donde $N > gr(G_\alpha)$, de donde resulta que φ^{-1} es un morfismo, y por lo tanto, un isomorfismo.

■

Proposición 3.1.3. *Sea X una variedad, $P, Q \in X$, entonces existe un conjunto afín abierto V de X que contiene a P y a Q.*

Demostración. Sea X una variedad, entonces existe V variedad algebraica tal que $X \subset V$, y X es abierto en V, por lo tanto $V \setminus X$ es cerrado en V. $P, Q \in X$ si $P, Q \notin V \setminus X$. Por la Proposición 1.3.5 sabemos que existe un polinomio F, tal que $F(R) = 0$ si $R \in V \setminus X$, y $F(P) \neq 0$, $F(Q) \neq 0$. Sea f la imagen de F en $\Gamma(V)$.

Sea $V_f = \{P \in V \mid f(P) \neq 0\} \subset X$, y $P, Q \in V_f$. Por la Proposición 3.1.2, V_f es una variedad afín abierta de V, y como está contenida en X, V_f es abierto en X (por la topología inducida). ■

Proposición 3.1.4. *Sea X una variedad, P, Q dos puntos distintos de X. Existe una $f \in k(X)$ definida en P y en Q, con $f(P) = 0$, $f(Q) \neq 0$. Por lo tanto $f \in \mathfrak{m}_P(X)$, $f \notin \mathcal{O}_Q(X)$. Todos los anillos locales $\mathcal{O}_P(X)$, $P \in X$, son distintos.*

Demostración. Por la Proposición 3.1.3 sabemos que existe W variedad afín abierta de X tal que $P, Q \in W$. Dado que $\Gamma(W) = \bigcap_{P \in W} \mathcal{O}_P(X)$, si $z \in \Gamma(W)$, entonces z está definida en P y en Q, es decir, si $z = f/g$, entonces $g(P) \neq 0$, y $g(Q) \neq 0$, con $f, g \in \Gamma(V)$, donde $X \subset V$, y V es variedad irreducible. Por la Proposición 1.3.5 existe $H \in k[X_1, \ldots, X_n]$ tal que $H(P) = 0$, y $H(Q) \neq 0$, entonces $H \notin I(V)$.

Sea $h = \overline{H} \in \Gamma(V)$, entonces $h/g \in k(X)$, y $\frac{h}{g}(P) = \frac{h(P)}{g(P)} = 0$, y $\frac{h(Q)}{g(Q)} \neq 0$, es decir, $f = h/g$ es tal que $f(P) = 0$, y $f(Q) \neq 0$. ■

Proposición 3.1.5. *Si $V \subset A$, $W \subset B$ son subvariedades cerradas, entonces $V \times W$ es una subvariedad cerrada de $A \times B$.*

Demostración. Como V es una subvariedad cerrada de A, quiere decir que V es el conjunto de ceros de ciertos polinomios (a saber, aquellos que están en el ideal $I(V)$), y además es irreducible. Lo análogo para W, con lo cual concluimos que $V \times W$ es el conjunto de ceros de los polinomios del ideal $I(V) \times I(W)$, con lo cual es un conjunto algebraico, sólo falta ver que es irreducible.

Supongamos que $V \times W = Z_1 \cup Z_2$, donde Z_i es cerrado en $A \times B$. Sea $U_i = \{y \in W \mid V \times \{y\} \nsubseteq Z_i\}$. Tenemos que $V \times \{y\}$ es irreducible, pues es isomorfo a V, entonces $U_1 \cap U_2 = \varnothing$, pero U_i es abierto en B pues si $F_\alpha(X, Y)$ es el conjunto de polinomios que definen a Z_1, donde $X = X_1, \ldots, X_n$ y $Y = Y_1, \ldots, Y_m$. Si $y \in U_1$, entonces para algún α y algún $x \in V$, $F_\alpha(x, y) \neq 0$. Sea $G_\alpha(Y) = F_\alpha(x, Y)$. Entonces $\{y' \in W \mid G_\alpha(y') \neq 0\}$ es una vecindad abierta de y en U_1, por lo tanto U_1 es abierto. El mismo argumento sirve para ver que U_2 es abierto.

Por lo tanto, como cada U_i es abierto y no se intersecan, al ser W una variedad nos implica

que por lo menos uno de los U_i es vacío (sin pérdida de generalidad, digamos que $U_1 = \varnothing$), y entonces $V \times W \subset Z_1$, con lo cual tenemos que $V \times W$ es irreducible. ■

Proposición 3.1.6. *Sean X, Y abiertos en $V \subset A$ y $W \subset B$ respectivamente, donde V, W, A, B son como en la proposición anterior. Entonces se cumplen las siguientes afirmaciones:*

(1) *Las proyecciones $\pi_1 : X \times Y \to X$, y $\pi_2 : X \times Y \to Y$ son morfismos.*

(2) *Si $f : Z \to X$, $g : Z \to Y$ son morfismos, entonces $(f, g) : Z \to X \times Y$ definida por $(f, g)(z) = (f(z), g(z))$ es un morfismo.*

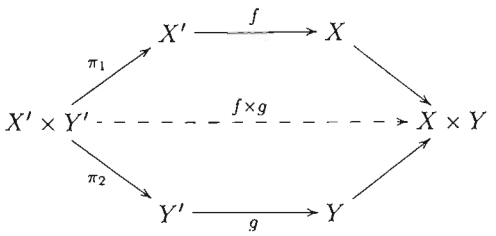
(3) *Si $f : X' \to X$, $g : Y' \to Y$ son morfismos, entonces $f \times g : X' \times Y' \to X \times Y$ definida por $(f \times g)(x', y') = (f(x'), g(y'))$ es un morfismo.*

(4) *La diagonal $\triangle_X = \{(x, y) \in X \times X \mid y = x\}$ es una subvariedad cerrada de $X \times X$, y la aplicación diagonal $\delta_X : X \to \triangle_X$ definida por $\delta_X(x) = (x, x)$ es un isomorfismo.*

Demostración. (1): Sea $U \subset X$ un subconjunto abierto de X, entonces $\pi_1^{-1}(U) = U \times Y$ que es abierto en $X \times Y$, y por tanto π_1 es continua, de manera análoga se muestra que π_2 también es continua. Ahora sea $f \in \Gamma(U, \mathcal{O}_X)$, entonces f está definida en todo U, queremos mostrar que $\widetilde{\pi}_1(f) = f \circ \pi_1$ está definida en todo $\pi_1^{-1}(U) = U \times Y$; pero $\widetilde{\pi}_1(f)(x, y) = (f \circ \pi_1)(x, y) = f(x)$ es una función que va de $U \times Y$ en k, por lo que $\widetilde{\pi}_1(f)$ está definida en todo $U \times Y$ porque f lo está en U, por lo tanto π_1 es un morfismo. El mismo argumento muestra que π_2 también lo es.
(2): Sea $U_1 \times U_2$ un abierto en $X \times Y$, entonces $(f, g)^{-1}(U_1 \times U_2) = f^{-1}(U_1) \cup g^{-1}(U_2)$ que es abierto en Z pues f, g son continuas, por lo tanto (f, g) es también continua. Sea $\varphi \in \Gamma(U_1 \times U_2, \mathcal{O}_{X \times Y})$, entonces φ está definida para todo $P \in U_1 \times U_2$, nos fijamos en un punto $P_0 \in f^{-1}(U_1) \cup g^{-1}(U_2)$, entonces $\widetilde{(f, g)}(\varphi)(P_0) = (\varphi \circ (f, g))(P_0) = \varphi((f(P_0), g(P_0)))$ y como φ está definida en $(f(P_0), g(P_0)) \in U_1 \times U_2$ entonces $\widetilde{(f, g)}(\varphi) \in \Gamma(f^{-1}(U) \cup g^{-1}(U_2), \mathcal{O}_Z)$, por lo tanto (f, g) es morfismo.
(3): Descompongamos la aplicación

$$X' \times Y' \xrightarrow{f \times g} X \times Y$$

en lo siguiente:



entonces, aplicando el inciso (2) de ésta proposición, tenemos que

$$f \times g = (f \circ \pi_1, g \circ \pi_2)$$

que ya mostramos que es un morfismo.
(4): La diagonal $\triangle_X$ es un conjunto algebraico, puesto que X es una variedad, entonces X es el conjunto de ceros de $f_\alpha \in k[X_1, \ldots, X_n]$, entonces podemos ver a este conjunto cómo $F_\alpha \in k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, donde los f_α son los polinomios F_α vistos como polinomios valuados sólo en las primeras $X_1, \ldots, X_2$ variables, y entonces $\triangle_X$ es el conjunto de ceros de $F_\alpha - G_\alpha$ dónde los G_α son los polinomios f_α vistos como polinomios en las variables $X_1, \ldots, X_n, Y_1, \ldots, Y_n$, pero sólo valuados en las variables $Y_1, \ldots, Y_n$, por lo tanto $\triangle_X$ es una subvariedad cerrada de $X \times X$.
Por el inciso (2) de esta proposición, δ_X es un morfismo, pues viene de considerar dos veces $id_X : X \longrightarrow X$, por tanto $\delta_X = (id_X, id_X)$ que ya mostramos que es un morfismo; y la proyección $\pi_1 : X \times X \longrightarrow X$ es la inversa de δ_X que ya mostramos también que es un morfismo, por lo tanto δ_X es un isomorfismo. ■

Corolario 3.1.1. *Si $f, g : X \to Y$ son morfismos de variedades, entonces $\{x \in X \mid f(x) = g(x)\}$ es cerrado en X. Si f y g coinciden sobre un conjunto denso en X, entonces $f = g$.*

Demostración. Por los incisos (3) y (4) de la proposición anterior, tenemos que $\{x \in X \mid f(x) = g(x)\} = (f \times g)^{-1}(\triangle_Y)$, que ya mostramos que es una subvariedad cerrada isomorfa a X. Entonces, si f y g coinciden en un conjunto denso en X, entonces por el Lema 3.1.2, ese conjunto denso es un abierto no vacío de X, su complemento en X es un cerrado que es una subvariedad, y ya vimos que el conjunto en donde coinciden es isomorfo a X. ■

Proposición 3.1.7. *Sean X, Y afines, y $f : X \longrightarrow Y$ un morfismo de variedades. Entonces $f(X)$ es denso en Y si y sólo si $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ es uno a uno.*

Definición 3.1.5. Sean X, Y variedades. Decimos que dos morfismos $f_i : U_i \longrightarrow Y$ $(i = 1, 2)$ de subvariedades abiertas $U_i \subset X$ están relacionadas si sus restricciones a $U_1 \cap U_2$ coinciden, es decir

$$f_1 \sim f_2 \iff f_1 \mid_{U_1 \cap U_2} = f_2 \mid_{U_1 \cap U_2}$$

Proposición 3.1.8. *La relación de la Definición 3.1.5 es de equivalencia.*

Demostración. La reflexividad y la simetría son inmediatas, para ver que es transitiva consideremos que $U_1 \cap U_2$ es denso por los Lemas 3.1.1 y 3.1.2; entonces, por el Corolario 3.1.1, toda f_i está determinada por su restricción sobre $U_1 \cap U_2$. Entonces, si $f_1 \sim f_2$ y $f_2 \sim f_3$, entonces, el abierto $U_1 \cap U_2 \cap U_3$ es denso y por tanto, f_1, f_2, f_3 están determinadas por su restricción en $U_1 \cap U_2 \cap U_3$, con lo que son iguales en ese abierto, lo que implica que $f_1 \sim f_3$. ■

Definición 3.1.6. Llamamos *aplicación racional* a una clase de equivalencia de los morfismos de X en Y relacionados como en la Definición 3.1.5.

Definición 3.1.7. El *dominio* de una aplicación racional es la unión de todas las subvariedades abiertas U_α de X tales que algún $f_\alpha : U_\alpha \longrightarrow Y$ pertenece a la clase de equivalencia de la aplicación racional.

Observación 3.1.1. Si U es el dominio de una aplicación racional, la función $f : U \longrightarrow Y$ definida por $f \mid_{U_\alpha} = f_\alpha$ es un morfismo perteneciente a la clase de equivalencia de la aplicación; todo morfismo equivalente es una restricción de f. Así, una aplicación racional de X en Y puede también definirse como un morfismo f de una subvariedad abierta $U \subset X$ en Y tal que f no puede extenderse a un morfismo de algún subconjunto abierto mayor de X en Y.

Definición 3.1.8. Una aplicación racional de X en Y se llama *dominante* si $f(U)$ es denso en Y, donde $f : U \to Y$ es un morfismo representante de la aplicación.

Dado que f está determinado por su restricción, entonces el morfismo f de la definición de arriba es independiente de U.

Definición 3.1.9. Si A y B son anillos locales, y A es un subanillo de B, diremos que B *domina* a A si el ideal maximal de B contiene al ideal maximal de A; es decir si $\mathfrak{m}_A \subset \mathfrak{m}_B$.

Proposición 3.1.9. (1) *Sea F una función racional dominante de X en Y. Sean $U \subset X$, $V \subset Y$ subconjuntos afines abiertos. $f : U \longrightarrow Y$ un morfismo que represente a F. Entonces la aplicación inducida $\widetilde{f} : \Gamma(V) \longrightarrow \Gamma(U)$ es uno a uno, así que $\widetilde{f}$ se extiende a un homomorfismo uno a uno de $k(Y) = k(V)$ en $k(X) = k(U)$. Este homomorfismo es independiente de la elección de f, y se designa $\widetilde{F}$.*

(2) *Si P pertenece al dominio de F, y $F(P) = Q$, entonces $\mathcal{O}_P(X)$ domina a $\widetilde{F}(\mathcal{O}_Q(Y))$. Recíprocamente, si $P \in X$, $Q \in Y$ y $\mathcal{O}_P(X)$ domina a $\widetilde{F}(\mathcal{O}_Q(Y))$, entonces P pertenece al dominio de F, y $F(P) = Q$.*

(3) *Todo homomorfismo de $k(Y)$ en $k(X)$ viene inducido por una aplicación dominante única de X en Y.*

Demostración. La demostración de (1) es consecuencia de la Proposición 3.1.7. Sólo hay que destacar que $k(X) = k(U)$ puesto que U es un abierto máximo gracias a la Observación 3.1.1.

(2): Si $\mathcal{O}_P(X)$ domina a $\widetilde{F}(\mathcal{O}_Q(Y))$, consideremos vecindades afines V de P, W de Q. Sea $\Gamma(W) = k[y_1, \ldots, y_n]$. Entonces $\widetilde{F}(y_i) = a_i b_i^{-1}$, con $a_i, b_i \in \Gamma(V)$, y $b_i(P) \neq 0$. Si hacemos $b = b_1 \cdot b_2 \cdot \ldots \cdot b_n$, entonces $\widetilde{F}(\Gamma(W)) \subset \Gamma(V_b)$ gracias a la Proposición 3.1.2, luego $\widetilde{F} : \Gamma(W) \longrightarrow \Gamma(V_b)$ está inducida por un morfismo único $f : V_b \longrightarrow W$ por la Proposición 3.1.1. Si $g \in \Gamma(W)$ se anula en Q, entonces $\widetilde{F}(g)$ se anula en P, de donde resulta que $f(P) = Q$.

(3): Podemos suponer X y Y afines. Entonces como en (2), si $\varphi : k(Y) \longrightarrow k(X)$, $\varphi(\Gamma(Y)) \subset \Gamma(X_b)$ para algún $b \in \Gamma(X)$, luego φ está inducido por un morfismo f que va de X_b a Y. Según la Proposición 3.1.7, $f(X_b)$ es denso en Y puesto que $\widetilde{f}$ es uno a uno. ■

Definición 3.1.10. Una aplicación racional $F : X \to Y$ se dice que es *birracional* si existen conjuntos abiertos $U \subset X$, $V \subset Y$, y un isomorfismo $f : U \to V$ que represente a F.

Definición 3.1.11. Decimos que X y Y son *birracionalmente equivalentes* si existe una aplicación birracional de X en Y.

Ser birracionalmente equivalente es una relación de equivalencia. Por ejemplo, una variedad es birracionalmente equivalente a toda subvariedad abierta de sí misma. $\mathbb{A}^n$ y $\mathbb{P}^n$ son birracionalmente equivalentes.

Proposición 3.1.10. *Dos variedades son birracionalmente equivalentes si y sólo si sus campos de funciones son isomorfos.*

Demostración. Como $k(U) = k(X)$ para toda subvariedad abierta U de X, variedades birracionalmente equivalentes poseen campo de funciones isomorfos.

Recíprocamente, por hipótesis $\varphi : k(X) \to k(Y)$ es un isomorfismo. Podemos suponer que X y Y son afines. Entonces $\varphi(\Gamma(X)) \subset \Gamma(Y_b)$ para un cierto $b \in \Gamma(Y)$, y también

$\varphi^{-1}(\Gamma(Y)) \subset \Gamma(X_d)$ para algún $d \in \Gamma(X)$, como en la demostración de la Proposición 3.1.9. Entonces la restricción de φ es un isomorfismo de $\Gamma((X_d)_{\varphi^{-1}(b)})$ sobre $\Gamma((Y_b)_{\varphi(d)})$. Luego $(X_d)_{\varphi^{-1}(b)}$ es isomorfo a $(Y_b)_{\varphi(d)}$, como queríamos. ■

Corolario 3.1.2. *Toda curva es birracionalmente equivalente a una curva plana.*

Demostración. Si V es una curva, $k(V) = k(x, y)$ para ciertos $x, y \in k(V)$. Sea I el núcleo del homomorfismo natural de $k[X, Y]$ sobre $k[x, y] \subset k(V)$. Entonces I es primo, luego $V' = V(I) \subset \mathbb{A}^2$ es una variedad. Como $\Gamma(V') = k[X, Y]/I$ es isomorfo a $k[x, y]$, se tiene que $k(V')$ es isomorfo a $k(x, y) = k(V)$. Luego $dim(V') = 1$, y por tanto V' es una curva plana. ■

Definición 3.1.12. Una variedad se llama *racional* si es birracionalmente equivalente a $\mathbb{A}^n$ (o $\mathbb{P}^n$) para un cierto n.

3.2. Modelos no-singulares de curvas

Como vimos en la Definición 2.1.7, un punto P de una curva $\mathcal{C}$ se dice que es un punto simple, si $\mathcal{O}_P(\mathcal{C})$ es un anillo de valuación discreta. Consideramos que $ord_P{}^{\mathcal{C}}$ u ord_P designa a la función orden sobre $k(\mathcal{C})$ definida por $\mathcal{O}_P(\mathcal{C})$ como en la Definición 1.1.5. Diremos que $\mathcal{C}$ es *no-singular* si cada punto de $\mathcal{C}$ es simple.

Definición 3.2.1. Sea K un campo que contenga a k. Diremos que un anillo local A es un *anillo local de* K, si A es un subanillo de K, A contiene a k y K es el campo de cocientes de A.

Como ejemplo de anillo local de un campo tenemos el siguiente: Si V es una variedad, $P \in V$, entonces $\mathcal{O}_P(V)$ es el anillo local de $k(V)$.

Definición 3.2.2. Un *anillo de valuación discreta de* K, es un AVD que además es un anillo local de K.

Teorema 3.2.1. *Sea $\mathcal{C}$ una curva proyectiva, $K = k(\mathcal{C})$. Supongamos que L es un campo que contiene a K, y R es un anillo de valuación discreta de L, tal que $K \not\subseteq R$. Entonces existe un punto único $P \in \mathcal{C}$ tal que R domina a $\mathcal{O}_P(\mathcal{C})$.*

Demostración. (Unicidad):
Si R domina a $\mathcal{O}_P(\mathcal{C})$ y a $\mathcal{O}_Q(\mathcal{C})$, elijamos $f \in \mathfrak{m}_P(\mathcal{C})$, $1/f \in \mathcal{O}_Q(\mathcal{C})$ como en la Proposición 3.1.4. Entonces $ord(f) > 0$ y $ord(1/f) \geq 0$, lo cual es una contradicción. ∎

Demostración. (Existencia):
Podemos suponer que $\mathcal{C}$ es una subvariedad cerrada de $\mathbb{P}^n$, y que $\mathcal{C} \cap U_i \neq \varnothing$, $i = 1, \ldots, n+1$. Entonces en $\Gamma_{hom}(\mathcal{C}) = k[X_1, \ldots, X_{n+1}]/I(\mathcal{C}) = k[x_1, \ldots, x_{n+1}]$, cada $x_i \neq 0$.

Sea $N = \max\limits_{i,j} ord(x_i/x_j)$. Supongamos que $ord(x_j/x_{n+1}) = N$ para un cierto j (Si es necesario, podemos efectuar un cambio de coordenadas para que esto suceda). Entonces para todo i tenemos

$$ord(x_i/x_{n+1}) = ord((x_j/x_{n+1})(x_i/x_j)) = N - ord(x_j/x_i) \geq 0.$$

Si $\mathcal{C}_*$ es la curva afín correspondiente a $\mathcal{C} \cap U_{n+1}$, entonces $\Gamma(\mathcal{C}_*)$ se puede identificar con $k[x_1/x_{n+1}, \ldots, x_n/x_{n+1}]$, luego $\Gamma(\mathcal{C}_*) \subset R$.

Sea M el ideal maximal de R, $J = M \cap \Gamma(\mathcal{C}_*)$. J es un ideal primo, por lo tanto a J le corresponde una subvariedad cerrada W de $\mathcal{C}_*$. Si $W = \mathcal{C}_*$, entonces $J = 0$, y todo elemento no nulo de $\Gamma(\mathcal{C}_*)$ es unidad en R; pero entonces $K \subset R$, lo cual contradice nuestra hipótesis. Luego $W = \{P\}$ es un punto, debido a que toda subvariedad cerrada propia de una curva es un punto. Por tanto, R domina a $\mathcal{O}_P(\mathcal{C}_*) = \mathcal{O}_P(\mathcal{C})$. ∎

Corolario 3.2.1. *Si C es una curva proyectiva y C' una curva no-singular, entonces existe una correspondencia natural y uno a uno entre los morfismos dominantes $f : C' \to C$ y los homomorfismos $\widetilde{f} : k(C) \to k(C')$.*

Corolario 3.2.2. *Dos curvas proyectivas no-singulares son isomorfas si y sólo si sus campos de funciones son isomorfos.*

Corolario 3.2.3. *Sea C una curva proyectiva no-singular, $K = k(C)$. Entonces existe una correspondencia natural uno a uno, entre los puntos de C y los anillos de valuación discreta de K. Si $P \in C$, $\mathcal{O}_P(C)$ es el correspondiente AVD.*

Demostración. Cada $\mathcal{O}_P(C)$ es ciertamente un AVD de K. Si R es uno de estos AVD, entonces R domina a uno solo de los $\mathcal{O}_P(C)$. Como R y $\mathcal{O}_P(C)$ son ambos AVD de K, esto prueba que $R = \mathcal{O}_P(C)$ debido a la Proposición 1.1.4.

Sean C, K como en el las hipótesis del Corolario, y X es el conjunto de todos los anillos de valuación discreta sobre k. Definimos una topología sobre X de la siguiente manera: Un conjunto U no vació de X es abierto si $X - U$ es finito. Entonces la correspondencia $P \to \mathcal{O}_P(C)$ de C en X es un homeomorfismo. Y si U es abierto en C, $\Gamma(U, \mathcal{O}_C) = \bigcap_{P \in C} \mathcal{O}_P(C)$, por lo tanto todos los anillos de funciones sobre C pueden ser recubiertos por X. Como X está determinado sólo por K, esto significa que C está determinado sólo por K salvo isomorfismos de K (gracias al Corolario 3.2.2). ■

A continuación enunciaremos un teorema y dos lemas, cuyos resultados nos son importantes, pero dado a que la demostración de estos utiliza técnicas para desingularizar una curva, y este tema sale del alcance de esta tesis, omitiremos las pruebas, y el lector podrá consultarlas en [4] Fulton W., *Algebraic Curves*, Capítulo 7, pág. 179-183.

Teorema 3.2.2. *Sea C una curva proyectiva. Entonces existe una curva proyectiva no-singular X y un morfismo birracional f de X sobre C. Si $f' : X' \to C$ es otro, entonces existe un isomorfismo único $g : X \to X'$ tal que $f'g = f$.*

Corolario 3.2.4. *Existe una correspondencia uno a uno natural entre curvas proyectivas no-singulares X y campos de funciones algebraicas en una variable K sobre k: $K = k(X)$. Si X, X' son dos de tales curvas, a morfismos dominantes de X' en X corresponden homomorfismos de $k(X)$ en $k(X')$.*

Estos dos resultados nos motivan a la siguiente definición.

Definición 3.2.3. Sea C una curva proyectiva, $f : X \to C$ como en el Teorema 3.2.2. Decimos que X es el *modelo no-singular* de C, o de $K = k(C)$.

Identificaremos $k(X)$ con K por medio de $\widetilde{f}$ como en el Corolario 3.2.1.

Los puntos Q de X están en correspondencia uno a uno con los anillos de valuación discreta $\mathcal{O}_Q(X)$ de K gracias al Corolario 3.2.3.

Observemos que $f(Q) = P$ cuando $\mathcal{O}_Q(X)$ domina a $\mathcal{O}_P(C)$.

Definición 3.2.4. Sea X el modelo no-singular de una curva proyectiva C, a los puntos de X los llamamos *lugares* de C o de K.

Definición 3.2.5. Diremos que un lugar Q está *centrado en* P, si $f(Q) = P$.

Lema 3.2.1. *Sea C una curva plana proyectiva, $P \in C$. Entonces existe un entorno afín U de C tal que:*

(1) $f^{-1}(U) = U'$ *es una subvariedad abierta afín de* X.

(2) $\Gamma(U')$ *es un módulo finito sobre* $\Gamma(U)$.

(3) *Para cada* $0 \neq t \in \Gamma(U)$, $t\Gamma(U') \subset \Gamma(U)$.

(4) *El espacio vectorial* $\Gamma(U')/\Gamma(U)$ *es de dimensión finita sobre* k.

El entorno U puede ser tomado excluyendo un conjunto finito S cualquiera de puntos de C, si $P \notin S$.

Notación: Sea una curva proyectiva plana, y $f : X \to C$ como antes, $Q \in X$, $f(Q) = P \in C$. Para toda curva plana G (posiblemente reducible), formamos $G_* \in \mathcal{O}_P(\mathbb{P}^2)$ como en la Sección 2.3; sea g la imagen de G_* en $\mathcal{O}_P(C) \subset k(C) = k(X)$. Definimos $ord_Q(G)$ identificando con $ord_Q(g)$. Como es usual, esta definición es independiente de la elección de G_*.

Proposición 3.2.1. *Sean C una curva plana proyectiva irreducible, $P \in C$, $f : X \to C$ como antes, y G una curva plana (posiblemente reducible). Entonces*

$$I_P(F \cap G) = \sum_{Q \in f^{-1}(P)} ord_Q(G).$$

Demostración. Sea g la imagen de G_* en $\mathcal{O}_P(C)$. Elegimos U como en el Lema 3.2.1, tan pequeño que g sea una unidad en todos los $\mathcal{O}_{P'}(C)$, $P' \in U$, $P' \neq P$. Entonces, por la Proposición 1.3.13, y el Corolario 1.3.1, tenemos $I_P(C \cap G) = dim_k(\mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*)) = dim_k(\mathcal{O}_P(C)/(g)) = dim_k(\Gamma(U)/(g))$. Sea $V = \Gamma(U)$, $V' = \Gamma(U')$, y $T : V' \to V'$ definida por $T(z) = gz$. V'/V es de dimensión finita, luego en virtud de la Proposición 1.3.18 tenemos que $dim(V/T(V)) = dim(V'/T(V'))$, y $dim_k(\Gamma(U)/(g)) = dim_k(\Gamma(U')/(g))$. En virtud del Corolario 1.3.1, $dim(\Gamma(U')/(g)) = \sum_{Q \in f^{-1}(P)} dim(\mathcal{O}_Q(X)/(g)) = \sum ord_Q(g)$, como queríamos ver. ∎

Lema 3.2.2. *Supongamos que P es un punto múltiple ordinario de C de multiplicidad r. Sea $f^{-1}(P) = \{P_1, \ldots, P_r\}$. Si $z \in k(C)$, y $ord_{P_i}(z) \geq r - 1$, entonces $z \in \mathcal{O}_P(C)$.*

Proposición 3.2.2. *Sea F una curva plana proyectiva e irreducible, P un punto múltiple ordinario de F de multiplicidad r. Sean $P_1, \ldots, P_r$ los lugares centrados en P, y G, H curvas planas, posiblemente reducibles. Entonces las condiciones de Noether se satisfacen en P (respecto a F, G, H), si $ord_{P_i}(H) \geq ord_{P_i}(G) + r - 1$ para $i = 1, \ldots, r$.*

Demostración. $H_* \in \langle F_*, G_* \rangle \subset \mathcal{O}_P(\mathbb{P}^2)$ es equivalente a $\overline{H}_* \in \langle \overline{G}_* \rangle \subset \mathcal{O}_P(F)$, o a $z = (\overline{H}_*/\overline{G}_*) \in \mathcal{O}_P(F)$. Aplicando el Lema 3.2.2 a z se obtiene la proposición. ■

Proposición 3.2.3. *Sea X una curva proyectiva no-singular, $P_1, \ldots, P_r \in X$. Para todo $m_1, \ldots, m_r \in \mathbb{Z}$, existe un $z \in k(X)$ tal que $ord_{P_i}(z) = m_i$*

Demostración. Como ya vimos, X es birracionalmente equivalente a una curva plana C, entonces sea L_i una recta que pasa por P_i (y no es tangente a C en P_i) y no pasa por los demás P_j, y sea L_0 la recta que no pasa por ninguno de los puntos P_i. Sea $z = \prod L_i^{m_i} L_0^{-\sum m_i}$; por el Teorema 2.1.1, tenemos que L_i es un parámetro de uniformización de $\mathcal{O}_{P_i}(C)$ para cad i, y $L_0^{-\sum m_i} / \prod L_j^{m_j}$ $(j \neq i)$ es una unidad porque no pasan por P_i, por lo que $ord_{P_i}(z) = m_i$. ■

Capítulo 4

Teorema de Riemann-Roch

En todo este capítulo, C será una curva proyectiva irreducible, $f : X \to C$ el morfismo birracional del modelo no-singular X sobre C. $K = k(C) = K(X)$ su campo de funciones. Los puntos $P \in X$ serán identificados con los lugares de K, ord_P designa la función orden correspondiente sobre K.

4.1. Divisores

Definición 4.1.1. Un *divisor* de X es un elemento del grupo abeliano libre sobre el conjunto X, es decir, una suma formal $D = \sum_{P \in X} n_P P$, $n_P \in \mathbb{Z}$ y $n_P = 0$ salvo para un número finito.

Definición 4.1.2. El *grado* de un divisor es la suma de sus coeficientes: $gr(\sum n_P P) = \sum n_P$.

Con el grado así definido, es claro que $gr(D + D') = gr(D) + gr(D')$.

Definición 4.1.3. Decimos que un divisor $D = \sum n_P P$ es *efectivo* (o *positivo*) si todo $n_P \geq 0$.

Escribiremos $\sum n_P P \succ \sum m_P P$ si cada $n_P \geq m_P$.

Definición 4.1.4. Sea C una curva de grado n y G es una curva plana que no contenga a C como una componente. Definiremos el *divisor de* G, que denotaremos $div(G)$, como $\sum_{P \in X} ord_P(G) P$, donde $ord_P(G)$ está definido como en la Sección 3.2. Recordemos que ord_P es una valuación discreta sobre K.

Por la Proposición 3.2.1, tenemos que $\sum_{P\in X} ord_P(G) = \sum_{Q\in C} I_Q(C\cap G)$. Por el Teorema de Bézout, $div(G)$ es un divisor de grado mn, donde m es el grado de G. Notemos que el $div(G)$ contiene más información que el ciclo de intersección $G \cdot C$.

Definición 4.1.5. Para todo $z \in K$ no nulo, definimos el *divisor* de z, que denotaremos $div(z)$, como $\sum_{P\in X} ord_P(z)P$.

Como z posee solamente un número finito de ceros y polos, $div(z)$ es un divisor bien definido.

Definición 4.1.6. Definimos por $(z)_0 = \sum_{ord_P(z)>0} ord_P(z)P$, al *divisor de los ceros de* z, y por $(z)_\infty = \sum_{ord_P(z)<0} -ord_P(z)P$, al *divisor de los polos de* z.

Entonces tenemos que $div(z) = (z)_0 - (z)_\infty$. Observemos también que

$$div(zz') = div(z) + div(z'), \text{ y } div(z^{-1}) = -div(z).$$

Proposición 4.1.1. *Para todo $z \in K$ no nulo, $div(z)$ es un divisor de grado cero. Una función racional tiene el mismo número de ceros que de polos, siempre que se cuenten de forma adecuada.*

Demostración. Consideremos una curva plana C de grado n. Sea $z = g/h$, con g, h polinomios homogéneos del mismo grado en $\Gamma_{hom}(C)$; sabemos que g, h son clases residuales de polinomios homogéneos G, H de grado m en $k[X,Y,Z]$. Entonces $div(z) = div(G) - div(H)$, y hemos visto que $div(G)$ y $div(H)$ tienen grado mn. ■

Corolario 4.1.1. *Sea $0 \neq z \in K$, entonces las proposiciones siguientes son equivalentes:* (i) $div(z) \succ 0$, (ii) $z \in k$, (iii) $div(z) = 0$.

Demostración. Si $div(z) \succ 0$ entonces $ord_P(z) \geq 0$ para todo $P \in X$, entonces tenemos que $z \in \mathcal{O}_P(X)$ para todo $P \in X$. Si $z(P_0) = \lambda_0$ para algún P_0, entonces $div(z - \lambda_0) \succ 0$ y $gr(div(z - \lambda_0)) > 0$, pero en la Proposición 4.1.1 ya vimos que el grado debe ser cero, lo cual es absurdo, salvo que $z - \lambda_0 = 0$, es decir, $z \in k$, con lo que tenemos que *(i)* $\Rightarrow$ *(ii)*. Para demostrar que *(ii)* $\Rightarrow$ *(iii)*, simplemente hay que observar que si $z \in k$ entonces z no tiene ni ceros ni polos para ningún $P \in X$, por lo que $div(z) = 0$. Por último, la implicación *(iii)* $\Rightarrow$ *(i)* es obvia, ya que, si $div(z) = 0$ entonces claramente $ord_P(z) = 0$ para todo $P \in X$, y más claro aún es que, entonces $ord_P(z) \geq$ para todo P, con lo que $div(z) \succ 0$. ■

Corolario 4.1.2. *Sean $z, z' \in K$, ambos no nulos, entonces $div(z) = div(z')$ si y sólo si $z' = \lambda z$ para un cierto $\lambda \in k$.*

Demostración. Supongamos que $div(z) = div(z')$, entonces $div(z'z^{-1}) = 0$, y por el Corolario 4.1.1 tenemos que $z'z^{-1} \in k$, sea $\lambda = z'z^{-1}$, entonces $z' = \lambda z$.

Ahora supongamos que $z' = \lambda z$ con $\lambda \in k$, entonces $z'z^{-1} = \lambda \in k$, por el Corolario 4.1.1 tenemos que $div(z'z^{-1}) = 0 \Rightarrow div(z') - div(z) = 0$. ■

Definición 4.1.7. Dos divisores D, D' son *linealmente equivalentes* si $D = D' + div(z)$ para un cierto $z \in K$, en cuyo caso escribiremos $D \equiv D'$.

Proposición 4.1.2. (1): *La relación $\equiv$ es una relación de equivalencia.*

(2): *$D \equiv 0$ si y sólo si $D = div(z)$, $z \in K$.*

(3): *Si $D \equiv D'$, entonces $gr(D) = gr(D')$.*

(4): *Si $D \equiv D'$ y $D_1 \equiv D_1'$ entonces $D + D_1 \equiv D' + D_1'$.*

(5): *Sea C una curva plana, entonces $D \equiv D'$ si y sólo si existen dos curvas G, G' del mismo grado tales que $D + div(G) = D' + div(G')$.*

Demostración. (1): Sea D un divisor, para cualquier $z \in k$ no nulo, por el Corolario 4.1.1 tenemos que $div(z) = 0$, y por tanto $D = D + div(z)$, con lo que $D \equiv D$. Si $D \equiv D'$ entonces $D = D' + div(z)$ para algún $z \in K$, y es claro que también $z^{-1} \in K$ y que $D' = D - div(z) = D' + div(z^{-1})$, y por tanto $D' \equiv D$. Si $D \equiv D'$ y $D' \equiv D''$, entonces $D = D' + div(z_1)$ y $D' = D'' + div(z_2)$, con $z_1, z_2 \in k$; claramente $z_1 z_2 \in K$, y tenemos que $D = D'' + div(z_1) + div(z_2) = D'' + div(z_1 z_2)$, con lo que $D \equiv D''$.

(2): Supongamos $D \equiv 0$, entonces $D = 0 + div(z) = div(z)$ con $z \in K$. Ahora supongamos que $D = div(z)$ con $z \in K$, entonces $D = 0 + div(z)$ con lo que $D \equiv 0$.

(3): Si $D \equiv D'$, entonces $D = D' + div(z)$ con $z \in K$, entonces $gr(D) = gr(D' + div(z)) = gr(D') + gr(div(z))$, y debido a la Proposición 4.1.1 tenemos que $gr(div(z)) = 0$, por lo que $gr(D) = gr(D')$.

(4): Supongamos $D \equiv D'$ y $D_1 \equiv D_1'$, entonces $D = D' + div(z)$ y $D_1 = D_1' + div(z')$, con $z, z' \in K$, entonces $D + D_1 = D' + D_1 + div(z) = D' + D_1' + div(z') + div(z) = D' + D_1' + div(z'z)$, y claramente $z'z \in K$, por tanto $D + D_1 \equiv D' + D_1'$.

(5): Sea C una curva plana, y $D \equiv D'$, entonces $D' = D + div(z)$ con $z \in K$; como en la prueba de la Proposición 4.1.1, existen polinomios homogéneos G, $G' \in k[X, Y, Z]$ del mismo grado, de tal manera que $z = G/G'$, y $div(z) = div(G) - div(G')$, por lo que podemos escribir $D' = D + div(G) - div(G')$, y por tanto $D' + div(G') = D + div(G)$.

Análogamente, si $D + div(G) = D' + div(G')$ con $G, G' \in k[X, Y, Z]$ del mismo grado, entonces tomamos $z = G'/G \in \Gamma_{hom}(\mathcal{C})$, y por tanto $div(z) = div(G') - div(G)$, con lo cual $D = D' + div(G') - div(G) = D' + div(z)$, y por tanto $D \equiv D'$. ■

El criterio demostrado en la Sección 3.2 para las condiciones de Noether tiene una expresión elegante en el lenguaje de divisores:

Supongamos que $\mathcal{C}$ es una curva plana que sólo posee puntos múltiples ordinarios. Para cada $Q \in X$, sea $r_Q = m_{f(Q)}(\mathcal{C})$. Definimos al divisor $E = \sum_{Q \in X} (r_Q - 1)Q$. Observemos que E es un divisor efectivo de grado $\sum r_Q(r_Q - 1)$. Toda curva plana G tal que $div(G) \succ E$ se denomina *adjunta de* $\mathcal{C}$. Obsérvese que G es una adjunta de $\mathcal{C}$ si y sólo si $m_P(G) \geq m_P(\mathcal{C}) - 1$ para cada uno de los puntos (múltiples) $P \in \mathcal{C}$. Si $\mathcal{C}$ es no-singular, toda curva es una adjunta.

Teorema 4.1.1. (Del Residuo) *Sean $\mathcal{C}$, E como antes. Supongamos que D, D' son divisores efectivos de X, y $D \equiv D'$. Supongamos que G es una adjunta de grado m, tal que $div(G) = D + E + A$. para un cierto divisor efectivo A. Entonces existe una adjunta G' de grado m tal que $div(G') = D' + E + A$.*

Demostración. Como $D \equiv D'$, entonces por la Proposición 4.1.2 tenemos que existen H, H' curvas del mismo grado tales que $D + div(H) = D' + div(H')$. Entonces $div(GH) = div(H) + div(G) = div(H) + D + E + A = div(H') + D' + E + A$ y observemos que $div(H') + D' + E + A \succ div(H') + E$. Sea F el polinomio homogéneo que define a $\mathcal{C}$. Aplicando la Proposición 3.2.2 a F, H' y GH, vemos que las condiciones de Noether se satisfacen para todo $P \in \mathcal{C}$. Por el Teorema de Noether (2.4.1), $GH = F'F + G'H$ para ciertos F', G', donde $gr(G') = m$. Entonces $div(G') = div(GH) - div(H') = D' + E + A$. ■

4.2. El espacio vectorial $L(D)$

Sea $D = \sum n_P P$ un divisor de X. D selecciona un número finito de puntos, y les asigna enteros. Deseamos determinar cuándo existe una función racional cuyos polos sean, precisamente, los puntos escogidos, y con polos no "inferiores" al orden n_P en P; si es así, ¿cuántas de tales funciones existen?

Definición 4.2.1. Designamos por $L(D)$ al conjunto $\{f \in K \mid ord_P(f) \geq -n_P;\ \forall P \in X\}$, donde $D = \sum n_P P$.

Observemos que una función racional f pertenece a $L(D)$ si $div(f) + D \succ 0$, o bien, si $f = 0$.

Proposición 4.2.1. *El conjunto $L(D)$ constituye un espacio vectorial sobre k. Designamos por $\ell(D)$ a la dimensión de $L(D)$.*

Demostración. Observemos que para todo $\lambda \in k$, si $f \in L(D)$, entonces $div(\lambda f) + D = div(\lambda) + div(f) + D = div(f) + D \succ 0$, por consecuencia del Corolario 4.1.1, con lo que concluimos que $\lambda f \in L(D)$. Ahora veamos que, si $f_1, f_2 \in L(D)$, entonces $ord_P(f_1 + f_2) \geq$ mín$[ord_P(f_1), ord_P(f_2)] \geq -n_P$ para todo $P \in X$, y dado por cómo se definió ord_P tenemos que si $ord_P(f) \geq -n_P$ entonces $ord_P(-f) \geq -n_P$. Con esto tenemos un candidato a ser espacio vectorial, pues $L(P)$ es un subgrupo de K y tenemos definida una multiplicación por escalar. Como $k \subset K$ es un subcampo, entonces se cumplen que $\lambda(f_1+f_2) = \lambda f_1 + \lambda f_2$, $(\lambda_1 + \lambda_2)f = \lambda_1 f + \lambda_2 f$, $\lambda_1(\lambda_2 f) = (\lambda_1\lambda_2)f$, y $1f = f$, para todo $\lambda_1, \lambda_2, \lambda \in k$ y $f, f_1, f_2 \in K$. Con lo que la proposición es cierta. ∎

La siguiente proposición muestra que $\ell(D)$ es finita.

Proposición 4.2.2. (1) *Si $D \prec D'$, entonces $L(D) \subset L(D')$, y $dim_k(L(D')/L(D)) \leq gr(D' - D)$.*

(2) *$L(0) = k$; $L(D) = 0$ si $gr(D) < 0$.*

(3) *$L(D)$ es de dimensión finita para todo D. Si $gr(D) \geq 0$, entonces $\ell(D) \leq gr(D)+1$.*

(4) *Si $D \equiv D'$, entonces $\ell(D) = \ell(D')$.*

Demostración. (1): $D' = D+P_1+\ldots+P_s$ y $L(D) \subset L(D+P_1) \subset \ldots \subset L(D+P_1+\ldots+P_s)$, entonces es suficientes probar que $dim(L(D + P)/L(D)) \leq 1$. Para comprobarlo, sea t el parámetro de uniformización de $\mathcal{O}_P(X)$, y sea $r = n_P$ el coeficiente de P en D. Definimos $\varphi : L(D + P) \to k$ por $\varphi(f) = (t^{r+1}f)(P)$; como $ord_P(f) \geq -r - 1$, está bien definido. φ es una aplicación lineal, y $Ker(\varphi) = L(D)$, luego φ induce una aplicación uno a uno

$\widetilde{\varphi}: L(D+P)/L(D) \to k$ que da el resultado.

(2): Por el Corolario 4.1.1, tenemos que si $0 \neq f \in K$ es tal que $div(f) \succ 0$ entonces $f \in k$, por lo que $L(0) = k$. Supongamos que $gr(D) < 0$, sea $f \in L(D)$ no nulo, entonces $div(f) + D \succ 0$, pero $gr(div(f) + D) = gr(div(f)) + gr(D) \geq 0$, por la Proposición 4.1.1 tenemos que $gr(div(f)) = 0$ por lo que $gr(D) \geq 0$, lo cual contradice la hipótesis, por lo tanto $f = 0$.

(3): Si $gr(D) = n \geq 0$, elegimos $P \in X$, y consideramos $D' = D - (n+1)P$. Entonces, por (2) tenemos que $L(D') = 0$, y por (1) tenemos que $dim(L(D)/L(D')) \leq n+1$, por lo tanto $\ell(D) \leq n+1$.

(4): Supóngase que $D' = D + div(g)$. Definimos $\psi: L(D) \to L(D')$ por $\psi(f) = fg$. ψ es un isomorfismo de espacios vectoriales, por tanto $\ell(D) = \ell(D')$. ■

Podemos dar una generalidad de los conceptos abarcados en éste capítulo.

Definición 4.2.2. Para todo subconjunto S de X, y todo divisor $D = \sum n_P P$ de X, definimos $gr^S(D) = \sum_{P \in S} n_P$, y $L^S(D) = \{f \in K \mid ord_P(f) \geq -n_P;\ \forall P \in S\}$.

Lema 4.2.1. *Si $D \prec D'$, entonces $L^S(D) \subset L^S(D')$. Además, si S es finito, entonces $dim_k(L^S(D')/L^S(D)) = gr^S(D' - D)$.*

Demostración. Procediendo como en la Proposición 4.2.2, supondremos que $D' = D + P$, y definimos $\varphi: L^S(D+P) \to k$, por el mismo camino. Debemos probar que φ aplica $L^S(D+P)$ sobre k, es decir, $\varphi \neq 0$, por lo tanto $\widetilde{\varphi}$ es un isomorfismo. Entonces debemos encontrar un $f \in K$ con la propiedad de que $ord_P(f) = -r-1$, y $ord_Q(f) \geq -n_Q$ para todo $Q \in S$. Pero esto sabemos que lo podemos hacer gracias a que S es finito, y usando la Proposición 3.2.3. ■

La siguiente proposición es un primer paso importante para el cálculo de las dimensiones $\ell(D)$.

Proposición 4.2.3. *Sea $x \in K$, $x \notin k$. Sea $(x)_0$ el divisor de los ceros de x, y sea $n = [K : k(x)]$. Entonces*

(1) *$(x)_0$ es un divisor efectivo de grado n.*

(2) *Existe una constante τ tal que $\ell(r(x)_0) \geq rn - \tau$ para todo r.*

Demostración. Sea $Z = (x)_0 = \sum n_P P$, y sea $m = gr(Z)$. Ante todo probaremos que $m \leq n$.

Sea $S = \{P \in X \mid n_P > 0\}$ y elegimos $v_1, \ldots, v_m \in L^S(0)$ tales que las clases laterales $\overline{v}_1, \ldots, \overline{v}_m \in L^S(0)/L^S(-Z)$ formen una base de este espacio vectorial (Lema 4.2.1). Probaremos que $v_1, \ldots, v_m$ son linealmente independientes sobre $k(x)$. Si no (quitando denominadores y multiplicando por una potencia de x), obtendríamos polinomios $g_i = \lambda_i + xh_i \in k[x]$ con $\sum g_i v_i = 0$, y no todos los $\lambda_i = 0$. Pero entonces $\sum \lambda_i v_i = -x \sum h_i v_i \in L^S(-Z)$, por lo tanto $\sum \lambda_i \overline{v}_i = 0$, lo cual es absurdo. Luego $m \leq n$. A continuación probaremos (2).

Sean $w_1, \ldots, w_n$ una base de K sobre $k(x)$, pues K es algebraico sobre $k(x)$. Podemos suponer que cada w_i satisface una ecuación del tipo $w_i^{n_i} + a_{i1} w_i^{n_i - 1} + \ldots = 0$, con $a_{ij} \in k[x^{-1}]$. Entonces $ord_P(a_{ij}) \geq 0$ si $P \notin S$. Si $ord_P(w_i) < 0$, $P \notin S$, entonces $ord_P(w_i^{n_i}) < ord_P(a_{ij} w_i^{n_i - j})$, que es imposible por la Proposición 1.1.5. Se sigue entonces que para un cierto $t > 0$, $div(w_i) + tZ \succ 0$, $i = 1, \ldots, n$. Entonces $w_i x^{-j} \in L((r+t)Z)$ para $i = 1, \ldots, n$, y $j = 0, 1, \ldots, r$. Como los w_i son independientes sobre $k(x)$, y $1, x^{-1}, \ldots, x^{-r}$ son independientes sobre k, $\{w_i x^{-j} \mid i = 1, \ldots, n;\ j = 0, \ldots, r\}$ son independientes sobre k. Por lo tanto $\ell((r+t)Z) \geq n(r+1)$. Pero $\ell((r+t)Z) = \ell(rZ) + dim(L((r+t)Z)/L(rZ)) \leq \ell(rZ) + tm$ por la Proposición 4.2.2 (1). En consecuencia $\ell(rZ) \geq n(r+1) - tm = rn - \tau$, como deseábamos.

Finalmente, como $rn - \tau \leq \ell(rZ) \leq rm + 1$ (Proposición 4.2.2 (3)), si elegimos r suficientemente grande, vemos que $n \leq m$, lo que prueba (1). ■

Corolario 4.2.1. *Las siguientes proposiciones son equivalentes:*

(i) *C es racional. (ver Definición 3.1.12)*

(ii) *X es isomorfo a $\mathbb{P}^1$.*

(iii) *Existe un $x \in K$ con $gr((x)_0) = 1$.*

(iv) *Para algún $P \in X$, es $\ell(P) > 1$.*

Proposición 4.2.4. *Si $D \prec D'$, entonces $\ell(D') \leq \ell(D) + gr(D' - D)$, es decir,*

$$gr(D) - \ell(D) \leq gr(D') - \ell(D').$$

Demostración. Del álgebra lineal sabemos que si V' es un subespacio de un k–espacio vectorial finito V, entonces $dim_k(V/V') = dim_k(V) - dim_k(V')$.

Sean D, D' divisores tales que $D \prec D'$. Por la Proposición 4.2.2 sabemos que

$$dim_k(L(D')/L(D)) \leq gr(D' - D),$$

y como $L(D)$ es subespacio de $L(D')$, ambos de dimensión finita, tenemos entonces que

$$dim_k(L(D')/L(D)) = dim_k(L(D')) - dim_k(L(D)) = \ell(D') - \ell(D),$$

de donde concluimos que

$$\ell(D') - \ell(D) \leq gr(D' - D)$$

■

Proposición 4.2.5. *Sea D un divisor, entonces $\ell(D) > 0$ si y sólo si D es linealmente equivalente a un divisor efectivo.*

Demostración. Sea D un divisor tal que $\ell(D) > 0$, entonces $L(D) \neq \{0\}$, sea entonces $z \in L(D)$ no nulo. Tenemos que $div(z) + D \succ 0$, sea $D' = div(z) + D$, y claramente $D' \equiv D$; además D' es efectivo.

Ahora supongamos que $D \equiv D'$, con $D' \succ 0$, entonces existe $z \in K$ no nulo, tal que $D' = D + div(z) \succ 0$, entonces $div(z) \succ -D$, con lo que tenemos que $z \in L(D)$, con $z \neq 0$, por tanto $\ell(D) \neq 0$, y por último $\ell(D) > 0$. ■

Proposición 4.2.6. *Supongamos que $\ell(D) > 0$, y sea $f \neq 0$, $f \in L(D)$. Entonces $f \notin L(D - P)$ para todo P salvo un número finito. Por lo tanto, $\ell(D - P) = \ell(D) - 1$ para todo P, salvo un número finito.*

Demostración. Sea D un divisor, tal que $\ell(D) > 0$, y sea $f \in L(D)$ no nulo. En virtud de la Proposición 4.2.6, podemos considerar a D como un divisor efectivo. Supongamos que $f \in L(D - P)$ para todo $P \in X$, excepto para un número finito, entonces $f \in L(D)$, lo que implica que $ord_P(f) \geq -n_P$ para todo $P \in X$, análogamente $f \in L(D - P) \Rightarrow ord_P(f) \geq -n_P + 1$, para casi todo $P \in X$.

De estas dos desigualdades tenemos que $ord_P(f) > -n_P$ para casi todo $P \in X$. Como $n_P = 0$ para casi todo $P \in X$, entonces $ord_P(f) > 0$ para casi todo $P \in X$, entonces f tiene una infinidad de ceros, pero un número finito de polos, pero al ser f una función racional, gracias a la Proposición 4.1.1, entonces f debe tener igual cantidad de polos que de ceros, lo que nos lleva a una contradicción; por lo tanto $f \in L(D)$, y $f \notin L(D - P)$ para todo P excepto un número finito. ■

4.3. Teorema de Riemann

Si D es un divisor grande, entonces $L(D)$ también lo es. La Proposición 4.2.3 lo prueba para un tipo especial de divisores.

Teorema 4.3.1 (Riemann). *Existe una constante g tal que $\ell(D) \geq gr(D) + 1 - g$ para todos los divisores D. El menor de tales g se denomina género de X (o de K, o de C), y g es un entero no negativo.*

Demostración. Para cada D, sea $S(D) = gr(D) + 1 - \ell(D)$. Deseamos encontrar un g tal que $S(D) \leq g$ para todo D.

(i) $S(0) = 0$, por lo tanto $g \geq 0$, sí existe.

(ii) Si $D \equiv D'$, entonces $S(D) = S(D')$ (Proposiciones 4.1.2 y 4.2.2).

(iii) Si $D \prec D'$, entonces $S(D) \leq S(D')$ (Proposición 4.2.4).

Sea $x \in K$, $x \notin k$, y $Z = (x)_0$, y sea τ el menor entero que verifica la Proposición 4.2.3 (2). Como $S(rZ) \leq \tau + 1$ para todo r, y como $rZ \prec (r+1)Z$, deducimos de (iii) que:

(iv) $S(rZ) = \tau + 1$ para todo $r > 0$ suficientemente grande.

Sea $g = \tau + 1$. Para terminar la demostración, bastará probar (gracias a (ii) y (iii)) que:

(v) Para todo divisor D, existe un divisor $D' \equiv D$, y un entero $r \geq 0$ tal que $D' \prec rZ$.

Para probarlo, sea $Z = \sum n_P P$, $D = \sum m_P P$. Deseamos que $D' = D - div(f)$, entonces necesitamos que $m_P - ord_P(f) \leq r n_P$ para todo P. Sea $y = x^{-1}$, y $T = \{P \in X \mid m_P > 0 \text{ y } ord_P(y) \geq 0\}$. Sea $f = \prod_{P \in T} (y - y(P))^{m_P}$. Entonces $m_P - ord_P(f) \leq 0$ siempre que $ord_P(y) \geq 0$. Si $ord_P(y) < 0$, entonces $n_P > 0$, luego un r suficientemente grande hará que se verifique. ∎

Corolario 4.3.1. *Si $\ell(D_0) = gr(D_0)+1-g$, y $D \equiv D' \succ D_0$, entonces $\ell(D) = gr(D)+1-g$.*

Corolario 4.3.2. *Si $x \in K$, $x \notin k$, entonces $g = gr(r(x)_0) - \ell(r(x)_0) + 1$ para todo r suficientemente grande.*

Corolario 4.3.3. *Existe un entero N tal que para todo divisor D de grado mayor que N, $\ell(D) = gr(D) + 1 - g$.*

Demostración. Sea D_0 tal que $\ell(D_0) = gr(D_0) + 1 - g$, y sea $N = gr(D_0) + g$. Entonces si $gr(D) \geq N$, $gr(D - D_0) + 1 - g > 0$, y, por el Teorema 4.3.1 de Riemman, $\ell(D - D_0) > 0$. Por lo tanto $D - D_0 + div(f) \succ 0$ para un cierto f, es decir, $D \equiv D + div(f) \succ D_0$, y entonces el resultado se sigue del Corolario 4.3.1. ■

La utilidad del Teorema de Riemann depende de que sea posible calcular el género de una curva. Por su misma definición, el género depende sólo del modelo no-singular, o del campo de funciones, por lo tanto, dos curvas birracionalmente equivalentes tiene el mismo género. Debido a que es posible encontrar una curva plana que sólo posea puntos múltiples ordinarios que además sea birracionalmente equivalente a una curva dada[1], la proposición siguiente es todo lo que necesitamos:

Proposición 4.3.1. *Sea $\mathcal{C}$ una curva plana que sólo posea puntos múltiples ordinarios. Sea n el grado de $\mathcal{C}$, $r_P = m_P(\mathcal{C})$. Entonces el género g de $\mathcal{C}$ está dado por la fórmula*

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in \mathcal{C}} \frac{r_P(r_P - 1)}{2}.$$

Demostración. Por el Corolarios 4.3.3, necesitamos encontrar un divisor "grande" D para que podamos calcular $\ell(D)$. El Teorema 4.1.1 nos permite encontrar todos los divisores efectivos linealmente equivalentes a ciertos divisores D. Estas dos observaciones conducen al cálculo de g.

Podemos suponer que la recta $Z = 0$ corta a $\mathcal{C}$ en n puntos distintos $P_1, \ldots, P_n$, y se designa por F al polinomio homogéneo que define a $\mathcal{C}$.

Sean $E = \sum_{Q \in X} (r_Q - 1)Q$, $r_Q = r_{f(Q)} = m_{f(Q)}(\mathcal{C})$ como en la sección 1 de este capítulo; y sea $E_m = m\sum_{i=1}^{n} P_i - E$. E_m es un divisor de grado $mn - \sum_{P \in \mathcal{C}} r_P(r_P - 1)$.

Consideremos $V_m = \{$polinomios homogéneos G de grado m tales que G sea adjunto de $\mathcal{C}\}$. Como G es adjunta si y sólo si $m_P(G) \geq r_P - 1$ para todo $P \in \mathcal{C}$, podemos aplicar el Teorema 2.3.1 para calcular la dimensión de V_m. Encontramos que $dim(V_m) \geq \frac{(m+1)(m+2)}{2} - \sum \frac{r_P(r_P-1)}{2}$, y la igualdad se cumple si m es grande. (Nótese que V_m es el espacio vectorial de los polinomios homogéneos, no el espacio proyectivo de las curvas).

Sea $\varphi : V_m \to L(E_m)$ definido por $\varphi(G) = G/Z^m \in K$. φ es una aplicación lineal, y $\varphi(G) = 0$ si y sólo si G es divisible por F.

Veamos que φ es exhaustiva. Si $f \in L(E_m)$, se puede escribir $f = R/S$, donde R y S son polinomios homogéneos del mismo grado. Entonces $div(RZ^m) \succ div(S) + E$. Por la

[1] El método utilizado es el de las Transformaciones Cuadráticas, y se puede consultar en [4] Fulton W., *Algebraic Curves*, Capítulo 7, sección 4, pág. 171-177.

Proposición 3.2.2, existe una ecuación $RZ^m = AS + BF$. Luego $R/S = A/Z^m$ en $k(F)$, y por lo tanto $\varphi(A) = f$. (Nótese que $div(A) = div(RZ^m) - div(S) \succ E$, luego $A \in V_m$).

Esto prueba que la siguiente sucesión de espacios vectoriales es exacta:

$$0 \longrightarrow W_{m-n} \xrightarrow{\psi} V_m \xrightarrow{\varphi} L(E_m) \longrightarrow 0$$

donde W_{m-n} es el espacio de todas los polinomios homogéneos de grado $m-n$ y $\psi(H) = FH$ para $H \in W_{m-n}$.

Por la Proposición 1.3.15, podemos calcular $dim(L(E_m))$, por lo menos para m grande. Resulta, pues, que

$$\ell(E_m) = gr(E_m) + 1 - \left(\tfrac{(n-1)(n-2)}{2} - \sum \tfrac{r_P(r_P-1)}{2} \right)$$

para m grande. Pero como $gr(E_m)$ crece con m, aplicamos el Corolario 4.3.3 del Teorema de Riemann y termina la demostración. ■

Corolario 4.3.4. (i): *Con E_m definido como en la demostración de la Proposición 4.3.1, toda $h \in L(E_m)$ se puede escribir $h = H/Z^m$, donde H es una forma adjunta de grado m.*

(ii): $gr(E_{n-3}) = 2g - 2$. *Además* $\ell(E_{n-3}) \geq g$.

Demostración. La demostración se sigue de la sucesión exacta construida en la demostración de la Proposición 4.3.1. Nótese que si $m < n$, entonces $V_m = L(E_m)$. ■

4.4. Derivadas y diferenciales

Esta sección contiene las nociones algebraicas necesarias para estudiar diferenciales sobre una curva.

Definición 4.4.1. Sea R un anillo que contenga a k, y sea M un $R-$módulo. Una *derivación de R en M sobre k* es una aplicación $k-$lineal $D : R \to M$ tal que

$$D(xy) = xD(y) + yD(x)$$

para todo $x, y \in R$.

De esta definición se sigue que para todo

$$F \in k[X_1, \ldots, X_n] \text{ y } x_1, \ldots, x_n \in R,\ D(F(x_1, \ldots, x_n)) = \sum_{i=1}^{n} F_{X_i}(x_1, \ldots, x_n) D(x_i).$$

Como k está en todos los anillos, omitiremos la frase "sobre k".

Lema 4.4.1. *Si R es un dominio cuyo campo de cocientes es K, y M un espacio vectorial sobre K, entonces toda derivación $D : R \to M$ se extiende de forma única a una derivación $\widetilde{D} : K \to M$.*

Demostración. Sea $z \in K$, $z = x/y$, con $x, y \in R$, entonces como $x = yz$, debemos tener que $Dx = y\widetilde{D}z + zDy$, de donde $\widetilde{D}(z) = y^{-1}(Dx - zDy)$, lo que prueba la unicidad. Si definimos $\widetilde{D}$ por esta fórmula, no es difícil verificar que $\widetilde{D}$ está bien definida como derivación de K en M. ∎

Deseamos definir diferenciales de R de modo que sean elementos de la forma $\sum x_i\, dy_i$, con $x_i, y_i \in R$, y que se comporten como las diferenciales del cálculo.

Esta definición se puede dar de una manera más fácil, que se expone a continuación:

Para cada $x \in R$ sea $[x]$ un símbolo y se considera el $R-$módulo libre F sobre el conjunto $\{[x] \mid x \in R\}$. Sea N el submódulo de F generado por los siguientes elementos:

(i): $\{[x+y] - [x] - [y] \mid x, y \in R\}$

(ii): $\{[\lambda x] - \lambda[x] \mid x \in R,\ \lambda \in k\}$

(iii): $\{[xy] - x[y] - y[x] \mid x, y \in R\}$

Se designa con $\Omega_k(R) = F/N$ el módulo cociente. Sea dx la clase residual de $[x]$ en F/N, y $d : R \to \Omega_k(R)$ la función que aplica x en dx. $\Omega_k(R)$ es un $R-$módulo, que llamaremos el *módulo de las diferenciales* de R sobre k, y $d : R \to \Omega_k(R)$ es una derivación.

Lema 4.4.2. *Para todo R–módulo M, y toda derivación $D : R \to M$, existe un homomorfismo único de R–módulos $\varphi : \Omega_k(R) \to M$ tal que $D(x) = \varphi(dx)$ para todo $x \in R$.*

Demostración. Si definimos $\varphi' : F \to M$ por $\varphi'(\sum x_i[y_i]) = \sum x_i D(y_i)$, entonces $\varphi'(N) = 0$, luego φ' induce un $\varphi : \Omega_k(R) \to M$. ∎

Si $x_1, \ldots, x_n \in R$, y $G \in k[X_1, \ldots, X_n]$, entonces

$$d(G(x_1, \ldots, x_n)) = \sum_{i=1}^{n} G_{X_i}(x_1, \ldots, x_n) dx_i.$$

Esto prueba que si $R = k[x_1, \ldots, x_n]$, entonces $\Omega_k(R)$ es generado (como R–módulo) por $dx_1, \ldots, dx_n$.

Análogamente, si R es un dominio con campo de cocientes K, y $z = x/y \in K$, $x, y \in R$, entonces $dz = y^{-1}dx - y^{-1}zdy$. En particular, si $K = k(x_1, \ldots, x_n)$, entonces $\Omega_k(R)$ es un subespacio vectorial de dimensión finita sobre K, generado por $dx_1, \ldots, dx_n$.

Proposición 4.4.1. (1): *Sea K un campo de funciones algebraicas de una variable sobre k. Entonces $\Omega_k(K)$ es un espacio vectorial de dimensión uno sobre K.*

(2): *Si $x \in K$, $x \notin k$ (con k de característica 0), entonces dx es una base de $\Omega_k(K)$ sobre K.*

Demostración. Sea $F \in k[X, Y]$ una curva afín plana con campo de funciones K (se puede tomar así gracias a la Proposición 3.1.2), y sea $R = k[X, Y]/\langle F \rangle = k[x, y]$; $K = k(x, y)$. Podemos suponer que $F_Y \neq 0$, por lo tanto F no divide a F_Y (ya que F es irreducible), es decir, $F_Y(x, y) \neq 0$. La discusión previa a la proposición prueba que dx y dy generan $\Omega_k(K)$ sobre K. Pero $0 = d(F(x, y)) = F_X(x, y)dx + F_Y(x, y)dy$, luego $dy = udx$, donde $u = -F_X(x, y)F_Y(x, y)^{-1}$. Por lo cual dx genera $\Omega_k(K)$, luego $dim_K(\Omega_k(K)) \leq 1$.

Por lo tanto debemos probar que $\Omega_k(K) \neq 0$. Por los Lemas 4.4.1 y 4.4.2, bastará encontrar una derivación no nula $D : R \to M$ para algún espacio vectorial M sobre K. Sea $M = K$, llamemos $\overline{G}$ a la imagen en R de $G \in K[X, Y]$, y se considera $D(\overline{G}) = G_X(x, y) - uG_Y(x, y)$. Verifiquemos que D es una derivación bien definida, y que $D(x) = 1$, por lo que $D \neq 0$. ∎

De esta proposición se sigue que para todo $f, t \in K$, y $t \notin k$ (con k de característica 0), existe un elemento único $v \in k$ tal que $df = vdt$. Es natural escribir $v = \frac{df}{dt}$, y llamar a v la *derivada* de f con respecto de t.

Proposición 4.4.2. *Sea K como en la Proposición 4.4.1, $\mathcal{O}$ un anillo de K de valuación discreta, y t un parámetro de uniformización de $\mathcal{O}$. Si $f \in \mathcal{O}$, entonces $\frac{df}{dt} \in \mathcal{O}$.*

Demostración. Utilizando la notación de la demostración de la Proposición 4.4.1, podemos suponer que $\mathcal{O} = \mathcal{O}_P(F)$ y $P = (0,0)$ un punto simple de F. Para $z \in K$, escribamos z' en vez de $\frac{dz}{dt}$, t fijo a lo largo de toda la demostración.

Elijamos N suficientemente grande para que $ord_P(x) \geq -N$, $ord_P(y') \geq -N$. Entonces si $f \in R = k[x,y]$, $ord_P(f') \geq -N$, ya que $f' = f_X(x,y)x' + f_Y(x,y)y'$.

Si $f \in \mathcal{O}$, escribimos $f = g/h$, con $g, h \in R$ y $h(P) \neq 0$. Entonces $f' = h^{-2}(hg' - gh')$, luego $ord_P(f') \geq -N$.

Ahora estamos en condiciones de acabar la demostración. Sea $f \in \mathcal{O}$, y escribamos $f = \sum_{i<N} \lambda_i t^i + t^N g$, con $\lambda_i \in k$, $g \in \mathcal{O}$ (esto se puede por la Proposición 1.1.6). Entonces $f' = \sum i\lambda_i t^{i-1} + gNt^{N-1} + t^N g'$. Como $ord_P(g') \geq -N$, cada uno de los términos pertenece a $\mathcal{O}$, luego $f' \in \mathcal{O}$, como se quería. ■

4.5. Divisores canónicos

Sea C una curva proyectiva, X su modelo no-singular, K su campo de funciones como antes. Sea $\Omega = \Omega_k(K)$ el espacio de las diferenciales de K sobre k; los elementos $\omega \in \Omega$ también se pueden llamar *diferenciales* en X o en C.

Definición 4.5.1. Sea $\omega \in \Omega$, $\omega \neq 0$, y $P \in X$ un lugar. Definimos el *orden* de ω en P, $ord_P(\omega)$, como sigue. Sea t un parámetro de uniformización de $\mathcal{O}_P(X)$; escribamos $\omega = fdt$, $f \in K$. Se define $ord_P(\omega) = ord_P(f)$.

Para ver que esta definición no depende de la elección del parámetro de uniformización, sea u otro parámetro tal que $fdt = gdu$, entonces $f/g = \frac{du}{dt} \in \mathcal{O}_P(X)$ por la Proposición 4.4.2, y como también se tiene que $g/f \in \mathcal{O}_P(X)$, entonces $ord_P(f) = ord_P(g)$.

Definición 4.5.2. Si $0 \neq \omega \in \Omega$, se define el *divisor* de ω, $div(\omega)$, por $\sum_{P \in X} ord_P(\omega)$.

En la Proposición 4.5.1 probaremos que sólo un número finito verifica $ord_P(\omega) \neq 0$ para un ω dado, por lo que la definición del $div(\omega)$ es correcta.

Definición 4.5.3. Sea $W = div(\omega)$. W se denomina el *divisor canónico*.

Si ω' es otra diferencial no nula de Ω, entonces $\omega' = f\omega$, $f \in K$, luego $div(\omega') = div(f) + div(\omega)$, y por tanto $div(\omega') \equiv div(\omega)$. Recíprocamente, si $W \equiv W'$ pondremos que $W' = div(f) + W$, y entonces $W' = div(f\omega)$. Por lo tanto los divisores canónicas constituyen una clase de equivalencia respecto a la equivalencia lineal. En particular, todos los divisores canónicos tienen el mismo grado.

Proposición 4.5.1. *Supongamos que C es una curva plana de grado $n \geq 3$, y que sólo posea puntos múltiples ordinarios. Sea $E = \sum_{Q \in X} (r_Q - 1)Q$, como en la sección 4.1, y G una curva plana de grado $n-3$. Entonces $div(G) - E$ es un divisor canónico. (Si $n = 3$, entonces $div(G) = 0$).*

Demostración. Escojamos coordenadas X, Y, Z en $\mathbb{P}^2$ de tal forma que $Z \cdot C = \sum_{i=1}^{n} P_i$, con los P_i distintos; $(1,0,0) \notin C$; y que ninguna tangente a C en un punto múltiple pase por $(1,0,0)$. Se consideran $x = X/Z$, $y = Y/Z$ en K, y F el polinomio homogéneo que define a C, con $f_x = F_X(x,y,1)$ y $f_y = F_Y(x,y,1)$.

Sea $E_m = m\sum_{i=1}^{n} P_i - E$. Se considera $\omega = dx$. Como los divisores de la forma $div(G) - E$ tal que $gr(G) = n-3$, son linealmente equivalentes, bastará probar que $div(\omega) = E_{n-3} +$

$div(f_y)$. Como $f_y = F_Y/Z^{n-1}$, es lo mismo que probar:

$$div(dx) - div(F_Y) = -2\sum_{i=1}^{n} P_i - E. \tag{4.1}$$

Nótese primero que $dx = -(f_y/f_x)dy = -(F_Y/F_X)dy$, por lo tanto $ord_Q(dx) - ord_Q(F_Y) = ord_Q(dy) - ord_Q(F_X)$ para todo $Q \in X$.

Supongamos que Q es un lugar centrado en $P_i \in Z \cap \mathcal{C}$. Entonces $y^{-1} = Z/Y$ es un parámetro de uniformización de $\mathcal{O}_{P_i}(X)$, y $dy = -y^2 d(y^{-1})$, luego $ord_Q(dy) = -2$. Gracias a la Proposición 2.3.2, tenemos que $F_X(P_i) \neq 0$, y por tanto los dos miembros de la Ecuación 4.1 tienen orden -2 en Q.

Supongamos que Q es un lugar centrado en $P = (a, b, 1) \in \mathcal{C}$. Podemos suponer que $P = (0, 0, 1)$, ya que $dx = d(x - a)$, y las derivadas no cambian por traslación.

Consideremos el caso en que Y es tangente a $\mathcal{C}$ en P. Entonces P no es un punto múltiple (por hipótesis), por lo tanto x es un parámetro de uniformización, y $F_Y(P) \neq 0$. Además $ord_Q(dx) = ord_Q(F_Y) = 0$, como pretendíamos. Si Y no es tangente, entonces y es un parámetro de uniformización en Q, luego $ord_Q(dy) = 0$, y $ord_Q(f_x) = r_Q^{-1}$, como queríamos. ■

Corolario 4.5.1. *Sea W un divisor canónico. Entonces $gr(W) = 2g - 2$, y $\ell(W) \geq g$.*

Demostración. Podemos suponer que $W = E_{n-3}$. Entonces aplicamos el Corolario 4.3.4–(ii). ■

4.6. Teorema de Riemann-Roch

En este célebre teorema se determina el término que falta en la desigualdad del teorema de Riemann para transformarlo en igualdad. Nuestra demostración sigue la demostración clásica de Brill y Noether.

Lema 4.6.1 (Reducción de Noether). *Sea W un divisor canónico de X, $P \in X$, y D un divisor. Si $\ell(D) > 0$, y $\ell(W - D - P) \neq \ell(W - D)$, entonces $\ell(D + P) = \ell(D)$.*

Demostración. Escojamos C como antes con puntos múltiples ordinarios, y tal que P sea un punto simple C (Proposición 3.2.3), y por lo tanto $Z \cdot C = \sum_{i=1}^{n} P_i$, con los P_i distintos. Sea $E_m = m \sum P_i - E$. Los términos del enunciado del lema dependen sólo de las clases de equivalencia lineal de los divisores implicados, por lo tanto podemos suponer, gracias a las Proposiciones 4.5.1 y 4.2.5, que $W = E_{n-3}$, y $D \succ 0$. Luego $L(W - D) \subset L(E_{n-3})$.

Sea $h \in L(W - D)$, tal que $h \notin L(W - D - P)$. Escribamos $h = G/Z^{n-3}$, y G una adjunta de grado $n - 3$ (se sigue del Corolario 4.3.4). $div(G) = D + E + A$, con $A \succ 0$, pero $A \not\succ P$.

Tomemos una recta L tal que $L \cdot C = P + B$, donde B consta de $n - 1$ puntos simples de C, todos distintos de P. $div(LG) = (D + P) + E + (A + B)$.

Ahora supongamos $f \in L(D+P)$; sea $div(f)+D = D'$. Debemos probar que $f \in L(D)$, es decir, $D' \succ 0$.

Como $D + P \equiv D' + P$, y ambos divisores son efectivos, aplicamos el Teorema 4.1.1 (teorema del residuo), entonces existe una curva H de grado $n - 2$ tal que $div(H) = (D' + P) + E + (A + B)$.

Pero B contiene $n-1$ puntos distintos alineados, y H es una curva de grado $n-2$. Por el Teorema de Bézout, H debe contener a L como componente. En particular, $H(P) = 0$. Como P no está en $E + A + B$, se tiene que $D' + P \succ P$, o $D' \succ 0$, como se pretendía. ■

Teorema 4.6.1 (Riemann-Roch). *Sea W un divisor canónico de X. Entonces para todo divisor D, se tiene que*

$$\ell(D) = gr(D) + 1 + \ell(W - D). \tag{4.2}$$

Demostración. Antes de probar el teorema, obsérvese que conocemos ya este teorema para divisores de grado suficientemente elevado. Lograremos demostrar el caso general si podemos comparar los dos miembros de la Ecuación 4.2 para D y $P + D$, $P \in X$; obsérvese que $gr(D + P) = gr(D) + 1$, mientras que los otros dos términos no constantes cambian por 0 o por 1. El núcleo de la demostración es por tanto el Lema 4.6.1 (Lema de reducción de Noether).

Empecemos pues la demostración. Para cada divisor D, consideremos la ecuación:

$$\ell(D) = gr(D) + 1 - g + \ell(W - D). \tag{4.3}$$

Caso 1: $\ell(W - D) = 0$. Del Corolario 4.5.1 se sigue que $g \leq \ell(W)$, y de la Proposición 4.2.4 sabemos que $\ell(W) \leq \ell(W - D) + gr(D)$, entonces tenemos que $gr(D) \geq g$ en este caso. Por el Teorema 4.3.1 (Teorema de Riemann), $\ell(D) \geq gr(D) + 1 - g \geq 1$, y si la ecuación 4.3 fuera falsa sería $\ell(D) > 1$.

Probaremos este caso por inducción respecto a $\ell(D)$. Elijamos un P tal que $\ell(D - P) = \ell(D) - 1$ (Proposición 4.2.6). Si la ecuación 4.3 fuese falsa, entonces $\ell(D - P) > 0$, por lo tanto el Lema de reducción implicaría que $\ell(W - (D - P)) = 0$. Aplicando la hipótesis de inducción a $D - P$, obtenemos que $\ell(D - P) = gr(D - P) + 1 - g$, luego $\ell(D) = gr(D) + 1 - g$, que es precisamente 4.3.

Caso 2: $\ell(W - D) > 0$. Este caso sólo puede presentarse si $gr(D) \leq gr(W) = 2g - 2$ (Proposición 4.2.2–(ii)). Entonces podríamos elegir un D maximal para el cual la ecuación 4.3 sería falsa; es decir,

$$\ell(D + P) = gr(D + P) + 1 - g + \ell(W - D - P) \tag{4.4}$$

sería verdad para todo $P \in X$. Escojamos, gracias a la Proposición 4.2.6, un P tal que $\ell(W - D - P) = \ell(W - D) - 1$. Por el Lema 4.6.1, $\ell(D + P) = \ell(D)$. Como la ecuación 4.4 es verdad, tenemos $\ell(D) = \ell(D + P) = gr(D + P) + 1 - g + \ell(W - D - P) = gr(D) + 1 - g\ell(W - D)$, como queríamos. ■

De este teorema se deducen los corolarios que se enuncian a continuación; los primeros tres no se demostrarán pues se siguen directamente del teorema, y utilizando la Proposición 4.2.2.

Corolario 4.6.1. $\ell(W) = g$ *si* W *es un divisor canónico.*

Corolario 4.6.2. *Si* $gr(D) \geq 2g - 1$, *entonces* $\ell(D) = gr(D) + 1 - g$.

Corolario 4.6.3. *Si* $gr(D) \geq 2g$, *entonces* $\ell(D - P) = \ell(D) - 1$ *para todo* $P \in X$.

Corolario 4.6.4 (Teorema de Clifford). *Si* $\ell(D) > 0$, *y* $\ell(W - D) > 0$, *entonces* $\ell(D) \leq \frac{1}{2}gr(D) + 1$.

Demostración. Podemos suponer que $D \succ 0$, $D' \succ 0$, $D + D' = W$, y también que $\ell(D - P) \neq \ell(D)$, para todo P, ya que en otro caso se trabaja con $D - P$ y se consigue una desigualdad mejor.

Elegimos $g \in L(D)$ tal que $g \notin L(D-P)$ para cada $P \prec D'$. Entonces es fácil ver que la aplicación lineal $\varphi : L(D)/L(0) \to L(W)/L(D)$ definida por $\varphi(\overline{f}) = \overline{(f/g)}$ (las barras designan las clases laterales) es uno a uno. Además $\ell(D') - 1 \leq g - \ell(D)$. Aplicando el Teorema de Riemann-Roch a D' se acaba la demostración. ■

El término $\ell(W-D)$ puede ser además interpretado por medio de diferenciales. Sea D un divisor. Definimos $\Omega(D)$ como el conjunto $\{\omega \in \Omega \mid div(\omega) \prec D\}$, que es un subespacio vectorial de Ω (sobre k). Sea $\delta(D) = dim_k \Omega(D)$, el *índice de* D. Las diferenciales de $\Omega(0)$ se denominan *diferenciales de primera especie* (o diferenciales holomorfas, si $k = \mathbb{C}$).

Proposición 4.6.1. (1): $\delta(D) = \ell(W-D)$.

(2): *Existen* g *diferenciales linealmente independientes de primer orden sobre* X.

(3): $\ell(D) = gr(D) + 1 - g + \delta(D)$.

Demostración. Sea $W = div(\omega)$. Definimos una aplicación lineal $\varphi : L(W-D) \to \Omega(D)$ por $\varphi(f) = f\omega$. Tenemos que φ es un isomorfismo, que prueba (1). Las afirmaciones (2) y (3) se siguen ya inmediatamente. ■

Bibliografía

[1] Atiyah M. F., MacDonald I. G., *Introduction to Commutative Algebra*, Addison-Wesley, New York, 1994.

[2] Bourbaki N., *Elements of Mathematics: Commutative Algebra, Chapters 1-7*, Springer-Verlag, Berlin, 1989.

[3] Debarre O., *Higher-Dimensional Algebraic Geometry*, Springer-Verlag, New York, 2000.

[4] Fulton W., *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley, New York, 1969.

[5] Harris J., *Algebraic Geometry: A first course*, Springer-Verlag, New York, 1992.

[6] Hartshorne R., *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[7] Kunz E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.

[8] Li H., Van Oystaeyen F., *A Primer Of Algebraic Geometry: Constructive Computational Methods*, Marcel Dekker, New York, 2000.

[9] Matsumura H., *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986.

[10] Musili C., *Algebraic Geometry For Beginners*, Hindustan Book Agency, New Delhi, 2001.

[11] Samuel P., *Projective Geometry*, Springer-Verlag, New York, 1988.

[12] Sharp, R. Y., *Steps in commutative algebra*, Cambridge University, Cambridge, 2000.

[13] Silverman J.H., Tate J., *Rational Points on Elliptic Curves*, Springer–Verlag, New York, 1992.