Geometría Algebraica aplicada a códigos

Daniel Miguel Ortiz
Joel Nava Lara

17 de febrero de 2009

Índice general

Agradecimientos
Daniel Miguel Ortiz

A mis padres Don Esteban y Doña Reyna agradezco infinitamente el apoyo que me brindan en cada momento de mi vida, porque sin su amor, cariño y confianza no habría podido alcanzar este sueño.

Gracias Papá Gracias Mamá.

Agradezco a mis hermanos Diego, Jorge, Esteban y Carla Patricia que siempre me animan a seguir adelante.

A mis amigos de la licenciatura de los cuales tengo locos recuerdos y fabulosas aventuras.

Al profesor Raúl De la Torre gracias sensei.

Al Dr. Manuel Gonzales por el apoyo para la realización de este trabajo.

Asimismo deseo agradecer al Dr. Carlos Rentería por el apoyo, la paciencia y la dedicación que nos bríndo en la realización de este trabajo. Gracias Maestro.

Agradecimientos
Joel Nava Lara

Agradezco a mis padres por todo lo que me han brindado, en especial por su cariño y apoyo incondicional a lo largo de mi vida.

Asi mismo quiero agradecer a mi hermana, a mis abuelos y mi familia en general.

A Yesica por su cariño y paciencia todo este tiempo.

A mis amigos un agradecimiento por su compañia y animos durante mi carrera.

A mis profesores, en particular al Dr. Carlos Rentería quien me ha guiado en estos ultimos años por un camino que sigo recorriendo, tambien al Dr. Manuel Gonzales por su apoyo, comprension y paciencia a los largo del trabajo de esta tesis.

Por ultimo quiero dedicar el trabajo y esfuerzo que se empleo en esta tesis a mis padres por sus 25 años de matrimonio, a mis abuelas Doña Luisa y Doña Tere . A todos ellos les debo mi mas grande amor, respeto y cariño.

Introducción

El estudio de la geometría algebraica surge de implementar herramientas del álgebra abstracta, en mayor medida el álgebra conmutativa, a temas relacionados con la geometría. Algunos de estos temas se relacionan con ceros de polinomios en varias variables, el espacio afín y el espacio proyectivo.

Historicamente se desarrolla a principios del siglo veinte con la escuela italiana, ofreciendo un estudio más intuitivo y un tanto carente del rigor moderno. Después, en la década de los 30, los matemáticos Oscar Zariski y André Weil comienzan a fundamentar la geometría algebraica sobre el álgebra conmutativa, desarrollada fuertemente por Hilbert, Max Noether, Emmy Noether, Emanuel Lasker, Wolfgang Krull y otros matemáticos. Para la década de los cincuentas Jean-Pierre Serre y Alexander Grothendieck rehacen la fundamentación sobre la teoria de haces, para más tarde encontrar las ideas de esquemas y el álgebra homológica.

Por su parte la teoría de códigos comienza formálmente a mediados del siglo veinte, cuando se presenta un auge en las comunicaciones, y se desarrolla principálmente en los laboratorios Bell, donde trabajó Claude E. Shannon. Claude E. Shannon publicó en 1948 un artículo llamado "*A mathematical theory of communication*", presentando las bases de lo que hoy se conoce como teoría de la información, tomando en cuenta compresión de datos, canales de transmisión, criptografía, etc.

Para 1950 Richard Hamming desarrolla varios códigos distintos a los de repetición, dando definiciones tales como distancia entre dos palabras y peso de una palabra, que además eran capaces de detectar y corregir errores en mayor proporción que los códigos de repetición.

El propósito de esta tesis es presentar una introducción a la geometría algebraica y a la teoría de códigos, en el último caso, enfocada a los que se obtienen a partir de curvas algebraicas.

En el primer capítulo, el más extenso, presentamos las herramientas necesarias para el desarrollo básico de códigos geométrico algebraicos, estas herramientas se encuentran en los primeros capítulos de cualquier libro de geometría algebraica y forman parte del conocimiento "clásico" de esta area. Se omiten las demostraciones de los primeros teoremas y proposiciones, dando en su lugar la referencia donde se encuentran, por el contrario las demostraciones de los teoremas y proposiciones importantes, que se encuentran de la mitad del capítulo en cuestión en adelante, se presentan con un detalle razonable para un estudiante de licenciatura en matemáticas.

El segundo capítulo dá las bases para la teoría de códigos y presenta algunos algoritmos para la construcción explícita de varios de ellos, así mismo presenta algunos teoremas de gran utilidad para el cálculo de los parámetros de cada uno.

En el tercer y último capítulo se encuentra el estudio de algunas curvas, conocidas en la geometría algebraica por sus propiedades, se calculan los elementos necesarios para la construcción de un código a partir de cada una de ellas y después se utilizan los algoritmos del capítulo 2 para construir los códigos correspondientes calculando sus parámetros de definición.

Capítulo 1

Geometría Algebraica

1.1. Preliminares

Cuando hablemos de un anillo, nos referiremos a anillos conmutativos con elemento identidad. Un homomorfismo entre dos anillos deberá mandar la unidad del primero a la unidad del segundo. Un dominio, o dominio entero, es un anillo (con dos elementos por lo menos) que posee la ley de cancelación. Un campo es un dominio en el que cada elemento distinto de cero es unitario, es decir posee inverso respecto a la multiplicación.

$\mathbb{Z}$ designa el dominio de los enteros, mientras que $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ designan a los campos racionales, reales y complejos, respectivamente. Un dominio R posee un campo de fracciones K. K es un campo que contiene a R como subanillo, y todo elemento de K se puede escribir (no necesariamente de forma única) como cociente de dos elementos de R. Todo homomorfismo de anillos uno a uno, de R en un campo L, se extiende de modo único a un homomorfismo de anillos de K en L. Todo homomorfismo de anillos de un campo en un anillo es uno a uno.

Para todo anillo R, $R[X]$ designa el anillo de polinomios con coeficientes en R y variable X. El grado de un polinomio $\sum a_i X^i$ es el mayor entero d tal que $a_d \neq 0$; el polinomio se llama mónico si $a_d = 1$.

El anillo de polinomios en n variables sobre R se designa por $R[X_1, ..., X_n]$. Escribiremos $R[X, Y]$ o $R[X, Y, Z]$ cuando $n = 2$ ó $n = 3$. Los monomios de $R[X_1, ..., X_n]$ son los polinomios $X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$, con cada i_j entero no negativo; el grado del monomio es $i_1 + i_2 + \cdots + i_n$.

Todo elemento F de $R[X_1, ..., X_n]$ se puede expresar de manera única como $F = \sum a_{(i)} X^{(i)}$ donde los $X^{(i)}$ son monomios, $a_{(i)} \in R$.

F es homogéneo, o una forma, de grado d, si los coeficientes, salvo quizá los pertenecientes a monomios de grado d, son todos cero. Todo polinomio F tiene expresión única de la forma $F = F_0 + F_2 + \cdots + F_d$, donde F_i es una forma de grado i; si $F_d \neq 0$, d es el grado de F, y se escribe grad(F). Los términos $F_0, F_1, F_2, ...$ se denominan términos constante, lineal, cuadrático, etc. de F.

F es constante si $F = F_0$. Si R es un dominio, grad(FG) = grad(F) + grad(G). R es un subanillo de $R[X_1, ..., X_n]$, y $R[X_1, ..., X_n]$ se caracteriza por la siguiente propiedad: si φ es un homomorfismo de anillos de R en un anillo S, y $s_1, ..., s_n \in S$,entonces existe una extensión única de φ en un homomorfismo de anillos $\widetilde{\varphi}$ de $R[X_1, ..., X_n]$ en S tal que $\widetilde{\varphi}(X_i) = s_i$, $i = 1, ..., n$. La imagen de F por $\widetilde{\varphi}$ se indica por $F(s_1, ..., s_n)$. $R[X_1, ..., X_n]$ es canónicamente isomorfo a $R[X_1, ..., X_{n-1}][X_n]$.

Un elemento a de un anillo R se llama irreducible si toda descomposición de el es de la forma $a = bc$, $b, c \in R$, con b o c unidades. Un dominio R es de factorización única, abreviado DFU, si todo elemento no nulo de R se descompone de modo único, salvo unidades y salvo el orden de los factores, en elementos irreducibles.

Si R es un DFU con campo de fracciones K, entonces un elemento irreducible $F \in R[X]$ permanece irreducible considerado en $K[X]$; de ello se sigue que si F y G son polinomios de $R[X]$ sin divisores comunes en $R[X]$, tampoco tienen divisores comunes en $K[X]$.

Si R es un DFU, entonces $R[X]$ también es un DFU. Por consiguiente, $k[X_1, ..., X_n]$ es un DFU para cualquier campo k. El campo de fracciones de $k[X_1, ..., X_n]$ se indica por $k(X_1, ..., X_n)$ y se denomina campo de las funciones racionales de n variables sobre k.

Si $\varphi : R \to S$ es un homomorfismo de anillos, el conjunto $\varphi^{-1}(0)$, de elementos aplicados al cero, es el núcleo de φ, designado por $Ker(\varphi)$, y es un ideal de R. Un ideal I de un anillo R es propio si $I \neq R$. Un ideal propio es maximal si no está contenido en ningún otro ideal mayor propio, es decir diferente del anillo total. Un ideal primo es un ideal I tal que si $ab \in I$ entonces $a \in I$ o $b \in I$. Un conjunto S de elementos de un anillo R genera un ideal $I = \left\{ \sum a_i s_i \quad | \quad s_i \in S,\ a_i \in R \right\}$. Un ideal es de generación finita si ésta generado por un conjunto finito $S = \{f_1,..., f_n\}$;entonces se escribe $I = (f_1,..., f_n)$. Un ideal es principal si ésta generado por un solo elemento. Un dominio en el que todo ideal es principal se denomina dominio de ideales principales, designado por DIP. El anillo de los enteros y el anillo de polinomios en una variable sobre un campo son ejemplos de DIP. Cada DIP es un DFU. Un ideal principal $I = (a)$ en un DFU es primo si y sólo si a es irreducible.

Sea I un ideal en un anillo R. El anillo cociente de R módulo I se designa por R/I; es el conjunto de las clases de equivalencia de los elementos de R en la relación de equivalencia: $a \backsim b$ si $a - b \in I$. Denominaremos I-clase residual de a a la clase que contiene al elemento a; y se denota por $\overline{a}$. R/I constituye un anillo tal que la función $\pi : R \to R/I$ que aplica a cada elemento en su I-clase residual, es un homomorfismo de anillos. R/I está caracterizado por la siguiente propiedad : si $\varphi : R \to S$ es un homomorfismo del anillo R en el anillo S, y $\varphi(I) = 0$, existe un homomorfismo único $\overline{\varphi} : R/I \to S$ tal que $\varphi = \overline{\varphi} \circ \pi$.

Un ideal propio I de R es primo si y sólo si R/I es un dominio, y maximal si y sólo si R/I es un campo. Todo ideal maximal es primo.

Sea k un campo, I un ideal propio en $k[X_1, ..., X_n]$. El homomorfismo $\pi : k[X_1, ..., X_n] \to k[X_1, ..., X_n]/I$ se restringe a un homomorfismo de anillos de k en $k[X_1, ..., X_n]/I$. Entonces podemos considerar a k como un subanillo de $k[X_1, ..., X_n]/I$; en particular $k[X_1, ..., X_n]/I$ es un espacio vectorial sobre k.

Sea R un dominio. La característica de R, $car(R)$, es el menor entero positivo tal que $1 + \cdots + 1(p - veces) = 0$, cuando tal número exista; en caso contrario $car(R) = 0$. Si $\varphi : Z \to R$ es el único homomorfismo de anillos entre Z y R, entonces $Ker(\varphi) = (p)$, es decir $car(R)$ es un número primo.

Si R es un anillo, $a \in R, F \in R[X]$, y a una raíz de F, entonces $F = (X-a)G, G \in R[X]$. Un campo K es algebraicamente cerrado si cualquier $F \in R[X]$, no constante, tiene una raíz en él. Se demuestra entonces que $F = \mu \prod (X-\lambda_i)^{e_i}$, $\mu, \lambda_i \in k$ donde las λ_i son las distintas raíces de F, y e_i es la multiplicidad de λ_i. Un polinomio de grado d tiene d raíces en K, contando con las multiplicidades. El campo $\mathbb{C}$ es algebraicamente cerrado.

Sea R un anillo. La derivada de un polinomio $F = \sum a_i X^i \in R[X]$ se define por $\sum i a_i X^{i-1}$, y se escribe $\frac{\partial F}{\partial X}$ o F_x. Si $F \in R[X_1, ..., X_n]$, $\frac{\partial F}{\partial X_i}$ se define considerando F como un polinomio en X_i con coeficientes en $R[X_1, ..., X_{i-1}, X_{i+1}, ..., X_n]$. Se comprueban fácilmente las siguientes propiedades:

(1) $(aF + bG)_x = aF_x + bG_x$, $a, b \in R$

(2) $F_x = 0$ si F es una constante.

(3) $(FG)_x = F_x G + F G_x$, y $(F^n)_x = nF^{n-1}F_x$

(4) Si $G_1, ..., G_n \in R[X]$, y $F \in R[X_1, ..., X_n]$ entonces $F(G_1, ..., G_n)_x = \sum_{i=1}^{n} F_{x_i}(G_1, ..., G_n)G_{x_i}$.

(5) $F_{x_i}F_{x_j} = F_{x_j}F_{x_i}$, donde hemos escrito $F_{x_i}F_{x_j}$ por $(F_{x_i})_{x_j}$

(6) (*Teorema de Euler*). Si F es una forma de grado m en $R[X_1, ..., X_n]$, entonces $mF = \sum_{i}^{n} X_i F_{x_i}$.

1.2. Espacios afines y conjuntos algebraicos

Sea k un campo. Por $\mathbb{A}^n(k)$, o simplemente por $\mathbb{A}^n$ (si k se sobreentiende), se designa el producto cartesiano de k por sí mismo n veces: $\mathbb{A}^n(k)$ es el conjunto de n-adas de elementos de k. $\mathbb{A}^n(k)$ se llama *n-espacio afín* sobre k; sus elementos se denominarán puntos. $\mathbb{A}^1(k)$ es la recta afín, $\mathbb{A}^2(k)$ es el plano afín.

Si $F \in k[X_1, ..., X_n]$, un punto $P = (a_1, ..., a_n) \in \mathbb{A}^n(k)$ es un cero de F

si $F(P) = F(a_1, ..., a_n) = 0$. Si F no es constante, el conjunto de los ceros de F se denomina hipersuperficie definida por F, y se designa $V(F)$. Una hipersuperficie en $\mathbb{A}^2(k)$ es llamada curva afín plana. Si F es un polinomio de grado uno, $V(F)$ se llama hiperplano en $\mathbb{A}^n(k)$; si $n = 2$, es una recta.

En general, si S es un conjunto de polinomios de $k[X_1, ..., X_n]$, pongamos

$$V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ para todo } F \in S\}$$

$V(F) = \underset{F \in S}{\cap} V(F)$. Si $S = \{F_1, ..., F_r\}$ escribiremos usualmente $V(F_1, ..., F_r)$.

Un subconjunto $X \subset \mathbb{A}^n(k)$ es un *conjunto algebraico afín*, o simplemente un conjunto algebraico, si $X = V(S)$ para algún S.

Las siguientes propiedades se verifican fácilmente :

(1) Si I es el ideal en $k[X_1, ..., X_n]$ generado por S, entonces $V(S) = V(I)$; es decir, cada conjunto algebraico es igual a $V(I)$ para algún ideal I.

(2) Si $\{I_\alpha\}$ es una colección de ideales, entonces $V\left(\underset{\alpha}{\cup} I_\alpha\right) = \underset{\alpha}{\cap} V(I_\alpha)$; es decir, la intersección de una colección de conjuntos algebraicos es un conjunto algebraico.

(3) Si $I \subset J$, entonces $V(I) \supset V(J)$.

(4) $V(FG) = V(F) \cup V(G)$ para cualesquiera polinomios F, G, $V(F) \cup V(G) = V(\{FG \mid F \in I, G \in J\})$; es decir, cualquier unión finita de conjuntos algebraicos es un conjunto algebraico.

(5) $V(0) = \mathbb{A}^n(k)$.$V(1) = \emptyset$. $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\}$ para $a_i \in k$. Es decir, cualquier subconjunto finito de $\mathbb{A}^n(k)$ es un conjunto algebraico.

1.2.1. El ideal de un conjunto de puntos

Dado un subconjunto X de $\mathbb{A}^n(k)$, consideremos aquellos polinomios que se anulan en X, estos forman un ideal de $k[X_1, ..., X_n]$, llamado el *ideal de*

X, que designaremos por $I(X)$ donde

$$I(X) = \{F \in k[X_1, ..., X_n] \mid F(a_1, ..., a_n) = 0 \ \forall \ (a_1, ..., a_n) \in X \}$$

.

Las propiedades siguientes muestran algunas de las relaciones entre

ideales y conjuntos algebraicos;

(6) Si $X \subset Y$, entonces $I(X) \supset I(Y)$.

(7) $I(\emptyset) = k[X_1, ..., X_n]$. $I(\mathbb{A}^n(k)) = 0$ si k es un campo infinito. $I(\{a_1, ..., a_n\}) = (X_1 - a_1, ..., X_n - a_n)$ para $a_i \in k$.

(8) $I(V(S)) \supset S$ para todo conjunto de polinomios S de polinomios. $V(I(X)) \supset X$ para todo conjunto X de puntos.

(9) $V(I(V(S))) = V(S)$ para todo conjunto de polinomios S de polinomios, $I(V(I(X))) = I(X)$ para todo conjunto X de puntos.

Luego, si V es un conjunto algebraico, $V = V(I(V))$, y si I es el ideal de un conjunto algebraico, $I = I(V(I))$.

Un ideal de un conjunto algebraico tiene una propiedad de la que no participan todos los ideales: si $I = I(X)$, y $F^n \in I$ para un entero $n > 0$, entonces $F \in I$. Si I es un ideal de un anillo R, llamaremos radical de I, designado por $Rad(I)$, al $\{a \in R \mid a^n \in I$ para un entero $n > 0\}$. $Rad(I)$ es un ideal que contiene a I. I se llama un ideal radical si $Rad(I) = I$. Por lo tanto tenemos la siguiente propiedad :

(10) $I(X)$ es un ideal radical para todo conjunto $X \subset \mathbb{A}^n(k)$.

1.2.2. El teorema fundamental de Hilbert

Aunque hemos definido un conjunto algebraico a partir de un conjunto cualquiera de polinomios, de hecho basta siempre un número finito.

Teorema 1 *Todo conjunto algebraico es intersección de un número finito de hipersuperficies.*

Demostración. *1* ■

Un anillo se llama *noetheriano* o *anillo de Noether* si todo ideal del anillo es de generación finita. Los campos y los DIP son anillos noetherianos . El Teorema 1 es una consecuencia del siguiente teorema.

Teorema 2 *(de la Base de Hilbert) Si R es un anillo noetheriano entonces $R[x_1, ..., x_n]$ es un anillo noetheriano.*

Demostración. *1* ■

Corolario 3 *$k[x_1, ..., x_n]$ es noetheriano para todo campo k*

1.2.3. Componentes irreducibles de un conjunto algebraico

Un conjunto algebraico puede ser una reunión de varios conjuntos algebraicos menores. Un conjunto algebraico $V \subset \mathrm{A}^n$ es *reducible*, si $V = V_1 \cup V_2$, donde V_1, V_2 son conjuntos algebraicos de $\mathbb{A}^n$, y $V_i \neq V$ $i = 1, 2$. En caso contrario, V es *irreducible*.

Proposición 4 *Un conjunto algebraico V es* irreducible *si y sólo si $I(V)$ es primo.*

Demostración. *1* ■

Deseamos probar que un conjunto algebraico es la reunión de un número finito de conjuntos algebraicos irreducibles. Si V es reducible, escribiremos $V = V_1 \cup V_2$; si V_2 es reducible escribiremos $V_2 = V_3 \cup V_4$, etc. Es preciso ver que esta sucesión se acaba.

Lema 5 *Sea S una colección no vacía de ideales en un anillo noetheriano R.Entonces S posee un elemento maximal, es decir existe un ideal I de S que no está contenido en ningún otro ideal de S.*

De este lema se sigue inmediatamente que toda colección de conjuntos algebraicos de $\mathbb{A}^n(k)$ posee un elemento minimal. Si $\{V_\alpha\}$ es una de estas colecciones, consideremos un elemento maximal $I(V_{\alpha_0})$ de $\{I(V_\alpha)\}$. Entonces V_{α_0} es evidentemente minimal en la colección.

Teorema 6 *Sea V un conjunto algebraico de $\mathbb{A}^n(k)$. Entonces existen conjuntos algebraicos irreducibles $V_1, ..., V_m$, unívocamente determinados, tales que $V = V_1 \cup \cdots \cup V_m$ y $V_i \not\subset V_j$ para todo $i \neq j$.*

Los V_i se llaman componentes irreducibles de V ; $V = V_1 \cup \cdots \cup V_m$ es la descomposición de V en componentes irreducibles.

1.2.4. Subconjuntos algebraicos en el plano

Antes de desarrollar la teoría general, daremos una breve ojeada al plano afín $\mathbb{A}^2(k)$, y buscaremos todos sus subconjuntos algebraicos. En virtud del teorema 6 bastará buscar los subconjuntos algebraicos irreducibles.

Proposición 7 *Sean F y G polinomios de $k[x, y]$ sin factores comunes. Entonces $V(F, G) = V(F) \cap V(g)$ es un conjunto finito de puntos.*

Corolario 8 *Si F es un polinomio irreducible en $k[x, y]$ y si $V(F)$ es infinito, entonces $I(V(F)) = (F)$ y $V(F)$ es irreducible.*

Corolario 9 *Supongamos que k es infinito. Entonces los subconjuntos algebraicos irreducibles de $\mathbb{A}^2(k)$ son: $\mathbb{A}^2(k), \varnothing$, puntos, y las curvas planas irreducibles $V(F)$ donde F es un polinomio irreducible y $V(F)$ es infinito.*

Corolario 10 *Supóngase k algebraicamente cerrado, $F \in k[x, y]$. Sea $F = F_1^{n_1}, ..., F_r^{n_r}$, la descomposición de F en factores irreducibles. Entonces $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ es la descomposición de $V(F)$ en componentes irreducibles, y $I(V(F)) = (F_1, ..., F_r)$.*

Si consideramos un conjunto algebraico V, la proposición 4 nos da un criterio para saber si V es irreducible o no. Hace falta encontrar un método para describir a V a partir de un conjunto dado de polinomios que defina a V. En el apartado anterior hemos iniciado esta cuestión, pero precisamente el teorema de los ceros de Hilbert es el que da la relación exacta entre ideales y conjuntos algebraicos. Empezaremos por un teorema más débil y veremos que es posible reducirlo a resultados totalmente algebraicos.

En esta sección supondremos en todo momento que k es algebraicamente cerrado.

Teorema 11 *(Nullstellensatz débil) Si I es un ideal propio de $k[X_1, ..., X_n]$, entonces $V(I) \neq \varnothing$.*

Demostración. 1 ■

Teorema 12 *(Nullstellenzats) Sea I un ideal de $k[x_1, ..., x_n]$ (k algebraicamente cerrado). Entonces $I(V(I)) = Rad(I)$.*

Demostración. 1 ■

Los corolarios siguientes son consecuencias inmediatas del teorema.

Corolario 13 *Si I es un ideal radical en $k[x_1, ..., x_n]$, entonces*

$$I(V(I)) = I$$

En consecuencia, existe una correspondencia uno a uno entre ideales radicales y conjuntos algebraicos.

Corolario 14 *Si I es un ideal primo, entonces $V(I)$ es irreducible.Existe una correspondencia uno a uno entre ideales primos y conjuntos algebraicos irreducibles. A los ideales maximales les corresponden puntos.*

Corolario 15 *Sea* $F \in k[x_1, ..., x_n], F = F_1^{n_1} \cdots F_r^{n_r}$ *la descomposición de* F *en factores irreducibles. Entonces* $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ *es la descomposición de* $V(F)$ *en componentes irreducibles, y* $I(V(F)) = (F_1, ..., F_r)$. *Existe una correspondencia uno a uno entre polinomios irreducibles* $F \in k[x_1, ..., x_n]$ *(salvo factores no nulos de* k*) e hipersuperficies irreducibles de* $\mathbb{A}^n(k)$.

Corolario 16 *Sea* I *un ideal de* $k[x_1, ..., x_n]$. *Entonces* $V(I)$ *es un conjunto finito si y sólo si* $k[x_1, ..., x_n]/I$ *es un espacio vectorial de dimensión finita sobre* k. *Si ello ocurre, el número de puntos de* $V(I)$ *es* $\leq \dim_k(k[x_1, ..., x_n]/I)$.

1.2.5. Variedades afines

Desde ahora, k indicará a un campo algebraicamente cerrado fijo. Los conjuntos algebraicos afines se consideran en $\mathbb{A}^n = \mathbb{A}^n(k)$ para un cierto n. Un conjunto algebraico afín irreducible será denominado una variedad afín.

Todos los anillos y los campos contendrán a k como subanillo. Por un homomorfismo $\varphi : R \to S$ entre tales anillos entenderemos un homomorfismo tal que $\varphi(\lambda) = \lambda$ para todos los $\lambda \in k$

Sea $V \subset \mathbb{A}^n$ una variedad. $I(V)$ será un ideal primo de $k[x_1, ..., x_n]$, por lo tanto $k[x_1, ..., x_n]/I(V)$ es un dominio.

Escribiremos $\Gamma(V) = k[x_1, ..., x_n]/I(V)$, y lo denominaremos *anillo coordenado de* V.

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

Si $V \subset \mathbb{A}^n$ es una variedad, una función $f \in \hat{J}(V, k)$ se denomina una *función polinómica* si existe un polinomio $F \in k[x_1, ..., x_n]$ tal que

$f(a_1, ..., a_n) = F(a_1, ..., a_n)$ para todo $(a_1, ..., a_n) \in V$. Las funciones polinómicas constituyen un subanillo de $\hat{J}(V, k)$ que contiene a k. Dos polinomios F, G determinan una misma función si y sólo si $(F - G)(a_1, ..., a_n) = 0$ para todo $(a_1, ..., a_n) \in V$. Tendremos dos maneras importantes de interpretar un elemento de $\Gamma(V)$: como una función sobre V, o como una clase de equivalencia de polinomios.

Sean $V \subset \mathbb{A}^n, W \subset \mathbb{A}^n$ varidades. Una función $\varphi : V \to W$ se denomina una aplicación polinómica si existen polinomios $T_1, ...T_m \in k[x_1, ..., x_n]$ tales que $\varphi : (a_1, ..., a_n) = (T_1(a_1, ..., a_n), ..., T_m(a_1, ..., a_n))$ para todo $(a_1, ..., a_n) \in V$.

Una función $\varphi : V \to W$ induce un homomorfismo $\widetilde{\varphi} : \hat{J}(V, k) \to \hat{J}(W, k)$, donde $\widetilde{\varphi}(f) = f \circ \varphi$. Si φ es una aplicación polinómica, 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* del polinomio $F(T_1, ..., T_m)$.

Si $V = \mathbb{A}^n$, $W = \mathbb{A}^m$, y $T_1, ..., T_m \in k[x_1, ..., x_n]$ determinan una aplicación polinómica $T : \mathbb{A}^n \to \mathbb{A}^m$, los T_i están unívocamente determinados por T por lo cual escribiremos, a menudo, $T = (T_1, ..., T_m)$.

Proposición 17 *Sean $V \subset \mathbb{A}^n, W \subset \mathbb{A}^n$ variedades afines. Existe una correspondencia natural uno a uno entre las aplicaciones polinómicas $\varphi : V \to W$ y los homomorfismos $\widetilde{\varphi} : \Gamma(V) \to \Gamma(W)$. Una aplicación tal φ es la restricción de una aplicación polinómica de $\mathbb{A}^n$ en $\mathbb{A}^m$.*

Demostración. 1 ■

Una aplicación polinómica $\varphi : V \to W$ es un isomorfismo si existe una aplicación polinómica $\psi : W \to V$ tal que $\psi \circ \varphi =$ identidad sobre V, $\varphi \circ \psi =$ identidad sobre W. La proposición 17 demuestra que dos variedades afines son isomorfas si y sólo si sus anillos coordenados lo son.

Si $T = (T_1, ..., T_m)$ es una aplicación polinómica de $\mathbb{A}^n$ en $\mathbb{A}^m$, y $F \in k[x_1, ..., x_n]$, escribiremos $F^T = \widetilde{T}(F) = F(T_1, ...T_m)$. Para ideales I y conjuntos algebraicos V de $\mathbb{A}^m$, I^T designará el ideal de $k[x_1, ..., x_n]$ generado por $\left\{F^T \mid F \in I\right\}$ y V^T el conjunto algebraico $T^{-1}(V) = V\left(I^T\right)$, donde

$I = I(V)$. Si V es la hipersuperficie de F, V^T es la hipersuperficie de F^T $\left(\text{si } F^T \text{ no es constante}\right)$.

Un cambio de coordenadas afín en $\mathbb{A}^n$ es una aplicación polinómica $T = (T_1, ..., T_m) : \mathbb{A}^n \to \mathbb{A}^m$ tal que cada T_i es un polinomio de grado 1, y que T es uno a uno y es exhaustivo. Si $T_i = \sum a_{ij}x_j + a_{i0,}$ entonces $T = T'' \circ T'$, donde T' es una aplicación lineal $(T_i' = \sum a_{ij}x_j)$ y T'' es una traslación $(T_i'' = x_i + a_{i0})$.

Como toda traslación posee una inversa (que también es una traslación), es claro que T será uno a uno (y exhaustiva) si y sólo si T' es invertible. Si T y U son cambios de coordenadas es $\mathbb{A}^n$, también lo serán $T \circ U$ y $T^{-1}; T$ es un isomorfismo de la variedad $\mathbb{A}^n$ en sí misma.

1.3. Funciones racionales y anillos locales

Sea V una variedad de $\mathbb{A}^n, \Gamma(V)$ su anillo de coordenadas. Como $\Gamma(V)$ es un dominio, podemos construir su campo de fracciones. Este campo se denomina *campo de las funciones racionales* de V, y lo designaremos por $k(V)$. Un elemento de $k(V)$ es una función racional de V.

Si f es una función racional de V, y $P \in V$,diremos que f está definida en P si para $a, b \in \Gamma(V), f = a/b$, y $b(P) \neq 0$. Nótese que puede haber distintas maneras de escribir f como cociente de funciones polinómicas; f estará definida en P si es posible hallar un denominador que no se anule en P. Si $\Gamma(V)$ es un DFU, entonces existe una representación única $f = a/b$ esencial, en la que a y b no tienen divisores comunes, y entonces f estará definida en P si y sólo si $b(P) \neq 0$.

Sea $P \in V$. Definimos $\mathcal{O}(V)$ como el conjunto de todas las funciones racionales sobre V que estan definidas en P. Es fácil verificar que $\mathcal{O}(V)$ constituye un subanillo de $k(V)$ que contiene a $\Gamma(V) : k \subset \Gamma(V) \subset \mathcal{O}(V) \subset k(V)$. $\mathcal{O}(V)$ se denomina anillo local de V en P.

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

Proposición 18 *(1) El conjunto de polos de una función racional sobre V, es un subconjunto algebraico de V.*

(2) $\Gamma(V) = \underset{P \in V}{\cap} \mathcal{O}(V)$.

Demostración. 1 ■

Supóngase que $f \in \mathcal{O}(V)$ .Podemos definir también el valor de f en P, que designaremos $f(P)$,de la siguiente manera: escrito $f = a/b, a, b \in \Gamma(V)$. $b(P) \neq 0$, sea $f(P) = a(P)/b(P)$ (se comprueba que es independiente de la elección de a y b). $M_P(V) = \{f \in \mathcal{O}_p(V) \mid f(P) = 0\}$ se denominará *ideal maximal de V en P.*

Se trata del núcleo del homomorfismo de valoración $f \to f(P)$ de $\mathcal{O}(V)$ sobre k, por lo tanto $\mathcal{O}(V)/M_P(V)$ es isomorfo a k. un elemento $f \in \mathcal{O}(V)$ es unitario en $\mathcal{O}(V)$ si y sólo si $f(P) \neq 0$, luego

$M_P(V) = \{\text{elementos de } \mathcal{O}_p(V) \text{ que no son unitarios}\}$.

Lema 19 *En todo anillo R las siguientes condiciones son equivalentes:*
(1) El conjunto de elementos de R que no son unitarios constituyen un ideal.
(2) R posee un ideal maximal único que contiene a todo ideal propio de R.

Demostración. 1 ■

Un anillo que satisfaga las condiciones del lema se denomina un anillo local; los elementos unitarios son aquellos elementos que no pertenecen al ideal maximal. Hemos visto que $\mathcal{O}(V)$ es un anillo local, y que $M_P(V)$ es su único ideal maximal.

Proposición 20 *$\mathcal{O}(V)$ Es un dominio local noetheriano.*

Demostración. 1 ■

1.3.1. Anillos de valoración discreta

Proposición 21 *Sea R un dominio que no sea un campo. Entonces tenemos las siguientes equivalencias.*
(1) R es noetheriano y local, y el ideal maximal es principal.
(2) Existe un elemento irreducible $t \in R$ tal que cada $z \in R$ no nulo se puede escribir de modo único en la forma $z = ut^n$, u unitario en R, n un entero no negativo.

Demostración. 1 ■

Un anillo que satisfaga las condiciones de la proposición 4 se denominará un *anillo de valoración discreta*, designado AVD. Un elemento t como el introducido en (2) se denominará *parámetro de uniformización de R*; cualquier otro parámetro de uniformización es de la forma ut, donde u es unitario en R. Sea K el campo de fracciones de R. Entonces todo elemento no nulo $z \in K$ se escribe de manera única en la forma $z = ut^n$, donde u es úntario en $R, n \in \mathbb{Z}$.

El exponente n se llama orden de z; se escribe $n = ord(z)$; definiremos $ord(0) = \infty$. $M = \{z \in K \mid ord(z) > 0\}$ es el ideal maximal de R.

1.3.2. Formas

Sea R un dominio. Si $F \in R[x_1, ..., x_{n+1}]$ es una forma, definiremos $F_* \in R[x_1, ..., x_n]$ por $F = F(x_1, ..., x_n, 1)$. Recíprocamente, para todo polinomio $f \in R[x_1, ..., x_n]$ de grado d, que se puede escribir de la siguiente manera: $f = f_0 + f_1 \cdots f_d$ donde f_i es una forma de grado i, definiremos $f^* \in R[x_1, ..., x_{n+1}]$ por

$$f^* = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots f_d = x_{n+1}^d f(x_1/x_{n+1}, ..., x_n/x_{n+1})$$

f^* es una forma de grado d. Al polinomio F_* se le llama deshomogeneización de F. Por su parte al polinomio f^* se le llama homogeneización de f.

(1) $(FG)_* = F_* G_*$; $(fg)^* = f^* g^*$.

(2) Si r es la mayor potencia de x_{n+1} que divide a F, entonces $x_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.

(3)$(F+G)_* = F_* + G_*$; $x_{n+1}^t (f+g)^* = x_{n+1}^r f^{\ *} + x_{n+1}^s g^*$, donde $r = \text{grad}(g)$, $s = \text{grad}(f)$, y $t = r + s - \text{grad}(f+g)$.

Demostración. 1 ■

Corolario 22 *Salvo las potencias de x_{n+1}, la descomposición en factores de una forma $F \in R[x_1, ..., x_{n+1}]$ es la misma que la descomposición en factores de $F_* \in R[x_1, ..., x_n]$. En particular, si $F \in k[x, y]$ es una forma, y k es algebraicamente cerrado, entonces F descompone en producto de factores lineales.*

1.3.3. Ideales con un número finito de ceros

La proposición de este apartado será utilizada para relacionar cuestiones locales (expuestas por medio de anillos locales $\mathcal{O}(V)$) con cuestiones globales (expuestas por medio de anillos coordenados).

Proposición 23 *Sea I un ideal de $k[x_1, ..., x_n]$, (k algebraicamente cerrado), y supóngase que $V(I) = \{P_1, ..., P_N\}$ es finito. Sea $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$. Entonces existe un isomorfismo natural de $k[x_1, ..., x_n]/I$ en $\prod_{i=1}^{N} \mathcal{O}_i/I\mathcal{O}_i$.*

Demostración. 1 ■

Corolario 24 $\dim_k (k[x_1, ..., x_n]/I) = \sum_{i=1}^{N} \dim_k (\mathcal{O}_i/I\mathcal{O}_i)$.

Corolario 25 *Si $V(I) = \{P\}$, entonces $k[x_1, ..., x_n]/I \cong \mathcal{O}(\mathbb{A}^n)/I\mathcal{O}(\mathbb{A}^n)$.*

1.3.4. Módulos cociente y sucesiones exactas

Sea R un anillo, M, M' R-módulos. Un homomorfismo (o bien, un isomorfismo) $\varphi : M \to M'$ de los grupos abelianos se llama un homomorfismo

de R-módulos (respectivamente, un isomorfismo) si $\varphi(am) = a\varphi(m)$ para todo $a \in R$ y todo $m \in M$.

Si N es un submódulo de un R-módulo M, el grupo cociente M/N de las clases laterales de M módulo N adquiere una estructura de R-módulo, tal que la aplicación natural de M en M/N es un homomorfismo entre R-módulos. M/N se denomina módulo cociente de M por N.

Sean $\psi : M' \to M$, $\varphi : M \to M''$ dos homomorfismos entre R-módulos. Diremos que la sucesión (de modulos y homomorfismos)

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

es exacta (o exacta en M) si la imagen de ψ coincide con el núcleo de φ, es decir, $\mathrm{Im}(\psi) = Ker(\varphi)$. Obsérvese que los homomorfismos de R-módulos entre el módulo 0 y cualquier R-módulo M, y el de M en 0 existen y son únicos. Entonces $M \xrightarrow{\varphi} M'' \to 0$ es exacta si y sólo si φ es exhaustiva, y

$0 \to M \xrightarrow{\psi} M''$ es exacta si y sólo si ψ es uno a uno.

Si $\varphi_i : M_i \to M_{i+1}$ son los homomorfismos entre R-módulos, diremos que la sucesión

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

es exacta si $\mathrm{Im}(\varphi_i) = Ker\left(\varphi_{i+1}\right)$ para cada $i = 1, ..., n-1$.Entonces

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

es exacta si y sólo si φ es exhaustiva, y ψ aplica M' isomórficamente sobre el núcleo de φ.

1.3.5. Módulos libres

Sea R un anillo y X un conjunto cualquiera.

Sea $M_X = \{\varphi : X \to R \mid \varphi(x) = 0 \text{ salvo un número finito de } x \in X\}$. M_X adquiere estructura de R-módulo de la siguiente manera: $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$, y $(a\varphi)(x) = a \cdot \varphi(x)$ para todo $\varphi, \psi \in M_X, a \in R, x \in X$. M_X recibe el nombre R-módulo libre sobre un conjunto X. Si definimos $\varphi_X \in M_X$ por las reglas $\varphi_X(y) = 0$ si $y \neq x, \varphi_X(x) = 1$, entonces cada $\varphi \in M_X$ se escribe en la forma $\varphi = \sum a_x \varphi_x$, y la expresión así obtenida para φ es única siendo $a_x \in R$ (de hecho, $a_x = \varphi(x)$). Normalmente, en lugar de φ_x escribiremos x, y consideraremos a X como un subconjunto de M_X. Diremos que X es una base de M_X: los elementos de M_X son precisamente las sumas formales $\sum a_x x$.

M_X está caracterizado por la siguiente propiedad: si $\alpha : X \to M$ es una función cualquiera del conjunto X en el R-modulo M, entonces α se extiende a un homomorfismo de M_X en M, y esta extensión es única.

Un R-módulo M se llama libre con base $m_1, ..., m_n \in M$ si para $X = \{m_1, ..., m_n\}$, el homomorfismo de $M_x \to M$ es un isomorfismo.

Si $R = \mathbb{Z}$, un $\mathbb{Z}$-módulo libre que se extiende sobre X se denomina grupo abeliano libre sobre X.

1.4. Variedades proyectivas

1.4.1. Espacio proyectivo

Sea k un campo. Un *n-espacio proyectivo sobre* k, designado por $\mathbb{P}^n(k)$, o simplemente por $\mathbb{P}^n$, se define como el conjunto de todas las rectas de $\mathbb{A}^{n+1}(k)$ que pasan por $(0, 0, ..., 0)$. Todo punto $(x) = (x_1, ..., x_{n+1}) \neq (0, ..., 0)$ determina una sola de dichas rectas, a saber $\{(\lambda x_1, ..., \lambda x_n) \mid \lambda \in k\}$. Dos de estos puntos (x) e (y) determinan la misma recta si y sólo si existe $\lambda \in k$, no

nulo, tal que $y_i = \lambda x_i$ para $i = 1, ..., n+1$; si se da este caso, diremos que (x) e (y) son equivalentes. Entonces $\mathbb{P}^n$ se puede identificar con el conjunto de clases de equivalencia de puntos de $\mathbb{A}^{n+1} - \{(0, ..., 0)\}$.

Llamaremos puntos a los elementos de $\mathbb{P}^n$. Si un punto $P \in \mathbb{P}^n$ está determinado como antes por un $(x_{1,}..., x_{n+1}) \in \mathbb{A}^{n+1}$, diremos que $(x_1, ..., x_{n+1})$ es un conjunto de coordenadas homogéneas para P. A menudo escribiremos $P = (x_{1,}..., x_{n+1})$ para indicar que $(x_{1,}..., x_{n+1})$ son las coordenadas homogéneas de P. Nótese que la i-esima coordenada x_i no está bien definida, pero nos permite saber perfectamente si la i-esima coordenada es cero o no; y si $x_i \neq 0$, las razones x_j/x_i están bien definidas (ya que son invariantes respecto a la equivalencia).

Sea $U_i = \{(x_{1,}..., x_{n+1}) \in \mathbb{P}^n \mid x_i \neq 0\}$. Cada $P \in U_i$ posee un único conjunto de coordenadas homogéneas de la forma $P = (x_{1,}..., x_{i-1}, 1, x_{i+1,}..., x_{n+1})$, llamadas coordenadas no homogéneas de P respecto a U_i (o a x_i, o a i). Si definimos $\varphi_i : \mathbb{A}^n \to U_i$ por medio de $\varphi_i(a_1, ..., a_n) = (a_1, ..., a_{i-1}, 1, a_{i+1}, ..., a_n)$, entonces φ_i establece una correspondencia uno a uno entre los puntos de $\mathbb{A}^n$ y los puntos U_i. Nótese que $\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$ por lo tanto $\mathbb{P}^n$ posee un recubrimiento formado por n+1 conjuntos, cada uno de los cuales se puede considerar como un n-espacio afín.

Por comodidad, nos referiremos ordinariamente al U_{n+1}. Sea

$H_\infty = \mathbb{P}^n - U_{n+1} = \{(x_{1,}x_n..., x_{n+1}) \mid x_{n+1} = 0\}$. H_∞ se denomina frecuentemente el hiperplano del infinito. La correspondencia $(x_{1,}..., x_n, 0) \longleftrightarrow (x_{1,}..., x_n)$ prueba que H_∞ se puede identificar con $\mathbb{P}^{n-1}$. De donde $\mathbb{P}^n = U_{n+1} \cup H_\infty$ es la unión de un n-espacio afín y un conjunto que da todas las direcciones del n-espacio afín.

1.4.2. Conjuntos algebraicos proyectivos

Un punto $P \in \mathbb{P}^n$ se llama *cero de un polinomio* $F \in k[x_1, ..., x_{n+1}]$ si $F(x_1, ..., x_{n+1}) = 0$ para toda elección de las coordenadas homogéneas $(x_1, ..., x_{n+1})$ de P; escribiremos $F(P) = 0$. Si representamos a F como suma de formas en el sentido usual, entonces cada forma se anula en todo conjunto de coordenadas homógeneas de P.

Para todo conjunto S de polinomios de $k[x_1, ..., x_{n+1}]$, sea

$V(S) = \{P \in \mathbb{P}^n \mid P$ es un cero de todo polinomio $F \in S\}$. Si I es el ideal generado por S, $V(I) = V(S)$. Si $I = \left(F^{(1)}, ..., F^{(r)}\right)$ donde $F^{(i)} = \sum F_j^{(i)}$, siendo $F_j^{(i)}$ una forma de grado j, entonces $V(I) = V\left(\left\{F_j^{(i)}\right\}\right)$, por lo tanto $V(S) = V\left(\left\{F_j^{(i)}\right\}\right)$ es el conjunto de ceros de un número finito de formas. Dicho conjunto se denomina *conjunto algebraico de* $\mathbb{P}^n$, o un *conjunto algebraico proyectivo.*

Para todo conjunto $X \subset \mathbb{P}^n$, sea

$I(X) = \{F \in k[x_1, ..., x_{n+1}] \mid$ cada $P \in X$ es un cero de $F\}$. A $I(X)$ se le denomina ideal de X.

Un ideal $I \subset k[x_1, ..., x_{n+1}]$ se llama homogeneo si para todo $F = \sum_{i=0}^{m} F_i \in I$, siendo F_i una forma de grado i, se tiene también $F_i \in I$. Para todo conjunto $X \subset \mathbb{P}^n$, $I(X)$ es un ideal homogéneo.

Proposición 26 *Un ideal $I \subset k[x_1, ..., x_{n+1}]$ es homogéneo si y sólo si está generado por un conjunto (finito) de formas.*

Demostración. 1 ■

Un conjunto algebraico $X \subset \mathbb{P}^n$ es irreducible si no es unión de dos conjuntos algebraicos. Un conjunto algebraico irreducible de $\mathbb{P}^n$ se llama una variedad proyectiva. Un conjunto algebraico proyectivo se puede representar, de modo único, como unión de variedades proyectivas, que son sus componentes irreducibles.

Las operaciones

$$\left\{\begin{array}{c}\text{ideales homogéneos}\\ \text{de } k[x_1, ..., x_{n+1}]\end{array}\right\} \xrightarrow{V} \left\{\begin{array}{c}\text{conjuntos algebraicos}\\ \text{de } \mathbb{P}^n(k)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{conjuntos algebraicos}\\ \text{de } \mathbb{P}^n(k)\end{array}\right\} \xrightarrow{I} \left\{\begin{array}{c}\text{ideales homogéneos}\\ \text{de } k[x_1, ..., x_{n+1}]\end{array}\right\}$$

satisfacen la mayor parte de las propiedades halladas en la situación afín correspondiente. Hemos utilizado las mismas notaciones en ambos casos. En

la práctica siempre queda claro cuál es la mencionada; si hubiese peligro de confusión, se escribira V_P, I_P para las operaciones proyectivas, V_a, I_a para las afines.

Si V es un conjunto algebraico de $\mathbb{P}^n$, definimos

$$C(V) = \left\{(x_1, ..., x_{n+1}) \in \mathbb{A}^{n+1} \mid (x_1, ..., x_{n+1}) \in V \ o \ (x_1, ..., x_{n+1}) = (0, ..., 0)\right\}$$

como el cono sobre V. Si $V \neq \varnothing$, entonces $I_a(C(V)) = I_P(V)$; y si I es un ideal homogéneo de $k[x_1, ..., x_{n+1}]$ tal que $V_P(I) \neq \varnothing$, entonces $C(V_P(I)) = V_a(I)$.

Teorema 27 *(Nullstellenzats proyectivo) Sea I un ideal homogéneo en $k[x_1, ..., x_{n+1}]$. Entonces*
(1) $V_P(I) = \varnothing$ si y sólo si existe un entero N tal que I contenga todas las formas de grado $\geqslant N$.
(2) Si $V_P(I) \neq \varnothing$, entonces $I_P(V_P(I)) = Rad(I)$

Demostración. 1. ■

En particular, existe una correspondencia uno a uno entre hipersuperficies proyectivas $V = V(F)$ y formas (no constantes) F que definen las V, conviniendo que F no posee factores múltiples (F está determinado al menos de un factor no nulo $\lambda \in k$). A hipersuperficies irreducibles corresponden formas irreducibles.

Un hiperplano es una hipersuperficie definida por una forma de grado uno. Los hiperplanos $V(X_i)$, $i = 1, ..., n+1$, se suelen llamar hiperplanos coordenados, o hiperplanos del infinito con respecto a U_i. Si $n = 2$, los $V(X_i)$ son los tres ejes coordenados.

Sea V una variedad proyectiva de $\mathbb{P}^n$. $I(V)$ es un ideal primo, por lo tanto el anillo residual $\Gamma_h(V) = k[x_1, ..., x_{n+1}]/I(V)$ es un dominio. Se la llama *anillo de coordenadas homógeneas de V.*

En general, sea I un ideal homogéneo de $k[x_1, ..., x_{n+1}]$, y sea $\Gamma(V) = k[x_1, ..., x_{n+1}]/I$. Un elemento $f \in \Gamma$ se denominará *forma de grado d* si existe una forma F de grado d de $k[x_1, ..., x_{n+1}]$ cuya clase residual sea f.

Proposición 28 *Todo elemento $f \in \Gamma$ se puede expresar de forma única $f = f_o + \cdots + f_m$, donde f_i es una forma de grado i.*

Demostración. 1. ■

Sea $k_h(V)$ el campo de las fracciones de $\Gamma_h(V)$; se le llamará campo de las funciones homogéneas de V en contraste con el caso de las variedades afines, sólo los elementos de $\Gamma_h(V)$ que son constantes determinan funciones sobre V; así mismo, la mayoría de los elementos de $k_h(V)$ no pueden considerarse como funciones. No obstante, si $f,\ g$ son dos formas de $\Gamma_h(V)$ del mismo grado d entonces $f\ /g$ define una función, por lo menos, donde g no es cero: se tiene $\frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^d f(x)}{\lambda^d g(x)} = \frac{f(x)}{g(x)}$, luego el valor de f/g no depende de la elección de las coordenadas homogéneas.

El campo de las funciones de V, designado por $k(V)$, se define como el conjunto

$$\{z \in k_h(V) \mid \text{para ciertas formas } f,\ g \in \Gamma_h(V) \text{ del mismo grado, } z = f/g\ \}$$

No es difícil verificar que $k(V)$ es un subcampo de $k_h(V)$. $k \subset k(V) \subset k_h(V)$, pero $\Gamma_h(V) \not\subset k(V)$. Los elementos de $k(V)$ se denominan *funciones racionales sobre V*.

Sea $P \in V,\ z \in k(V)$. Diremos que z está definido en P si z se puede expresar en la forma $z = f/g,\ f$ y g formas del mismo grado, y $g(P) \neq 0$. Consideremos $\mathcal{O}(V) = \{z \in k_h(V) \mid z \text{ está definida en } P\ \}$. $\mathcal{O}(V)$ es un subanillo de $k(V)$; se trata de un anillo local con ideal maximal $M_P(V) = \{z \mid z = f/g,\ g(P) \neq 0,\ f(P) = 0\}$. El valor $z(P)$ de una función $z \in \mathcal{O}(V)$ está bien definido.

Si $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ es un cambio de coordenadas lineal, entonces T aplica rectas que pasen por el origen en rectas que pasan por el origen. O sea que T determina una aplicación de $\mathbb{P}^n$ en $\mathbb{P}^n$, que llamaremos un cambio de coordenadas proyectivo. Si V es un conjunto algebraico de $\mathbb{P}^n$, entonces $T^{-1}(V)$ es también un conjunto algebraico de $\mathbb{P}^n$; escribiremos V^T en lugar de $T^{-1}(V)$. Si $V = V(F_1, ..., F_r)$, y $T = (T_1, ..., T_{n+1})$, T_i formas de grado 1, entonces $V^T = V\left(F_1^T, ..., F_r^T\right)$, donde $F_i^T = F_i(T_1, ...T_{n+1})$.

V es una variedad si y sólo si V^T es una variedad, y T induce un isomorfismo $\widetilde{T} : \Gamma_h(V) \to \Gamma_h\left(V^T\right)$, $k(V) \to k\left(V^T\right)$, y $\mathcal{O}(V) \to \mathcal{O}_Q\left(V^T\right)$, si $T(Q) = P$.

1.4.3. Variedades afines y proyectivas

Podemos considerar $\mathbb{A}^n$ como un subconjunto de $\mathbb{P}^n$ por medio de la aplicación $\varphi_{n+1} : \mathbb{A}^n \to U_{n+1} \subset \mathbb{P}^n$. En este apartado estudiaremos las relaciones entre los conjuntos algebraicos de $\mathbb{A}^n$ y los de $\mathbb{P}^n$.

Sea V un conjunto algebraico de $\mathbb{A}^n$, $I = I(V) \subset k[x_1, ..., x_n]$. Sea I^* el ideal de $k[x_1, ..., x_n]$ generado por $\{F^* \mid F \in I\}$. I^* es un ideal homogéneo; definimos V^* por $V(I^*) \subset \mathbb{P}^n$.

Reciprocamente, sea V un conjunto algebraico de $\mathbb{P}^n$,
$I = I(V) \subset k[x_1, ..., x_{n+1}]$. Sea I_* el ideal de $k[x_1, ..., x_n]$ generado por $\{F_* \mid F \in I\}$. Definimos V_* por $V(I_*) \subset \mathbb{A}^n$.

Proposición 29 *(1) Si $V \subset \mathbb{A}^n$, $\varphi_{n+1}(V) = V^* \cap U_{n+1}$, y $(V^*)_* = V$.*
(2) Si $V \subset W \subset \mathbb{A}^n$, entonces $V^* \subset W^* \subset \mathbb{P}^n$. Si $V \subset W \subset \mathbb{P}^n$ entonces $V_* \subset W_* \subset \mathbb{A}^n$.
(3) Si V es irreducible en $\mathbb{A}^n$, entonces V^* lo es en $\mathbb{P}^n$.
(4) Si $V = \underset{i}{\cup} V_i$ es la descomposición de V en componentes irreducibles en $\mathbb{A}^n$, entonces $V^* = \underset{i}{\cup} V_i^*$ es la descomposición irreducible de V^* en $\mathbb{P}^*$.
(5) Si $V \subset \mathbb{A}^n$, entonces V^* es el menor conjunto algebraico de $\mathbb{P}^n$ que contiene a V.
(6) Si $V \underset{\neq}{\subset} \mathbb{A}^n$, entonces ninguna componente de V^* está en $H_\infty = \mathbb{P}^n - U_{n+1}$ o contiene a H_∞.
(7) Si $V \subset \mathbb{P}^n$, y ninguna componente de V está en H_∞ o contiene a H_∞, entonces $V_* \subsetneq \mathbb{A}^n$ y $(V_*)^* = V$.

Demostración. 1. ■

Si V es un conjunto algebraico de $\mathbb{A}^n$, $V^* \subset \mathbb{P}^n$ se denomina *clausura proyectiva de V*. Si $V = V(F)$ es una hipersuperficie afín, entonces $V^* =$

$V(F^*)$. Excepto para las variedades afines contenidas en H_∞, existe una correspondencia natural uno a uno entre variedades afines y proyectivas.

Sea V una variedad afín, $V \subset \mathbb{P}^n$ su clausura proyectiva. Si $f \in \Gamma_h(V^*)$ es una forma de grado d, podemos definir $f_* \in \Gamma(V)$ de la siguiente manera: tomemos una forma $F \in k[x_1, ..., x_{n+1}]$ con su $I_P(V^*)$ clase residual en f, y sea $f_* = I(V)$-clase residual de F_* (se comprueba que ésta no depende de la elección de F). Definimos un isomorfismo natural $\alpha : k(V^*) \to k(V)$ como sigue: $\alpha(f/g) = f_*/g_*$, donde $f,\ g$ son formas del mismo grado en V^*. Si $P \in V$, podemos conciderar que $P \in V^*$ (por medio de φ_{n+1}) y entonces α induce un isomorfismo de $\mathcal{O}(V^*)$ en $\mathcal{O}(V)$. Ordinariamente utilizaremos α para identificar $k(V)$ con $k(V^*)$, y $\mathcal{O}(V)$ con $\mathcal{O}(V^*)$.

Toda variedad proyectiva $V \subset \mathbb{P}^n$ está recubierta por los $n+1$ conjuntos $V \cap U_i$. Si formamos V_* con respecto a U_i (como se ha hecho con respecto a U_{n+1}), los puntos de $V \cap U_i$ corresponden a los puntos de V_* y los anillos locales son isomorfos. Entonces las cuestiones referentes a V en la proximidad de un punto P se pueden reducir a cuestiones sobre una variedad afín V_* (por lo menos si la cuestión puede ser contestada considerando $\mathcal{O}_p(V)$).

1.4.4. Espacio multiproyectivo

Deseamos convertir el producto cartesiano de dos variedades en una variedad. Como $\mathbb{A}^n \times \mathbb{A}^m$ se puede identificar con $\mathbb{A}^{n+m}$, no es difícil para variedades afines. El producto $\mathbb{P}^n \times \mathbb{P}^m$ requiere no obstante, cierta discusión.

Escribamos $k[x, y]$ en lugar de $k[x_1, ..., x_{n+1}, y_1, ..., y_{m+1}]$. un polinomio $F \in k[x, y]$ se llama *una biforma de bigrado* (p, q) si F es una forma de grado p $(o\ q)$ cuando se considera un polinomio de $x_1, ..., x_{n+1}$ (o respectivamente de $y_1, ..., y_{m+1}$) con coeficientes en $k[y_1, ..., y_{m+1}]$ (o respectivamente en $k[x_1, ..., x_{n+1}]$). Cada $F \in k[x, y]$ se puede expresar de modo único como la suma $F = \sum_{p,q} F_{p,q}$, donde $F_{p,q}$, es una biforma de bigrado (p, q).

Si S es un conjunto de biformas de $k[x_1, ..., x_{n+1}, y_1, ..., y_{m+1}]$ designare-

mos por $V(S)$ o $V_b(S)$ al conjunto

$$V(S) = \{(x, y) \in \mathbb{P}^n \times \mathbb{P}^n \mid F(x, y) = 0 \ \forall F \in S\}$$

Diremos que un subconjunto V de $\mathbb{P}^n \times \mathbb{P}^n$ es algebraico si $V = V(S)$ para algún S. Para todo $V \subset \mathbb{P}^n \times \mathbb{P}^n$ definimos $I(V)$, o $I_b(V)$ como el conjunto

$$I(V) = \{F \in k[x, y] \mid F(x, y) = 0 \ \forall \ (x, y) \in V\}$$

Si $V \subset \mathbb{P}^n \times \mathbb{P}^n$ es una variedad (irreducible), $\Gamma_b(V) = k[x, y]/I_b(V)$ es el anillo bihomogéneo de coordenadas, $k_b(V)$ su campo de cocientes y $K(V) = \{z \in k_b(V) \mid z = f/g, \ f, g$ biformas del mismo bigrado de $\Gamma_b(V)\}$ es el campo de funciones de V. El anillo local $\mathcal{O}_p(V)$ se definirá como antes así como la teoría de variedades multiproyectivas en $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_r}$.

1.4.5. Grado de una curva y multiplicidad de componentes

Se ha visto la correspondencia entre curvas planas afines y polinomios en $\mathbb{K}[x, y]$ no constantes y sin factores múltiples. Una curva plana afin se corresponde con un polinomio en $\mathbb{K}[x, y]$, que es único salvo multiplicación escalar.

En el caso práctico es mas útil la siguiente definición.

Definición 30 *Si $F, G \in \mathbb{K}[x, y]$ entonces decimos que los polinomios son* equivalentes *si existe $\lambda \in \mathbb{K}$ tal que $F = \lambda G$. Esta relación entre polinomios es una relación de equivalencia, y nos ayuda a definir una curva plana afín al tomar las clases de equivalencia, es decir, una curva plana afín será, desde este punto en nuestro trabajo, una clase de equivalencia dada la relación anterior.*

El *grado de una curva* plana afín se define entonces, de manera natural, como el grado del polinomio que la define.

Ya vimos que una curva $F \in \mathbb{K}[x, y]$ tiene una representación en factores irreducibles $F_i \in \mathbb{K}[x, y]$, de manera que $F = \prod F_i^{e_i}$ con $e_i \in \mathbb{Z}$. Diremos

que F_i es una *componente* de F con *multiplicidad* e_i, con lo cual podremos nombrar a F_i como *simple* si $e_i = 1$ o *múltiple* en caso contrario. Es importante notar que conociendo $V(F)$ podemos conocer las componentes F_i de F, pero no así sus multiplicidades.

Si F es irreducible $V(F)$ es una variedad, y denotaremos en lo sucesivo $\Gamma(F) = \Gamma(V(F))$, $k(F) = k(V(F))$ y $\mathcal{O}(F) = \mathcal{O}(V(F))$.

Definición 31 *Sea F una curva y $P = (a, b)$ un punto de $V(F)$. P es llamado* punto simple *si $F_x(P) \neq 0$ o $F_y(P) \neq 0$. En este caso podemos definir una nueva curva de la siguiente manera*

$$F_x(P)(x - a) + F_y(P)(y - b) = 0$$

Esta es llamada la tangente *a F en P. Un punto* no simple *se conoce como* multiple *o* singular*.*

Una curva con solo puntos simples se llamará *curva no singular*.

Definición 32 *Tomemos una curva F y $P = (0, 0)$, escribamos ahora $F = \sum_{j=m}^{n} F_j$ con F_j forma de grado j y $F_m \neq 0$.Definimos la* multiplicidad *de F en $P = (0, 0)$ como $m = m_P(F)$.*

Notemos ahora que de esta manera P está en F si y solo si $m_P(F) > 0$, P es punto simple si y solo si $m_P(F) = 1$ y en este caso la tangente a F en P es F_1.

Como F_m es una forma en dos variables, podemos escribir $F_m = \prod L_i^{r_i}$ con L_i lineas, y son llamadas las *tangentes a F en P*. El número r_i es la multiplicidad de L_i, si $r_i = 1$ entonces L_i es *simple*, y si F tiene m tangentes simples distintas en P decimos que P es un *punto ordinario múltiple*. Un punto ordinario doble es llamado nodo.

Por conveniencia diremos que una linea que pasa por P en F, sin ser tangente, es una tangente de multiplicidad 0.

Nuevamente consideremos la representación de F en componentes irreducibles, es decir $F = \prod F_i^{e_i}$, es fácil ver que $m_P(F) = \sum e_i m_P(F_i)$ y que si L es tangente a F_i de multiplicidad r_i entonces L es tangente a F con multiplicidad $\sum e_i r_i$.

De lo anterior vemos que P es simple si y solo si se cumplen las siguientes tres condiciones
1.- P pertenece solo a una F_i,
2.- F_i es simple en F y
3.- P es simple en F_i.

Hasta ahora solo hemos considerado el caso cuando $P = (0,0)$, pero podemos extender las definiciones dadas a el caso general, cuando $P = (a,b)$, basta tomar la traslación T de manera que $T(a,b) = (0,0)$. Esta transformación de coordenadas se comporta de manera que manda las lineas tangentes a F^T en $(0,0)$ a las lineas tangentes a F en P, además de que los valores de las multiplicidades, y por tanto la definición de punto simple, no sufre cambios al aplicar la traslación.

A continuación tomaremos, dada F una curva plana irreducible y $G \in \mathbb{K}[x,y]$, como g a la clase de equivalencia de G en $\Gamma(F)$, es decir, $g = \pi(G)$ con π la proyección de en $\Gamma(F)$.

Teorema 33 *Sea F una curva plana irreducible y P un punto en F. P es punto simple de F si y solo si $\mathcal{O}_p(F)$ es un anillo de valuación discreta, en este caso si $l = \pi(L)$, con L una linea tangente a F en P de multiplicidad cero, es un parámetro uniformizante para $\mathcal{O}_p(F)$.*

Por medio de este teorema podemos establecer una función sobre $k(F)$ que asocie a cada $G \in k(F)$ un número entero no negativo, esto de la siguiente manera.

Si P es un punto simple, de una curva F irreducible, el teorema anterior nos indica que $\mathcal{O}_p(F)$ es un anillo de valuación discreta, por lo tanto podemos definir la función $ord_P^F : k(F) \to \mathbb{Z}$ de manera que $ord_P^F(G) = r$ con $l^r = g$.

Si F esta fija solo escribiremos ord_P. Si $G \in \mathbb{K}[x,y]$ denotamos $ord_P(G) = ord_P(g)$ con $g = \pi(G)$.

La función anterior se puede extender a curvas F reducibles, basta definir $ord_P^F = ord_P^{F_i}$ donde F_i es la componente de F que contiene a P.

La función que acabamos de dar nos permite caracterizar a las lineas tangentes a F en P, por medio del valor obtenido al aplicarles esta función. Como podemos observar L no es tangente si $ord_P(L) = 1$ y es tangente si $ord_P(L) > 1$.

El siguiente teorema nos ofrece una manera de calcular las dimensiones de espacios vectoriales del tipo $\mathcal{O}(V)/I$, donde I es un ideal de $\mathcal{O}(V)$.

Teorema 34 *Sea P un punto en una curva F. Entonces*

$$m_P(F) = \dim_{\mathbb{K}}(M_P(F)^n / M_P(F)^{n+1})$$

para todas las n suficientemente grandes. En particular, la multiplicidad de F en P depende solo del anillo local $\mathcal{O}_p(F)$.

Notemos que si el anillo $\mathcal{O}_p(F)$ es de valuación discreta, entonces este teorema nos muestra que $m_P(F) = 1$ con lo cual P es simple en F, como se esperaba.

Existe un polinomio en la variable n (para n grande) muy importante para el estudio de anillos locales y multiplicidades, llamado *polinomio de Hilbert-Samuel*, definido por $\chi(n) = \dim_{\mathbb{K}}(\mathcal{O}/M^n)$.

1.4.6. Número de intersección

Definiremos el *numero de intersección* de F y G, curvas planas, en $P \in \mathbb{A}^2$ y lo denotamos por $I(P, F \cap G)$, de manera que cumpla las siguientes propiedades.

1.- $I(P, F \cap G)$ es un número entero no negativo, para cualquier elección de F, G y P que tomemos, siempre y cuando F y G no tengan componentes comunes, esto último se conoce como *intersección propia*. En caso de que la las dos curvas no se intersecten propiamente se tendrá que $I(P, F \cap G) = \infty$.

2.- $I(P, F \cap G) = 0$ si y solo si P no pertenece a la intersección de las curvas. Este número depende solo de las componentes de F y G que pasen por P.

3.- Para cualquier cambio de coordenadas T, de manera que $T(Q) = P$, se tiene que $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

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

5.- $I(P, F \cap G) \geq m_P(F)m_P(G)$, donde la igualdad se cumple si y solo si F y G no tienen tangentes comunes en P, esta propiedad se conoce como *intersección transversal*.

6.- Si $F = \prod F_i^{r_i}$ y $G = \prod G_j^{s_j}$ entonces $I(P, F \cap G) = \sum \sum r_i s_j I(P, F_i \cap G_j)$.

7.- Si F es irreducible entonces $I(P, F \cap G)$ solo depende de la imagen de G en $\Gamma(F)$, es decir $I(P, F \cap G) = I(P, F \cap (G + AF))$ para cualquier $A \in \mathbb{K}[x, y]$.

Con estas propiedades que estamos requiriendo de $I(P, F \cap G)$ se obtiene el siguiente teorema.

Teorema 35 *Existe un número de intersección único $I\,(P,\ F \cap G)$ definido para todas las curvas planas $F,\ G$, y todo punto $P \in \mathbb{A}^2$, tal que satisface las propiedades (1)-(7). Viene dado por la fórmula*

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

Demostración. *Unicidad:* Es suficiente dar un procedimiento constructivo para calcular $I\,(P,\ F \cap G)$ utilizando sólo las propiedades (1)-(7). Podemos suponer $P = (0, 0)$ (por (3)), y que $I\,(P,\ F \cap G)$ es finito (por(1)). El caso en que $I\,(P,\ F \cap G) = 0$ ya se ha considerado en (2), por lo tanto podemos suponer por inducción 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. Podemos suponer $r \leq s$ (por (4)).
Caso 1: $r = 0$. Entonces Y divide a F, por lo tanto $F = YH$ y (por (6)) es

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

Si $G(x,0) = x^m(a_0 + a_1x + \cdots),\ a_0 \neq 0$, entonces

$$I(P,\ Y \cap G) = I(P,\ F \cap G(x,0)) = I(P,\ Y \cap x^m) = m$$

(por (7), (2), (6) y (5)). 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 $H = G - X^{s-r}$. Entonces $I(P,\ F \cap G) = I(P,\ F \cap H)$, y $\operatorname{grad}(H(x,0)) = t < s$. Repitiendo este proceso (imtercambiando 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.
Existencia: Definamos $I(P, F \cap G)$ por $\dim_k(\mathcal{O}_p(\mathbb{A}^2)/(F,\ G))$. Deberemos demostrar que satisface las propiedades (1)-(7). Como $I(P, F \cap G)$ depende sólo del ideal de $\mathcal{O}(\mathbb{A}^2)$ generado por F y G, las propidades (2), (4) y (7) son obvias. Como un cambio de coordenadas afines induce un isomorfismo de anillos locales, (3) es también evidente. Podemos, por lo tanto, suponer que $P = (0,0)$ y que todas las componentes de F y de G pasan por P. Sea $\mathcal{O} = \mathcal{O}_p(\mathbb{A}^2)$.
Si F y G no tienen componentes comunes, $I(P, F \cap G)$ es finito (en virtud del corolario 24). Si F y G tienen una componente común H, entonces $(F,\ G) \subset (H)$, por lo tanto existe un homomorfismo de $\mathcal{O}/(F,\ G)$ sobre $\mathcal{O}/(H)$ e $I(P, F \cap G) \geq \dim_k(\mathcal{O}/(H))$. Pero $\mathcal{O}/(H)$ es isomorfo a $\mathcal{O}_p(H)$ y $\mathcal{O}_p(H) \supset \Gamma(H)$, y $dim_k\Gamma(H) = \infty$ por el corolario 16. Esto prueba (1).
Para comprobar (6), 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 $\varphi : \mathcal{O}/(F, GH) \to \mathcal{O}/(F, G)$ el homomorfismo natural, y definamos una aplicación k-lineal $\psi : \mathcal{O}/(F, H) \to \mathcal{O}(F, GH)$ haciendo $\psi(\overline{z}) = \overline{G}\overline{z}$, (las barras indican las clases residuales). En virtud de un teorema de sucesiones exactas, es suficiente probar que la sucesión

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

es exacta.
Verificaremos que ψ es uno a uno; es resto es fácil. Si $\psi(\overline{z}) = 0$; $Gz =$

$uF+vGH$, $u, v \in$O. Elijamos $S \in k[x,y]$ con $S(P) \neq 0$ y $Su = A$, $Sv = B$, 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 $C - BH = DF$. Luego $z = (B/S)H + (D/S)F$, por lo tanto $\overline{z} = 0$, que acaba la demostración.
La propiedad (5) es la más dificil. Sea $m = m_P(F)$, $n = m_P(G)$. Sea I el ideal de $k[x,y]$ generado por X e Y. Consideremos el siguiente diagrama de espacios vectoriales y aplicaciones lineales :

$$\begin{array}{ccccccc} {}^{k[x,y]}/_{I^n} \times {}^{k[x,y]}/_{I^m} & \xrightarrow{\psi} & {}^{k[x,y]}/_{I^{n+m}} & \xrightarrow{\varphi} & {}^{k[x,y]}/_{(I^{m+n},F,G)} & \rightarrow & 0 \\ & & & & \downarrow \alpha & & \\ & & {}^{\mathcal{O}}/_{(F,G)} & \xrightarrow{\pi} & {}^{\mathcal{O}}/_{(I^{m+n},F,G)} & \rightarrow & 0 \end{array}$$

π, y α son los homomorfismos naturales (de anillos), y ψ se define por $\psi\left(\overline{A}, \overline{B}\right) = \overline{AF + BG}$. φ y π son evientemente epiyectivas, y como
$V\left(I^{m+n}, F, G\right) \subset \{P\}$, α es un isomorfismo por el (cor. 25). Es fácil ver que la primera fila es exacta. Ello 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

$$dim\left(k[x,y]/\left(I^{m+n}, F, G\right)\right) = dim\left(k[x,y]/I^{m+n}\right) - dim(\ker(\varphi))$$

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

$$\begin{aligned} I(P, F \cap G) &= \dim(\mathcal{O}/(F,G)) \geq \dim\left(\mathcal{O}/\left(I^{m+n}, F, G\right)\right) = \\ &= \dim\left(k[x,y]/\left(I^{m+n}, F, G\right)\right) \geq \\ &\geq \dim\left(k[x,y]/I^{m+n}\right) - \dim(k[x,y]/I^n) - \dim(k[x,y]/I^m) \\ &= mn \end{aligned}$$

Todo lo cual 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 $I^{m+n} \subset (F,G)\mathcal{O}$. La segunda es una igualdad si y sólo si ψ es uno a uno. La propiedad (5) es, por lo tanto, una consecuencia del siguiente lema. ■

Lema 36 *(a) Si F y G tienen tangentes distintas en P, entonces $I^t \subset (F,G)\mathcal{O}$ 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 $L_1, ..., L_m$ las tangentes a F en P, $M_1, ..., M_n$ las tangentes a G. Sea $L_i = L_m$ si $i > m$, $M_j = M_n$ si $j > n$, y sea $A_{ij} = L_1 \cdot ... \cdot L_i \cdot M_1 \cdot ... \cdot M_j$ para todo $i, j \geq 0$ $(A_{00} = 1)$. $\{A_{ij} \mid i + j = t\}$ constituye una base del espacio vectorial de todas las formas de grado t de $k[x, y]$.

Para demostrar (a) es suficiente, por lo tanto, probar que $A_{ij} \in (F, G)\mathcal{O}$ para todo $i+j \geq m+n-1$. Pero $i+j \geq n+m-1$ implica que $i \geq m$ ó $j \geq n$. Si $i \geq m$, es $A_{ij} = A_{mo}B$, donde B es una forma de grado $t = i + j - m$. $F = A_{mo} + F'$, donde todos los términos de F' son de grado $\geq m + 1$. Entonces $A_{ij} = BF - BF'$, donde cada uno de los términos de BF' tiene grado $\geq i + j + 1$. Habremos terminado si podemos probar que $I^t \subset (F, G)$ para todo t suficientemente grande.

Este hecho es, sin duda, una concecuencia del "teorema de los ceros" : sea $V(F, G) = \{P, Q_1, ..., Q_s\}$, y elijamos un polinomio H tal que $H(Q_i) = 0, H(P) \neq 0$. $HX, HY \in I(V(F, G))$, por lo tanto $(HX)^N, (HY)^N \in (F, G) \subset k[x, y]$ para un cierto N. H^N es unitario en $\mathcal{O}$, luego $X^N, Y^N \in (F, G)\mathcal{O}$ y por lo tanto $I^{2N} \subset (F, G)\mathcal{O}$, como se pretendía.

(b) supongamos que las tangentes son distintas y que

$$\psi\left(\overline{A}, \overline{B}\right) = \overline{AF + BG} = 0$$

es decir, que $AF + BG$ consta exclusivamente de términos de grado $\geq m+n$. Escribamos $A = A_r +$ términos de grado superior, $B = B_s + ...$, luego

$$AF + BG = A_r F_m + B_s G_n + ...$$

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 en comunes, luego F_m divide a B_s, y G_n divide a A_r. Por lo tanto, $s \geq m,\ r \geq m$, y en consecuencia $\left(\overline{A}, \overline{B}\right) = (0, 0)$.

Recíprocamente, si L fuese tangente común a F y a G en P, se tendría $F_m = LF'_{m-1}$, $G_n = LG'_{n-1}$. Podemos entonces $\psi\left(G'_{n-1}, -F'_{m-1}\right) = 0$ y por lo tanto ψ no sería uno a uno. Esto completa la demostración del lema, y también la del teorema 35. ■

Teorema 37 *Sean F y G dos curvas planas y P un punto de $\mathbb{A}^2$, entonces $I(P, F \cap G)$ es único y cumple las propiedades arriba mencionadas, además $I(P, F \cap G) = \dim_{\mathbb{K}}(\mathcal{O}_p(\mathbb{A}^2) \diagup (F, G))$.*

Lema 38 *Sean F y G dos curvas planas y P un punto de $\mathbb{A}^2$. Si F y G no tienen tangentes distintas en P entonces $(x,y)^t \subseteq (F,G)\mathcal{O}$ para toda $t \geq m+n-1$, donde $m = m_P(F)$ y $n = m_P(G)$.*

Las propiedades del número de intersección pueden ser reducidas a un número menor de ellas, haciendo uso de algunas redundancias que entre ellas se tiene. Por otro lado existen dos propiedades más que son de interés.

8.- Si P es un punto simple de F entonces $I(P, F \cap G) = ord_P^F(G)$.

9.- Si F y G no tienen componentes comunes entonces $\sum_P I(P, F \cap G) = \dim_{\mathbb{K}}(\mathbb{K}[x,y]/(F,G))$.

Podemos extender las definiciones dadas hasta ahora para variedades afines al caso proyectivo, haciendo las aclaraciones previas correspondientes.

En el caso proyectivo las curvas planas son hipersuperficies en $\mathbb{P}^2$, y como en el caso afín, diremos que dos curvas planas proyectivas $F, G \in \mathbb{K}[x,y,z]$ son equivalentes si existe $\lambda \in \mathbb{K}$ tal que $F = \lambda G$. De esta manera una curva plana proyectiva es definida como una clase de equivalencia bajo la relación anterior. Así mismo definimos el grado de una curva plana proyectiva como el grado de la forma que la define. A partir de este punto la notación usada para curvas planas proyectivas y las curvas planas afines será la misma, si no se presta a confusión, en cuyo caso se hará la aclaración pertinente.

Notemos que, en algunos casos, se puede pasar del caso proyectivo al caso afín, por ejemplo, si tomamos un $P = (x,y,1)$ entonces $\mathcal{O}(F)$ es isomorfo a $\mathcal{O}_{(x,y)}(F_* = F(x,y,1))$.

Los resultados que hemos encontrado en el caso afín nos ayudan a dar definiciones para el caso poyectivo. Una manera de hacerlo es deshomogeneizar una forma F, que define una curva proyectiva, y aplicar lo que sabemos a F_*, que es una curva afín.

Definición 39 *Definimos la* multiplicidad $m_P(F)$ *de un punto $P \in \mathbb{P}^2$ en una curva plana proyectiva de manera que, si $P \in \mathbb{U}_i$ con $i = 1,\ 2$ ó 3, deshomogeneizamos F respecto a x_i y $m_P(F) = m_P(F_*)$.*

La multiplicidad, definida de esta manera, es independiente de la elección de $\mathbb{U}_i$ e invariante bajo transformación de coordenadas.

Si consideramos un conjunto finito de puntos de $\mathbb{P}^2$, digamos $\{P_1, ..., P_n\}$, entonces podemos encontrar una linea L que no pasa por ninguno de ellos. Si F es una curva de grado d entonces $F_* = F/L^d \in k(F)$. Es claro que F_* depende de la elección de L, pero también podemos ver fácilmente que, si tomamos una L' que tampoco pase por ninguno de los P_i, entonces $F/L^d = (L/L')^d F_*$, y como L/L' es una unidad en cada $\mathrm{O}_{P_i}(\mathbb{P}^2)$ podemos decir que F_* es única en $k(F)$ salvo unidades de $\cap \mathrm{O}_{P_i}(\mathbb{P}^2)$.

Tambien podemos ver que bajo transformaciones de coordenadas, podemos hacer que L se convierta en la linea Z a infinito, luego, bajo la identificación natural de $k(\mathbb{A}^2)$ con $k(\mathbb{P}^2)$, notamos que nuestra nueva forma de definir F_* es la misma que la original, $F_* = F(x, y, 1)$.

Si P es un punto simple de una curva irreducible F, entonces $\mathcal{O}_p(F)$ es un anillo de valuación discreta.

Definición 40 *Sean F una curva irreducible, P un punto simple de F y $G \in k(F)$. Definimos la* función de orden en $k(F)$*, y la denotamos ord_P^F, como*

$$ord_P^F(G) = ord_P^F(\overline{G_*})$$

donde $G_* \in \mathcal{O}_p(\mathbb{P}^2)$ y $\overline{G_*} \in \mathcal{O}_p(F)$.

Definición 41 *Sean F y G curvas planas proyectivas y P un punto en $\mathbb{P}^2$. Definimos el* número de intersección *de F y G en P, y lo denotamos por $I(P, F \cap G)$, como*

$$I(P, F \cap G) = \dim_{\mathbb{K}}(\mathcal{O}_p(\mathbb{P}^2)/(F_*, G_*))$$

.

Esta definición es independiente de la forma en que tomemos F_* y G_*, además cumple las propiedades 1-8 de la correspondiente al caso afín, tomando en cuenta que T debe ser un cambio de coordenadas proyectivo y en 7 A debe ser una forma con $\mathrm{grad}(A) = \mathrm{grad}(G) - \mathrm{grad}(F)$.

Podemos definir a una linea L como *tangente* si $I(P, F \cap L) > m_p(F)$, además P es un punto múltiple ordinario de F si F tiene $m_p(F)$ tangentes distintas en P.

Dos curvas F y G se dice que son *proyectivamente equivalentes* si existe un cambio de coordenadas proyectivo T tal que $F^T = G$, con lo cual el estudio que se siga haciendo a lo largo de este trabajo se aplica por igual a curvas proyectivamente equivalentes.

El siguiente teorema es de suma importancia en este trabajo, en él se determina el número de intersecciones de dos curvas sin componentes comunes.

1.5. Teorema de Bezout

Teorema 42 (De Bezout) *Sean F y G curvas planas proyectivas, sin componentes comunes, y $m = \text{grad}(F)$, $n = \text{grad}(G)$, entonces*

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = mn$$

Al combinar la propiedad cinco del número de intersección y el teorema de Bezout, podemos deducir los siguientes corolarios.

Corolario 43 *Si F y G no tienen componentes comunes entonces*

$$\sum_{P \in \mathbb{P}^2} m_P(F) m_P(G) \leq \text{grad}(F)\,\text{grad}(G)$$

Corolario 44 *Si F y G se encuentran en $\text{grad}(F)\,\text{grad}(G)$ puntos distintos, entonces estos puntos son simples.*

Corolario 45 *Si dos curvas F y G con $m = \text{grad}(F)$ y $n = \text{grad}(G)$, tiene mas de mn puntos comunes,entonces tienen componentes comunes.*

Una aplicación del teorema de Bezout nos muestra que si F es una curva irreducible de grado n y m_P es la multiplicidad de F en P, entonces

$$\sum_{P\in\mathbb{P}^2} \frac{m_P\,(m_P-1)}{2} \leq \frac{n(n-1)}{2}$$

Podemos mejorar aún más la cota que restringe a la suma, asi tenemos el siguiente teorema.

Teorema 46 *Si F es una curva irreducible de grado n y m_P es la multiplicidad de F en P, entonces*

$$\sum_{P\in\mathbb{P}^2} \frac{m_P\,(m_P-1)}{2} \leq \frac{(n-1)(n-2)}{2}$$

Si aplicamos este teorema a los casos donde $1 \leq n \leq 4$ podemos ver que las lineas y las cónicas irreducibles son no singulares, una cónica irreducible puede tener a lo sumo un punto doble, las cuárticas irreducibles tienen a lo sumo tres puntos dobles o un punto triple.

Para nuestro siguiente teorema, de suma importancia para nuestro trabajo, necesitamos primero la siguiente sección.

1.6. Ciclos

Definición 47 *Un* cero-ciclo *en $\mathbb{P}^2$ es una suma formal $\sum_{P\in\mathbb{P}^2} n_P P$, donde n_P es un entero, todos ellos cero excepto un número finito.*

El conjunto de los cero-ciclos en $\mathbb{P}^2$ forman un grupo abeliano, de hecho isomorfo al grupo abeliano libre con base $X = \mathbb{P}^2$ que se definió antes. El *grado de un cero-ciclo* $\sum_{P\in\mathbb{P}^2} n_P P$ lo definimos como $\sum_{P\in\mathbb{P}^2} n_P$. Un cero-ciclo es *positivo* si cada n_P es mayor o igual a cero, además podemos comparar de cierta manera dos ciclos $\sum_{P\in\mathbb{P}^2} n_P P$ y $\sum_{P\in\mathbb{P}^2} m_P P$, diremos que $\sum_{P\in\mathbb{P}^2} n_P P$ es mayor que $\sum_{P\in\mathbb{P}^2} m_P P$, y escribiremos $\sum_{P\in\mathbb{P}^2} n_P P \succ \sum_{P\in\mathbb{P}^2} m_P P$, si cada $n_P \geq m_P$.

Definición 48 *Sean F y G curvas planas proyectivas, sin componentes comunes, $m = \text{grad}(F)$ y $n = \text{grad}(G)$. Definimos el* ciclo de intersección *de F y G, y lo denotamos por $F \cdot G$, como*

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

.

El teorema de Bezout nos asegura que $F \cdot G$ es un cero-ciclo positivo de grado mn.

Algunas propiedades del número de intersección se heredan al ciclo de intersección, por ejemplo

(a) $F \cdot G = G \cdot F$

(b) $F \cdot GH = F \cdot G + F \cdot H$

(c) $F \cdot (G + AF) = F \cdot G$ si A es una forma con $\text{grad}(A) = \text{grad}(G) - \text{grad}(F)$.

Sopongamos que F, G y H son curvas y que $F \cdot G \succ F \cdot H$, es decir, H intersecta a F en un ciclo mayor que el correspondiente a G, esto plantea la pregunta ¿Existe una curva B tal que $B \cdot F = H \cdot F - G \cdot F$?

Notemos que en caso de que B exista, tiene que cumplir que $\text{grad}(B) = \text{grad}(H) - \text{grad}(G)$. Para encontrar tal B es suficiente que demos dos formas A y B de tal manera que $H = AF + BG$, con lo cual, al aplicar una de las propiedades arriba mencionadas, tendremos que $H \cdot F = BG \cdot F = B \cdot F + G \cdot F$.

Condición 49 (de Noether) *Sean F, G y H curvas, F y G sin componentes comunes y P un punto de $\mathbb{P}^2$. Decimos que se satisfacen la* condicion de Noether *en P, con respecto a F, G y H, si $H_* = aF_* + bG_*$ con a y b elementos de $\mathcal{O}_p(\mathbb{P}^2)$, es decir, $H_* \in (F_*, G_*) \subset \mathcal{O}_p(\mathbb{P}^2)$.*

El siguiente teorema relaciona propiedades locales con globales.

Teorema 50 (fundamental de Max Noether) *Sean F, G y H curvas proyectivas, F y G sin componentes comunes. Entonces exiten formas A y B, con*

$\text{grad}(A) = \text{grad}(H) - \text{grad}(F)$ *y* $\text{grad}(B) = \text{grad}(H) - \text{grad}(G)$*, tales que* $H = AF + BG$ *si y solo si se satisfece la condicion de Noether en todo punto* P *que se encuentre en* $F \cap G$*.*

El uso de este teorema depende en gran medida de asegurar que las condiciones de Noether se satisfagan en cada P de $F \cap G$. Para ello necesitamos la siguiente proposición.

Proposición 51 *Sean* F*,* G *y* H *curvas proyectivas y* P *un punto de* $F \cap G$*. Si cualquiera de las tres siguientes condiciones se satisface, entonces se cumple la condición de Noether en* P *:*
1.- F *y* G *se intersectan transversalmente en* P *y* P *esta en* H*.*
2.- P *es un punto simple de* F*, y* $I(P, H \cap F) \geq I(P, G \cap F)$*.*
3.- F *y* G *tienen distintas tangentes en* P*, y* $m_P(H) \geq m_P(F) + m_P(G) - 1$*.*

La pregunta que se hizo en un párrafo anterior puede ser contestada ahora en base al Teorema Fundamental de Noether y la proposición anterior.

Corolario 52 *Existe una curva* B *tal que* $B \cdot F = H \cdot F - G \cdot F$ *si cualquiera de las dos condiciones siguientes se cumple:*
1.- F *y* G *se intersectan en* $\text{grad}(F)\,\text{grad}(G)$ *puntos distintos, y* H *pasa por todos esos puntos, o*
2.- Todos los puntos de $F \cap G$ *son puntos simples de* F*, y* $H \cdot F \succ G \cdot F$*.*

Como podemos observar, la condición dos de este corolario se restringe solo al caso en que los puntos en $F \cap G$ son puntos simples en F, como se verá despues, podemos dar una condición que quite esta restricción, es decir, para puntos multiples de F.

1.7. Teorema de Riemann-Roch

En lo que resta de este capítulo, C será una curva proyectiva irreducible, $f : X \to C$ el morfismo birracional del modelo no-singular X sobre C. $K =$

$k(C) = K(X)$ el campo de funciones. Los puntos $P \in X$ serán identificados con los lugares de K, ord_p designa la función orden correspondiente sobre K.

1.7.1. Divisores

Un *divisor de* X es 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. Los divisores de X forman un grupo abeliano que es precisamente el grupo abeliano libre sobre el conjunto X.

El *grado de un divisor* es la suma de sus coeficientes: $\text{grad}\left(\sum n_P P\right) = \sum n_P$. Es claro que $\text{grad}(D + D') = \text{grad}(D) + \text{grad}(D')$. $D = \sum n_P P$ se dice que es efectivo (o positivo) si todo $n_P \geq 0$, y escribiremos $\sum n_P P \succ \sum m_P$ si cada $n_P \geq m_P$.

Supongamos que C es una curva plana de grado n, y G es una curva plana que no contenga a C como una componente. Definimos el *divisor de* G, $div(G)$ como $\sum_{P \in X} ord_P(G) P$, donde $ord_P(G)$ está definido por $ord_P(g)$, donde g es la imagen de G_* en el anillo $\mathcal{O}(C)$. Se verifica además que $\sum_{P \in X} ord_P(G) = \sum_{Q \in C} I(Q, C \cap G)$. Por el teorema de Bezout, $div(G)$ es un divisor de grado mn, donde m es el grado de G. Nótese que el $div(G)$ contiene más información que el ciclo de intersección $G.\ C$. Para todo $z \in K$, no nulo, definamos el divisor de z, $div(z)$, por $\sum_{P \in X} ord_P(z) P$.

Como z posee solamente un número finito de ceros y polos $div(z)$ es un divisor bien definido. Si consideramos $(z)_0 = \sum_{ord_P(z) > 0} ord_P(z) P$, como el divisor de los ceros de z, y $(z)_\infty = \sum_{ord_P(z) < 0} - ord_P(z) P$, como el divisor de los polos de z, entonces

$$div(z) = div(z)_0 - div(z)_\infty$$

Nótese que

$$\begin{aligned} div(zz') &= div(z) + div(z') \\ &\text{y} \\ div\left(z^{-1}\right) &= -div(z) \end{aligned}$$

Proposición 53 *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 $z = g/h$, g, h formas del mismo grado en $\Gamma_h(C)$; sabemos que g, h son clases residuales de formas 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 54 *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 $div(z) \succ 0$, $z \in \mathcal{O}_p(x)$ para todo $P \in X$. Si $z(P_0) = \lambda_0$ para algún P_0, entonces $div(z - \lambda_0) \succ 0$ y $\operatorname{grad}(div(z - \lambda_0)) > 0$, lo cual es absurdo, salvo que $z - \lambda_0 = 0$, es decir, $z \in k$. ■

Corolario 55 *Sean z, $z' \in K$, ambos no nulos, entonces $div(z) = div(z')$ si y sólo si $z' = \lambda z$ para un cierto $\lambda \in k$.*

Dos divisores D, D' son linealmente equivalentes si $D = D + div(z)$ para un cierto $z \in k$.

Proposición 56 *(1) La relación $\equiv$ es una relación de equivalencia.*

(2) Si $D \equiv 0$ si y sólo si $D = div\,(z)$, $z \in k$.

(3) Si $D \equiv D'$, entonces grad $(D) =$ grad (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)-(4) Son fáciles de demostrar.

Para probar (5) basta escribir $z = G/G'$, ya que $div\,(z) = div\,(G) - div\,(G')$. ■

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

Supongamos que C es una curva plana que sólo posee puntos multiples ordinarios. Para cada $Q \in X$, sea $r_Q = m_{f_{(Q)}}(C)$. Definamos $E = \sum_{Q \in X} (r_Q - 1)\,Q$. 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* C si y sólo si $m_P\,(G) \geq m_P\,(C) - 1$ para cada uno de los puntos (multiples) $P \in C$. Si C es no-singular, toda curva es adjunta.

Teorema 57 *(del Residuo) Sea $C,\ E$ como en el párrafo anterior. 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. Sean $H,\ H'$ curvas del mismo grado tales que $D + div\,(H) = D' + div\,(H')$. Entonces

$$div\,(GH) = div\,(H') + D' + E + A \succ div\,(H') + E$$

Sea F la forma que define a C. notemos que las condiciones de noether se satisfacen para $F,\ H'$ y GH, lueo $GH = F'F + G'H'$ para ciertos $F',\ G'$, donde grad $(G') = m$. Entonces

$$div\,(G') = div\,(GH) - div\,(H') = D' + E + A$$

como se pretendía. ■

1.7.2. El espacio vectorial L (D)

Sea $D = n_P P$ 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 escogidos, y con polos no "inferiores" a n_P en P; si es así ¿cuantas reflexiones existen?.

Designamos por $L(D)$ al conjunto

$$L(D) = \{f \in K \mid ord_P(f) \geq -n_P \text{ para todo } P \in X\}$$

donde $D = \sum n_P P$. Entonces una función racional f pertenece a $L(D)$ si $div(f) + D \succ 0$, o bien si $f = 0$. $L(D)$ constituye un espacio vectorial sobre k. Designado por $l(D)$ la *dimensión de* $L(D)$; la proposición siguiente prueba que $l(D)$ es finita.

Proposición 58 *(1) SI* $D \prec D'$, *entonces* $L(D) \subset L(D')$, *y*

$$\dim_k (L(D')/L(D)) \leq \operatorname{grad}(D' - D)$$

(2) $L(0) = k$; $L(D) = 0$ *si* $\operatorname{grad}(D) < 0$.
(3) $L(D)$ *es de dimensión finita para todo* D. *Si* $\operatorname{grad}(D) \geq 0$, *entonces* $l(D) \leq \operatorname{grad}(D) + 1$
(4) Si $D \equiv D'$, *entonces* $l(D) = l(D')$.

Demostración. (1) $D' = D + P_1 + \cdots + P_s$ y $L(D) \subset L(D + P_1) \subset \cdots \subset L(D + P_1 + \cdots P_s)$, luego es suficiente probar que

$$dim(L = (D + P)/L(D)) \leq 1$$

Para comprobarlo, sea t un parámetro de uniformización de $\mathcal{O}(X)$, 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 $\overline{\varphi}$:

$L(D+P)/L(P) \to k$ que da el resutado.
(2) : Este se sigue de la prop. 53, cor. 54 y de la prop 56 (3).
(3) : Si $\text{grad}(D) = n \geq 0$, elegimos $P \in X$, y consideramos $D' = D - (n+1)P$.

Entonces $L(D') = 0$, y por (1), $dim(L(D)/L(D')) \leq n+1$, por lo tanto $l(D) \leq n+1$.

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

Con más generalidad, para todo subconjunto S de X, y todo divisor $D = \sum n_P P$ de X, definimos $\text{grad}^s(D) = \sum_{P \in S} n_P$, y

$L^S(D) = \{f \in K \mid ord_P(f) \geq -n_P \text{ para todo } P \in S\}$. ■

Lema 59 *Si $D \prec D'$, entonces $L^S(D) \subset L^S(D')$. Si S es finito, entonces $dim\left(L^S(D')/L^S(D)\right) = \text{grad}^S(D'-D)$.*

Demostración. Procediendo como en la prop 58 supondremos que $D' = D + P$, y definiremos $\varphi : L^S(D+P) \to k$, por el mismo cambio. Debemos probar que φ aplica $L^S(D+P)$ sobre k, es decir, $\varphi \neq 0$, por lo tanto $\overline{\varphi}$ es un isomorfismo. Entonces hemos de encontar en $f \in K$ con $ord_P(f) = -r-1$, y con $ord_Q(f) \geq -n_Q$ para todo $Q \in S$. Pero esto es fácil, ya que S es finito. ■

La proposición es un primer paso importante para el calculo de las dimenciones $l(D)$. La demostración hace uso únicamente del campo de funciones racionales.

Proposición 60 *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 $l(r(x)_0) \geq rn - \tau$ para todo r.

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

Sea $S = \{P \in X \mid n_P > 0\}$ y elejimos $v_1, ..., v_m \in L^S(0)$ tales que los residuos $\overline{v_1}, ..., \overline{v_m} \in L^S(0)/L^S(-Z)$ formen una base de este espacio vectorial. Probaremos que $v_1, ..., v_m$ 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 $\sum \lambda_i \overline{v} = 0$, lo cual es absurdo. Luego $m \leq n$.

Lo que a continuación sigue prueba (2).

Sean $w_1, ..., w_n$ una base de K sobre $k(x)$. Podemos suponer que cada w_i satisface una ecuación del tipo

$$w_i^{n_i} + a_{i1} w_i^{n_{i-1}} + \cdots = 0, a_{ij} \in k\left[x^{-1}\right]$$

Entonces $ord_P(w_i^{n_i}) < ord_P\left(a_{ij} w_i^{n_{i-j}}\right)$, que es imposible. Se sigue entonces que para un cierto $t > 0$ se tiene que $div(w_i) + tZ \succ 0$, $i = 0, 1, ..., n$. Entonces $w_i x^{-j} \in L((r+t)Z)$ para $i = 1, ..., n$, $j = 0, 1, ...r$. Como los w_i son independientes sobre $k(x)$, y $1, x^{-1}, ..., x^{-r}$ son independientes sobre k, $\{w_i x^{-1} \mid i = 1, ..., n;\ j = 0, ..., r\}$ son independientes sobre k. Por lo tanto $l((r+t)Z) \geq n(r+1)$. Pero

$$l((r+t)Z) = l(rZ) + \dim\left(L((r+t)Z)/L(rZ)\right) \leq l(rZ) + tm$$

por la proposición 58 (1). En consecuencia

$$l(rZ) \geq n(r+1) - tm = rn - \tau$$

como deseábamos. Finalmente, como $rn - \tau \leq l\ (rZ) \leq rm + 1$, si elegimos r suficientemente grande, vemos que $n \leq m$. ■

Corolario 61 *Las siguientes proposiciones son equivalentes :*
(1) C es racional.
(2) X es isomorfo a P^1.
(3) Existe un $x \in K$ con $\operatorname{grad}(x)_0 = 1$.
(4) Para algún $P \in X$, es $l(P) > 1$.

Demostración. (4) dice que existe un $x \in L(P)$, no constante, tal que $(x)_\infty = P$. Luego $\operatorname{grad}((x)_0) = \operatorname{grad}((x)_\infty) = 1$, por lo tanto $[K : k(x)] = 1$, es decir, $K = k(x)$ es racional. El resto es fácil. ■

1.7.3. Teorema de Riemann

Si D es un divisor grande, $L(D)$ también lo es. La proposición 60 lo prueba para un tipo especial de divisores.

Teorema 62 *(Riemann) Existe una constante g tal que*

$$l(D) \geq \operatorname{grad}(D) + 1 - g$$

para todos los divisores D. El menor de tales g se denomina género *de X. (o de K, o de C). g es un entero no negativo.*

Demostración. Para cada D, sea $S(D) = \operatorname{grad}(D) + 1 - l(D)$. Deseamos encontrar un g tal que $S(D) \leq g$ para todo D.

(1) $S(0) = 0$, por lo tanto $g \geq 0$, si existe.

(2) Si $D \equiv D'$, entonces $S(D) = S(D')$.

(3) Si $D \prec D'$, entonces $S(D) \leq S(D')$.

Sea $x \in K$, $x \notin k$, y $Z = (x)_0$, y sea τ el menor entero que verifica la proposición 60 (2). Como $S(rZ) \leq \tau + 1$ para todo r, y como $rZ \prec (r+1)Z$, deducimos de (3) que:

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

Sea $g = \tau + 1$. Para acabar la demostración, bastará probar que (por (2) y (3)) que:

(5) 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 $D' = D - div(f)$, luego 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 grande hará que se verifique. ■

Corolario 63 *Si* $l(D_0) = \text{grad}(D_0) + 1 - g$, *y* $D \equiv D' \succ D_0$, *entonces*

$$l(D) = \text{grad}(D) + 1 - g$$

Corolario 64 *Si* $x \in K$, $x \notin k$, *entonces*

$$g = \text{grad}(r(x)_0) - l(r(x)_0) + 1$$

para todo r *suficientemente grande.*

Corolario 65 *Existe un entero* N *tal que para todo divisor* D *de grado* $> N$

$$l(D) = \text{grad}(D) + 1 - g$$

Demostración. Los dos primeros corolarios se demuestran siguiendo el mismo camino que el de demostrar el teorema de Riemann. Para demostrar el tercero, elijamos D_0 tal que $l(D_0) = \text{grad}(D_0)+1-g$, y sea $N = \text{grad}(D_0)+g$.

Entonces si $\text{grad}(D) \geq N$, $\text{grad}(D - D_0) + 1 - g > 0$, y , por el teorema de Riemann, $l(D - D_0) > 0$. 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 cor. 63. ■

Ejemplo 66 $g = 0$ *si y sólo si* C *es racional. Si* C *es racional,* $g = 0$ *(de la prop 68 siguiente). Reciprocamente. si* $g = 0$, $l(P) > 1$ *para todo* $P \in X$, *y el resultado se sigue del corolario 61.*

Ejemplo 67 $g = 1$ *si y sólo si* C *es birracionalmente equivalente a una cúbica no singular (característica* $(k) \neq 2$*). Ya que si* X *es una cúbica no-singular, el resultado se sigue (de la proposición 68). Reciprocamente, si* $g = 1$, *entonces* $l(P) \geq 1$ *para todo* P. *Por la proposición 58,* $l(P) = 1$, *y por el cor. 1 anterior,* $l(rP) = r$ *para todo* $r > 0$.
Sea 1, x *una base de* $L(2P)$. *Entonces* $(x)_\infty = 2P$, *ya que si* $(x)_\infty = P$, C *sería racional. Luego* $[K : k(x)] = 2$. *Sea* $1, x, y$ *una base de* $L(3P)$. *Entonces* $(y)_\infty = 3P$, *así que* $y \notin k(x)$, *por lo tanto* $K = k(x, y)$. *Como* $1, x, y, x^2, xy, x^3, y^2 \in L(6P)$, *existe una relación de la forma* $ay^2 +$

$(bx+c)\,y = Q\,(x)$, Q un polinomio de grado ≤ 3. Calculando ord_P en ambos miembros vemos que $a \neq 0$ y $\operatorname{grad} Q = 3$, por lo que podemos hacer $a = 1$. Substituyendo y por $y + 1/2\,(bx+c)$, podemos suponer que $y^2 = \prod_{i=1}^{3} (x - \alpha_i)$. Si $\alpha_1 = \alpha_2$, entonces $(y/\,(x-\alpha_1))^2 = x - \alpha_3$, luego $x, y \in k\,(y/\,(x-\alpha_1))$; pero entonces X sería racional, lo cual contradeciría el primer ejemplo. Por lo tanto los α_i son distintos.

Esto prueba que $K = k\,(C)$, donde $C = V\left(Y^2Z - \prod_{i=1}^{3} (X - \alpha_i Z)\right)$ es una cúbica no-singular.

La utilidad del teorema de Riemann depende que sea posible calcular el género de la 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 tienen el mismo género. Como disponemos de un método para encontrar la curva plana que sólo posea puntos múltiples ordinarios que además sea birracionalmente equivalente a una curva dada, la proposición siguiente es todo lo que necesitamos.

Proposición 68 *Sea C una curva plana que sólo posea puntos múltiples ordinarios. Sea n el grado de C, $r_P = m_P\,(C)$. Entonces el género de g de C viene dado por la formula $g = \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \frac{r_p(r_p-1)}{2}$.*

Demostración. Por el cor. 65, necesitamos encontrar un divisor "grande" D para que podamos calcular $l\,(D)$. El teorema de los residuos 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 C en n puntos distintos $P_1, ..., P_n$, y se designa por F la forma que define a C.

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

Consideremos $V_m = \{\text{formas } G \mid \text{grad}(G) = m \text{ y } G \text{ sea adjunto de } C\}$. Como G es adjunta si y sólo si $m_P(G) \geq r_P - 1$ para todo $P \in C$, podemos aplicar un teorema sobre sistemas lineales de curvas para calcular la dimensión de V_m. Encontramos

$$\dim\ V_m \geq \frac{(m+1)(m+2)}{2} - \sum \frac{r_P(r_p-1)}{2}$$

con igualdad si m es grande. (notese que V_m es el espacio vectorial de las formas, 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 formas del mismo grado. Entonces $div(RZ^m) \succ div(S) + E$ y se puede verificar que se cumplen las condiciones de Noether, por lo tanto 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 sucesión de espacios vectoriales es exacta:

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

Donde W_{m-n} es el espacio de todas las formas de grado $m-n$ y $\psi(H) = FH$ con $H \in W_{m-n}$, podemos calcular $\dim L(E_m)$, por lo menos para m grande po un teorema de sucesiones exactas. Resulta, pues, que

$$l(E_m) = \text{grad}(E_m) + 1 - \left(\frac{(n-1)(n-2)}{2} - \sum \frac{r_P(r_P-1)}{2}\right)$$

para m grande. Pero como que $\text{grad}(E_m)$ crece con m, se aplica el cor. 65 para acabar la demostración. ■

Corolario 69 *Sea C una curva plana de grado n, $r_P = m_P(P)$, $P \in C$. Entonces*

$$\frac{(n-1)(n-2)}{2} - \sum \frac{r_P(r_P-1)}{2} \geq g$$

Corolario 70 *Como en el cor. 69 si $\sum \frac{r_P(r_P-1)}{2} = \frac{(n-1)(n-2)}{2}$, entonces C es racional.*

Corolario 71 *(a) Con E_m como en la demostración de la proposición, toda $h \in L(E_m)$ se puede escribir $h = H/Z^m$, donde H es una forma adjunta de grado m.*
(b) $\operatorname{grad}(E_{n-3}) = 2g - 2$. $l(E_{n-3}) \geq g$.

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

Ejemplo 72 *Rectas y cónicas son racionales. Cúbicas no-singulares tienen género uno. Cúbicas singulares son racionales. Puesto que una curva no-singular de grado n, tiene género $\frac{(n-1)(n-2)}{2}$, no toda curva es birracionalmente equivalente a una curva plana no-singular. Por ejemplo $Y^2XZ = X^4 + Z^4$ tiene un nodo, luego es de género 2, y no hay ninguna curva plana no-singular que tenga género 2.*

Si nos restringimos a trabajar con curvas $f(x, y) \in k[x, y]$ de grado d y no singular entonces podemos calcular el género de la curva por medio de la siguiente fórmula, llamada *Fórmula de Plücker*:

$$g = \frac{(d-1)(d-2)}{2}$$

1.7.4. Derivadas y diferenciales

Sea R un anillo que contega 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

$D(xy) = xD(y) + yD(x)$ pára todo $x, y \in R$ de donde se sigue que para todo $F \in k[X_1, ..., X_n]$ y $x_1, ..., x_n \in R$

$$D(F(x_1, ..., x_n)) = \sum_{i=1}^{n} F_{x_i}(x_1, ..., x_n) D(x_i)$$

como k está en todos los anillos omitiremos la frase sobre k.

Lema 73 *Si R es un dominio cuyo campo de funciones 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 $z \in K$, $z = x/y$, $x, y \in R$, entonces como que $x = yz$, he de ser $Dx = y\widetilde{D}z + zDy$, 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 $\sum x_i dy_i$,$x_i, y_i \in R$, 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 construido en base a los siguientes conjuntos de 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 diferencias de R sobre k, y $d : R \to \Omega_k(R)$ es una derivación.

Lema 74 *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 toda $x \in R$.*

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 $\varphi : \Omega_k(R) \to M$. Si $x_1, ..., x_n \in R$, y

$G \in k[X_1, ..., X_n]$, entonces

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

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

Analogamente, si R es un dominio con campo de fracciones K, y $z = x/y \in K$, $x, y \in R$, entonces

$$dz = y^{-1}dx - y^{-1}zdy$$

En particular, si $K = k(x_1, ..., x_n)$, entonces $\Omega_k(R)$ es un espacio vectorial de dimensión finita sobre K, generado por $dx_1, ..., dx_n$. ■

Proposición 75 *(1) Sea K un campo de funciones algebraicas de una variable sobre k. Entonces $\Omega_k(R)$ es un espacio vectorial de dimensión uno sobre K.*
(2) (Si la característica de k es 0) Si $x \in K$, $x \notin k$, entonces dx es una base de $\Omega_k(R)$ sobre K.

Demostración. Sea $F \in k[X, Y]$ una curva afín plana con campo de funciones K, y sea $R = k[X, Y]/(F) = k[x, y]$; $K = k(x, y)$. 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 anterior discusión prueba que dx y dy generan $\Omega_k(R)$ 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 $\Omega_k(R)$, luego $\dim_K(\Omega_k(R)) \leq 1$. Por lo tanto podemos probar que $\Omega_k(R) \neq 0$. Por los lemas 73 y 74 bastará encontrar una derivación no nula $D : R \to M$ para algún espacio vectorial M sobre K. Sea $M = K$, llamaremos $\overline{G}$ a la imagen en R de $G \in k[X, Y]$, y se considera $D(\overline{G}) = G_X(x, y) - uG_Y(x, y)$ vemos además que D es una derivación bien definida, y que $D(x) = 1$, por lo que $D \neq 0$.

De todo ello se sigue (como la característica de k igual a 0) que para todo f, $t \in K$, $t \notin k$, 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 76 *Sea K como en la proposición 75, $\mathcal{O}$ un anillo de K de evaluación 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 prop. 75, podemos suponer que $\mathcal{O} = \mathcal{O}(F)$ 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 $ord_P(x) \geq -N$ y $ord_P(y') \geq -N$. Entonces si $f \in R = k[x,y]$ se tiene que $ord_P(f') \geq -N$, y $f' = f_X(x,y)\,x' + f_Y(x,y)\,y'$.

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

Ahora estamos en condiciones de acabar la demostración. Sea $f \in \mathcal{O}$. Escribamos $f = \sum_{i<N} \lambda_i t^N + t^N g$, $\lambda_i \in k$, $g \in \mathcal{O}$. 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. ■

1.7.5. 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.

Sea $\omega \in \Omega$, $\omega \neq 0$, y $P \in X$ un lugar. Definimos el *orden ω en P*, $ord_P(\omega)$ como sigue: elegido un páramentro de uniformización t de $\mathcal{O}(X)$

escribamos $\omega = fdt$, $f \in K$, y se define $ord_P(\omega) = ord_P(f)$. Para ver que esta definición no depende de la elección del párametro de uniformización, sea u otro páramentro tal que $fdt = gdu$, entonces $f/g = \frac{du}{dt} \in \mathcal{O}(X)$ por la prop. 76, y como además $g/f \in \mathcal{O}(X)$, entonces $ord_P(f) = ord_P(g)$.

Si $0 \neq \omega \in \Omega$, el *divisor de* ω, $div(\omega)$, se define por $\sum_{P \in X} ord_P(\omega) P$. En la proposición 77 probaremos que sólo un número finito verifica $ord_P(\omega) \neq 0$ para un ω dado, luego la definición del $ord(\omega)$ es correta.

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 $div(\omega') \equiv div(\omega)$. Reciprocamente, si $W \equiv W'$ pondremos que $W' = div(f) + W$, y entonces $W' = div(f\omega)$. Por lo tanto los divisores canónicos constituyen una clase de equivalencia respecto a la equivalencia lineal. En particular, todos los divisores canónicos tienen el mismo grado.

Proposición 77 *Supongamos que C es una curva plana de grado $n \geq 3$ que sólo posea puntos múltiples ordinarios. Sea $E = \sum_{Q \in X} (r_Q - 1) Q$, y G una curva plana de grado $n-3$. Entonces $div(G) - E$ es un divisor canónico. (Si $n = 3$, $div(G) = 0$).*

Demostración. Escojamos coordenadas X, Y, Z en P^2 de tal forma que $Z \cdot C = \sum_{i=1}^{n} P_i$, 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 $x = X/Z$, $y = Y/Z \in K$, y F la forma 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 $div(G) - E$, $\text{grad}(G) = n-3$ 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:

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

Notese 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 $P_i \in Z \cap C$. Entonces $y^{-1} = Z/Y$ es un páramentro de uniformización de $\mathcal{O}_{P_i}(X)$, y $dy = -y^2 d(y^{-1})$, luego $ord_Q(dy)\,0-2$. Como $F_X(P_i) \neq 0$, los dos miembros de $(*)$ tiene orden -2 en Q.

Supongamos que Q es un lugar centrado en $P = (a, b,1) \in C$. 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 C en P. Entonces P no es un punto múltiple (por hipótesis), por lo tanto x es un párametro de uniformización, y $F_Y(P) \neq 0$. Además

$$ord_Q(dx) = ord_Q(F_Y) = 0$$

como pretendiamos.

Si Y no es tangente, entonces y es un párametro de uniformización en Q, luego $ord_Q(dy) = 0$, y $ord_Q(f_x) = r_Q^{-1}$ como queríamos. ■

Corolario 78 *Sea W un divisor canónico. Entonces* $\text{grad}(W) = 2g-2$ *y* $l(W) \geq g$.

Demostración. Podemos suponer que $W = E_{n-3}$. Entonces aplicamos el corolario71(b). ■

1.7.6. Teorema de Riemann-Roch

En este célebre teorema se determina el término que falta en la desigualdad del teorema de Riemann para transformarle en igualdad.

Teorema 79 *Sea W un divisor canónico de X. Entonces para todo divisor D*

$$l(D) = \operatorname{grad}(D) + 1 - g + l(W - D)$$

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 precedente para D y $P+D,\ P \in X$; obsérvese que $\operatorname{grad}(D+P) = \operatorname{grad}(D)+1$, mientras que los otros dos términos no constantes cambian por 0 ó 1. El núcleo de la demostración es, por lo tanto el

Lema 80 *(de reducción de Noether)*
Si $l(D) > 0$, y $l(W - D - P) \neq l(W - D)$, entonces

$$l(D + P) = l(D)$$

Demostración. Escojamos C como antes con puntos múltiples ordinarios, y tal que P sea un punto simple de C y por lo tanto $Z \cdot C = \sum_{i=1}^{n} P_i,\ P_i$ 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 $W = E_{n-3}$, y $D \succ 0$ (prop. 77). Luego $L(W - D) \subset L(E_{n-3})$.

Sea $h \in L(W - D)$, $h \notin L(W - D - P)$. Escribamos $h = G/Z^{n-3}\ G$ un adjunto de grado $n-3$ (cor. 71). $div(G) = D + E + A,\ A \succ 0$, pero $A \not\succ P$.

Tomemos la 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 se supone $f \in L(D + P)$; 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 del residuo, luego existe una curva H de grado $n-2$ con $div(H) = (D' + P) + E + (A + B)$.

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

Volvamos ahora a la demostración del teorema. Para cada divisor D, consideremos la ecuación:

Demostración. (Teorema de Riemann-Roch)

$$(*)_D \qquad l(D)=\operatorname{grad}(D)+1-g+l(W-D)$$

Caso 1: $l(W-D)=0$. Como $g\leq l(W)$ (cor. 78) y $l(W)\leq l(W-D)+\operatorname{grad}(D)$, tenemos que $\operatorname{grad}(D)\geq g$ en este caso. Por el teorema de Riemann, $l(D)\geq \operatorname{grad}(D)+1-g\geq 1$, y si $(*)_D$ fuese falso sería $l(D)>1$. Probaremos este caso por inducción respecto $l(D)$. Elijamos un P tal que $l(D-P)=l(D)-1$. Si $(*)_D$ fuese falso, $l(D-P)>0$, por lo tanto el lema de reducción implicaría que $l(W-(D-P))=0$. Aplicando la hipótesis de inducción a $D-P$, $l(D-P)=\operatorname{grad}(D-P)+1-g$, luego $l(D)=\operatorname{grad}(D)+1-g$, que es $(*)_D$.

Caso 2: $l(W-D)>0$. Este caso sólo puede presentarse si $\operatorname{grad}(D)\leq \operatorname{grad}(W)=2g-2$ (prop. 58). Luego podríamos elejir un D maximal para el cual $(*)_D$ sería falso; es decir $(*)_{D+P}$ sería verdad para todo $P\in X$. Escojamos P tal que $l(W-D-P)=l(W-D)-1$. Por el lema de reducción, $l(D+P)=l(D)$. Como $(*)_{D+P}$ es verdad, tenemos

$$\begin{aligned} l(D) &= l(D+P)=\operatorname{grad}(D+P)+1-g+l(W-D-P) \\ &= \operatorname{grad}(D)+1-g+l(W-D) \end{aligned}$$

como queriamos. ■

Corolario 81 *$l(W)=g$ si W es un divisor canónico.*

Corolario 82 *Si $\operatorname{grad}(D)\geq 2g-1$, entonces $l(D)=\operatorname{grad}(D)+1-g$.*

Corolario 83 *Si $\operatorname{grad}(D)\geq 2g$, entonces $l(D-P)=l(D)-1$ para todo $P\in X$.*

Corolario 84 *(Teorema de clifford). Si* $l(D) > 0$, *y* $l(W - D) > 0$, *entonces* $l(D) \leq \frac{1}{2}\operatorname{grad}(D) + 1$.

Demostración. Los tres primeros son propiedades que se siguen directamente del teorema, utilizando la prop. 58. Para el cor. 84, podemos suponer que $D \succ 0,\ D' \succ 0,\ D + D' = W$, también que $l(D - P) \neq l(D)$, para todo P, ya que en otro caso se razona con $D - P$ y se consigna una desigualdad mejor.

Elejido $g \in L(D)$ 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 $\overline{\varphi(f)} = \overline{fg}$ (las barras designan las clases residuales) es uno a uno. Además $l(D') - 1 \leq g - l(D)$. Aplicando el teorema de Riemann-Roch a D' se acaba la demostración. ■

$L(W - D)$ puede ser además interpretado por medio de diferenciales.

Sea D un divisor. Definimos $\Omega(D)$ como el conjunto $\{\omega \in \Omega \mid div(\omega) \succ D\}$, que es un subespacio vectorial de Ω (sobre k). Sea $\delta(D) = \dim_k \Omega(D)$, el *indice de* D. Las diferenciales de $\Omega(0)$ se denominan diferenciales de primera especie (o diferenciales holomórficas, si $k = C$).

Proposición 85 *(1)* $\delta(D) = l(W - D)$.
(2) Existen g *diferenciales linealmente independientes de primer orden sobre* X.
(3) $l(D) = \operatorname{grad}(D) + 1 - g + \delta(D)$.

Demostración. Sea $W = div(\omega)$. Definimos una aplicación lineal

$$\varphi : L(W - D) \to \Omega(D)$$

por $\varphi(f) = f\omega$, φ es un isomorfismo, que prueba (1),(2) y (3) se siguen inmediatamente. ■

Capítulo 2

Teoría de Códigos

La comunicación es de suma importancia en una sociedad, en el proceso de comunicación intervienen cuatro elementos, a saber: fuente, mensaje, medio y receptor. Este proceso se lleva a cabo cuando la fuente desea mandar información, el mensaje, al receptor, para ello el mensaje debe ser transmitido por un medio, en el cual se pueden presentar errores que cambien el mensaje de manera que el receptor obtenga así una información erronea.

En general, el objetivo de la teoría de códigos es la transmisión efectiva de la información, usualmente es confundida con la criptografía, que se encarga de hacer segura la transmisión de los datos a travez de un medio, está centrada en la detección y corrección de errores que se puedan dar en el proceso de la transmisión de un mensaje.

Por ejemplo, el código usado para catalogar los libros es el International Standarized Book Number Code (ISBN) y es muy usado como se puede observar, en la cubierta posterior de los mismos. Este es un código que está a la vista, para poder ser decifrado por cualquier persona con conocimiento de la clave, y además fue diseñado para detectar exactamente un error, de manera que si se presenta una anomalía en la información esta pueda ser detectada. Por desgracia este código no permite saber dónde se ha cometido el error, y por tanto no podremos corregirlo, pero deja abierta la posibilidad de que el mesaje pueda ser enviado nuevamente.

2.1. Parámetros de definición

A lo largo de este capitulo se darán las bases necesarias para el desarrollo de la teoría de códigos en general, con bases algebraicas. Es de vital importancia pues junto con el capítulo anterior darán lugar al tema central de esta tesis. Comenzamos con una definición.

Definición 86 *Un* alfabeto A *es un conjunto de símbolos, los cuales son conocidos por la fuente y el receptor. Un* código C *es un subconjunto de* A^n*, con* $A^n = A \times A \times ... \times A$ n *veces.*

Es fácil ver que esta definición está en total concordancia con nuestra intuición de lo que es un alfabeto en las lenguas escritas. Por su parte un código representa un conjunto de palabras, que son formadas a partir del alfabeto, justo como la lingüística lo señala.

En nuestro caso los alfabetos suelen ser campos finitos, es decir $A = \mathbb{F}_q$ con q potencia de un número primo.

Los elementos de un código, como en el caso lingüístico, son llamados *palabras*. Al ser un código un subconjunto de A^n, definimos como la *longitud del código* a n. En caso de que A sea un campo finito, y C un espacio vectorial sobre el, entonces C es llamado *código lineal sobre* A, en cuyo caso podemos calcular la *dimensión* k *de* C *sobre* A. Existen códigos que no son lineales, es decir, no se pueden ver como subespacio de A^n, pero no serán tratados en este trabajo. Existe un parámetro más de los códigos, el cual junto con n y k da lugar a un código.

Definición 87 *Definimos la* distancia de Hamming *entre dos puntos* $x, y \in \mathbb{F}_q^n$ *como* $d(x, y) := \#\{i \mid x_i \neq y_i\}$.

Esta es una métrica, lo cual es fácil de ver. El parámetro que mencionabamos puede ser definido ahora.

Definición 88 *Sea* C *un código sobre un campo finito* $\mathbb{F}_q$*. Definimos la* distancia mínima de C *como*

$$d_{\text{mín}} = \text{mín}\,\{d(x, y) \mid x \neq y \in C\}$$

Podemos ver que, al definir el *peso* de una palabra como $w(x) = d(x, 0)$, entonces la distancia mínima de un código corresponde al peso mínimo de las palabras en el código distintas de cero.

La importancia de la distancia mínima radica en la posibilidad que nos brinda de establecer la cantidad de errores que un código puede corregir, de manera que no sólo detecta sino a la vez indica cual es el error. Al ser A^n un espacio vectorial y d una métrica, la distancia mínima $d_{\text{mín}}$ nos permite crear bolas centradas en cada palabra de nuestro codigo de manera que, si el radio es $\frac{d_{\text{mín}}-1}{2}$, no se intersecten. Lo anterior nos muestra que si una palabra transmitida sufre a lo sumo $\frac{d_{\text{mín}}-1}{2}$ errores entonces caerá exactamente en una de las bolas centradas en una de las palabras, con lo cual la palabra que se envió se corrige inmediatamente al tomar como corrección al centro de la bola.

Como hemos visto, los parametros que dan forma a cada código son esenciales, pero existen varias relaciones entre ellos que nos restringen a modificarlos a voluntad. Por ejemplo, si queremos corregir una gran cantidad de errores tenemos que encontrar un código con $d_{\text{mín}}$ grande. A su vez si k es grande el código contendrá una cantidad de palabras grande, con lo cual sería un código eficiente para transmitir información.

2.2. Cotas de los parámetros

Los parámetros que definen un código cumplen algunas relaciones, que nos permiten conocer las limitaciones de un código.

Teorema 89 *(cota de Singleton) Sea C un código lineal sobre $\mathbb{F}_q$ con parámetros n, k y d. Entonces*

$$d \leq n - k + 1$$

Demostración. *Definamos el conjunto*

$$W = \left\{a = (a_1, ..., a_n) \in \mathbb{F}_q^n \mid a_d = a_{d+1} = ... = a_n = 0\right\}$$

el cuál, como es fácil ver, tiene distancia mínima, y dimensión, a lo sumo $d-1$. *Esto nos indica que* $C \cap W = \varnothing$ *y por lo tanto*

$$\begin{aligned} \dim(C \cup W) &= \dim C + \dim W \\ &= d + k - 1 \end{aligned}$$

Pero C *y* W *son subespacios de* $\mathbb{F}_q^n$, *por lo tanto*

$$\dim(C \cup W) = d + k - 1 \leq \dim \mathbb{F}_q^n = n$$

con lo que la cota es correcta. ■

Como este trabajo solo se ocupa de códigos lineales no entraremos en detalles acerca de las modificaciones arriba mencionadas.

Cabe resaltar que existen códigos que cumplen la igualdad de la cota de Singleton, estos código son llamados de *Máxima Distancia Separable* o MDS, y su importancia radica en la optimización de los parámetros, por lo cual siempre es bueno encontrar códigos que pertenezcan a esta clase.

2.3. Códigos

2.3.1. Lineales

En este momento tenemos herramientas suficientes para comenzar a desarrollar códigos de manera explícita, al menos los algoritmos que los generan, y encontrar los parámetros y otras propiedades que puedan tener.

Los códigos lineales estan definidos sobre un campo finito y se trabaja con espacios vectoriales sobre este campo, de manera que podemos expresar a las palabras que conforman al código como imagenes de una transformación lineal entre espacios vectoriales.

En general, si tenemos un campo finito $\mathbb{F}_q$ entonces cualquier subespacio de un espacio vectorial definido sobre nuestro campo puede verse como un código. La dimensión k del subespacio es la dimensión de nuestro código,

la dimensión del espacio vectorial es la longitud n del código y la distancia mínima d de éste es el peso mínimo de las palabras diferentes de cero del subespacio.

Un elemento fundamental de la teoría referente a los código lineales es la posibilidad de generarlos por medio de una matriz, llamada matriz generadora, la cual puede encontrarse dando una base para nuestro código, recordemos que es un espacio vectorial, veamos.

Si C es un código lineal de longitud n sobre un campo finito $\mathbb{F}_q$ y k es la dimensión de éste, entonces podemos encontrar una *base para* C, digamos $\{X_1, ..., X_k\}$, de manera que cualquier palabra α de C puede verse como

$$\begin{aligned} \alpha &= a_1X_1 + ... + a_kX_k \\ &= (a_1, ..., a_k)A \end{aligned}$$

donde $(a_1, ..., a_k) \in \mathbb{F}_q^k$ y $A = \begin{pmatrix} X_1 \\ \vdots \\ X_k \end{pmatrix}$ una matriz $k \times n$. A la matriz A le lamaramos *matriz generadora* del código C.

2.3.2. Código Reed-Solomon

Comenzamos con definir al espacio vectorial L_{k-1} de polinomios en una variable respecto al campo $\mathbb{F}_q$.

Definición 90 *Sea $\mathbb{F}_q$ un campo finito y $\mathbb{F}_q[x]$ el anillo de polinomios en una variable sobre el campo $\mathbb{F}_q$. Definimos a L_{k-1} como*

$$L_{k-1} = \{f \in \mathbb{F}_q[x] | \operatorname{grad}(f) < k\}$$

Además es fácil observar que es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión k.

Una vez definido este espacio, y pidiendo que $1 \leq k \leq q-1$, podemos construir el *código Reed-Solomon* $RS(k, q)$ tomando

$$RS(k, q) = \{(f(\alpha_1), ..., f(\alpha_{q-1})) | f \in L_{k-1}\}$$

donde $\alpha_i \in \mathbb{F}_q^*$, es decir, α_i es unidad.

Una forma alterna de construir este código es usar la geometría algebraica, teniendo conocimiento de las definiciones de divisores y los espacios $L(D)$. Veamos pues que si tomamos el espacio proyectivo $\mathbb{P}^2_{\mathbb{F}_q} = \{(\alpha, 1) | \alpha \in \mathbb{F}_q\} \cup \{(1, 0) = P_\infty\}$ y definimos al divisor $D = (k-1)P_\infty$ entonces el espacio L_{k-1}, de la definición anterior, es isomorfo al espacio $L(D)$, basta identificar cada $f \in L_{k-1}$ con su homogeneización $f^* \in \mathbb{F}_q[x, y]$. De estas ideas podemos deducir que el código Reed-Solomon $RS(k, q)$ puede escribirse como

$$RS(k, q) = \{(f(P_1), ..., f(P_{q-1})) \, | f \in L((k-1)P_\infty)\}$$

teniendo en cuenta $P_i = (\alpha_i, 1)$ con $\alpha_i \in \mathbb{F}_q^*$.

A continuación veremos la importancia de estos códigos, la cual radica e que pertenecen a la clase de códigos MDS.

Teorema 91 *Los códigos Reed-Solomon son MDS.*

Demostración. Calculemos los parámetros que caracterizan a un código Reed-Solomon $RS(k, q)$, y veamos que cumplen la igualdad en la cota de Singleton.

Notemos primero que estos son códigos lineales, pues podemos ver que $RS(k, q) \subset \mathbb{F}_q^{q-1}$, más aun, tomando el mapeo de evaluación $\epsilon : L_{k-1} \to \mathbb{F}_q^{q-1}$ y recordemos que ϵ es lineal.

Claramente la longitud $n = q-1$ y la dimensión es a lo sumo k. Para ver que la dimensión del código es exactamente k basta demostrar que el mapeo evaluación es inyectivo, para ello supongamos que existen $f,\ g \in L_{k-1}$ y que $\epsilon(f) = \epsilon(g)$, esto último implica que el polinomio $f - g$ tiene al menos $q - 1$ raices, con lo cual su grado es al menos $q - 1 \geq k$. Pero $f - g \in L_{k-1}$ por lo cual $f = g$ y el mapeo evaluación es inyectivo, así pues la dimensión del código es k.

Para probar la igualdad de los parámetros notemos que si $f \in L_{k-1}$ y $w(\epsilon(f)) = d = d_{\text{mín}}$ entonces f tiene al menos $n - d$ raices, por lo cual su grado es al menos $n - d \leq k - 1$, que reescrito nos da la desigualdad $d \geq n - k + 1$. Pero por la cota de Singleton sabemos que para todos los

códigos lineales se cumple que $d \leq n - k + 1$, por lo tanto $d = n - k + 1$, y el código $RS(k, q)$ es MDS. ■

Como acabamos de ver, hemos introducido las ideas de geometría algebraica a la teoria de códigos, esta es una de las principales aportaciones debidas a Goppa, que en los años 70's desencadenó un estudio intensivo de las aplicaciones de la geometría algebraica a la teoria de códigos.

De manera concreta Goppa desarrollo un algoritmo que generaliza los códigos de Reed-Solomon.

2.3.3. Código Reed-Solomon geométrico

Siguiendo la propuesta de Goppa, tomemos una curva proyectiva plana χ no singular, con $gen(\chi) = g$, sobre el campo finito $\mathbb{F}_q$ y sea D un divisor sobre χ que cumple $2g - 2 < \text{grad}(D) < n$. Definimos $\mathcal{P} = \{P_1, ..., P_n\} \subset \chi(\mathbb{F}_q)$ un conjunto de puntos racionales sobre χ de manera que $\mathcal{P}$ y el soporte de D tienen intersección vacía, es decir, ningún P_i es polo de $f \in L(D)$, más aún $f(P_i) \in \mathbb{F}_q$ para cualquier $f \in L(D)$ y $P_i \in \mathcal{P}$.

Definimos ahora el código *Reed-Solomon geométrico* asociado a χ, $\mathcal{P}$ y D como

$$C(\chi, \mathcal{P}, D) = \{(f(P_1), ..., f(P_n)) \,|\, f \in L(D)\} \subset \mathbb{F}_q^n$$

o bien, usando la notación del mapeo de evaluación

$$C(\chi, \mathcal{P}, D) = \epsilon(L(D))$$

donde $\epsilon(f) = (f(P_1), ..., f(P_n))$.

Observación 92 *Al ver este código con la notación anterior es sencillo ver que, al ser $L(D)$ un espacio vectorial sobre $\mathbb{F}_q$ y ϵ lineal, el código es lineal de longitud n. La dimensión del código esta acotada por $l(D)$ y es exactamente $l(D)$ si y solo si el mapeo de evaluación es inyectivo, es decir, si y solo si el kernel de ϵ es trivial.*

Los parámetros del código construido se pueden calcular a partir del siguiente teorema, pero primero enunciaremos un lema que nos servira para calcular la dimensión del código.

Lema 93 *La dimensión del código Reed-Solomon geométrico $C(\chi, \mathcal{P}, D)$ es $l(d)$.*

Demostración. Basta demostrar que el mapeo de evaluación es inyectivo, para lo cual tomemos $f \in L(D)$ y supongamos que $\epsilon(f) = 0$. Entonces

$$f(P_1) = ... = f(P_n) = 0$$

por lo que el coeficiente de cada P_i en $\text{div}(f)$ es al menos 1. Como el soporte de D es disjunto de $\mathcal{P}$ tenemos que

$$\text{div}(f) + D - \sum_{i=1}^{n} P_i \geq 0$$

por lo cual $f \in L\left(D - \sum_{i=1}^{n} P_i\right)$. Recordemos ahora que $\deg(D) < n$, por lo tanto $\deg\left(D - \sum_{i=1}^{n} P_i\right)$ es negativo y su espacio asociado de funciones racionales es trivial. Asi pues $f = 0$. ■

Teorema 94 *El código Reed-Solomon geométrico $C(\chi, \mathcal{P}, D)$ tiene parámetros $(n, k, d) = (n, \deg(D) + 1 - g, d)$ con $d \geq n - k + 1 - g$.*

Demostración. Ya vimos que el código es lineal de longitud n. Además $k = l(D) = \deg(D) + 1 - g$ por el teorema de Riemman recordando que $\deg(D) > 2g - 2$, solo falta acotar la distancia mínima para completar la demostración.

Tomemos $\epsilon(f) = (f(P_1), ..., f(P_n))$ una palabra del código con peso mínimo $d \neq 0$, es decir, exactamente d coordenadas de nuestra palabra son cero, sin pérdida de generalidad tomemos $f(P_{d+1}) = ... = f(P_n) = 0$. Como en la demostración del lema anterior, esto significa que

$$\text{div}(f) + D - \sum_{i=d+1}^{n} P_i \geq 0$$

por lo cual $\deg\left(D - \sum_{i=d+1}^{n} P_i\right) > 0$, es decir $\deg(D) - (n - d) \geq 0$, que substituyendo $\deg(D)$ nos da la cota para d. ■

Este teorema nos muestra la importancia de escoger una curva con género g relativamente pequeño respecto a n.En general el problema fundamental para la construcción de un código Reed-Solomon geométrico se centra en dar una base $f_1, ..., f_k$ para el espacio $L(D)$, pues de esta manera $\epsilon(f_1, ..., \epsilon(f_k)$ es una base para nuestro código. Esto significa que la matriz generadora de $C(\chi, \mathcal{P}, D)$ es

$$\begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{pmatrix}$$

2.3.4. Código Reed-Solomon generalizado

Para esta clase de códigos necesitamos tomar $n \leq q$, un $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{F}_q^n$ con la restricción de que los α_i sean distintos a pares y un $v = (v_1, ..., v_n) \in \mathbb{F}_q^n$ donde las coordenadas son no cero aunque no necesariamente distintas. Una vez que tenemos α y v escogemos un k fijo que cumpla $1 \leq k \leq n$ y definimos al código *Reed-Solomon generalizado*

$$RSG_k(\alpha, v) = \{(v_1 f(\alpha_1), ..., v_n f(\alpha_n)) \,|\, f \in L_{k-1}\}$$

En la práctica los vectores α y v son llamados de *evaluación* y de *escala* respectivamente.

Resulta que los códigos así definidos cumplen con la cota de Singleton, como lo demostraremos en el siguiente resultado.

De la misma manera que construimos un código geométrico correspondiente a los códigos Reed-Solomon, podemos construir un código geométrico para los Reed-Solomon generalizados, basta escoger un vector de escala y aplicar el proceso visto en la generalización al código Reed-Solomon geométrico.

2.3.5. Codigos de Goppa

Una clase importante de códigos son los llamados Códigos de Goppa, que se construyen a partir de herramientas de geometría algebraica, y es el motivo por el cual el primer capítulo de este trabajo se dedicó a establecer conceptos como divisores, espacios $L(D)$, diferenciales sobre curvas y el teorema de Riemann-Roch.

Comenzaremos la construcción de estos códigos tomando una curva proyectiva plana χ no singular, con $gen(\chi) = g$, sobre el campo finito $\mathbb{F}_q$ y sea D un divisor sobre χ que cumple $2g - 2 < \text{grad}(D) < n$. Definimos $\mathcal{P} = \{P_1, ..., P_n\} \subset \chi(\mathbb{F}_q)$ un conjunto de puntos racionales sobre χ de manera que $\mathcal{P}$ y el soporte de D tienen intersección vacia, por lo que ningún P_i es polo de $f \in L(D)$, más aún $f(P_i) \in \mathbb{F}_q$ para cualquier $f \in L(D)$ y $P_i \in \mathcal{P}$, por último $P = \sum_{i=1}^{n} P_i$. Como hemos visto se piden las mismas condiciones que en la contrucción de los códigos Red-Solomon geométricos, más adelante se verá el porque de estas similitudes.

Definimos el *código de Goppa* $C^*(\chi, \mathcal{P}, D)$ de longitud n sobre $\mathbb{F}_q$ como

$$C^*(\chi, \mathcal{P}, D) = \{(R_{P_1}(f), ..., R_{P_n}(f) | f \in \Omega(D - P)\} \subset \mathbb{F}_q^n$$

recordando que $R_{P_i}(f)$ es el residuo de f en el punto P_i, es decir a_{-1} en la representación $f = \sum a_i t^i$ con t el parámetro uniformizante (generador del anillo maximal correspondiente al anillo $\mathcal{O}$ de funciones racionales definidas en P).

Los parámetros de este código los calcularemos en el siguiente teorema.

Teorema 95 *El código* $C^*(\chi, \mathcal{P}, D)$, *de longitud* n, *tiene dimensión* $k^* = n - \text{grad}(D) + g - 1$ *y distancia mínima* $d^* \geq \text{grad}(D) - 2g + 2$.

Al observar los valores de los parámetros de un código de Goppa podemos deducir una relación con el correspondiente Reed-Solomon bajo la misma curva, puntos y divisor D. Esto nos lleva al último teorema de este trabajo, un teorema que relaciona estos dos códigos.

Teorema 96 *Sea una curva proyectiva plana χ no singular, con $gen(\chi) = g$, sobre el campo finito $\mathbb{F}_q$ y D un divisor sobre χ que cumple $2g-2 < \text{grad}(D) < n$. Definimos $\mathcal{P} = \{P_1, ..., P_n\} \subset \chi(\mathbb{F}_q)$ un conjunto de puntos racionales sobre χ de manera que $\mathcal{P}$ y el soporte de D tienen intersección vacía y por último $P = \sum_{i=1}^{n} P_i$. Entonces los códigos $C(\chi, \mathcal{P}, D)$ y $C^*(\chi, \mathcal{P}, D)$ son duales.*

Demostración. Al calcular las dimensiones k y k^* vemos que $k + k^* = n$, asi que sólo falta demostrar que el producto interno de cualquier palabra del código $C(\chi, \mathcal{P}, D)$ con otra de $C^*(\chi, \mathcal{P}, D)$ es cero.

Sea $f \in L(D)$ y $\varphi \in \Omega(D - P)$, por la definicion de cada código aseguramos que la diferencial $f\varphi$ no tiene polos, con excepción de posibles polos de orden 1 en los puntos $P_1, ..., P_n$. El residuo de $f\varphi$ en P_i es $f(P_i)R_{P_i}(\varphi)$, pero la suma de residuos de una diferencial en una curva no singular es cero, por lo tanto tenemos

$$0 = \sum_{i=1}^{n} f(P_i)R_{P_i}(\varphi)$$

que es el producto interno de las dos palabras de los códigos. De esta manera se demuestra la veracidad del teorema. ■

Capítulo 3

Ejemplos

Para finalizar este trabajo expondremos algunos ejemplos de los códigos que presentamos en el capítulo anterior.

3.1. Cuártica de Klein sobre $\mathbb{F}_8$

Trabajaremos sobre el campo finito $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, ..., \alpha^6\}$ de ocho elementos, donde $\alpha^3 = \alpha + 1$, el cual es isomorfo a ${}^{\mathbb{F}_2[x]}/_{(x^3+x+1)}$, y con la curva χ definida por $x^3y + y^3z + z^3x = 0$ llamada la cuártica de Klein, la cual es una curva no singular con, aplicando la fórmula de Plücker, género $g = 3$ y 24 puntos racionales.

Los puntos racionales en $\mathbb{F}_8$ de esta curva se calculan tomando en cuenta que un punto $P = (x, y, z)$ es racional para nuestra curva dependiendo de algunas relaciones entre ellos

Si $xyz = 0$ entonces $P\epsilon\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$, lo que es fácil de verificar.

En caso contrario, si $xyz \neq 0$ entonces podemos tomar a $z = 1$, recordemos que esto es posible al trabajar en coordenadas homogeneas, y $y = \alpha^i$ para

algun $i\epsilon\{0,...,6\}$. Continuando con este razonamiento, podemos calcular

$$x^3y + y^3z + z^3x = x^3\alpha^i + \alpha^{3i} + x = 0$$

que arroja una solución $x = \alpha^{3i}\eta$, con $\eta\epsilon\{\alpha, \alpha^2, \alpha^4\}$. El resto es combinatoria, y contando 24 puntos racionales.

Definimos $Q = (0, 1, 0)$ y P como la suma de los restantes 23 puntos racionales de χ sobre $\mathbb{F}_8$, $D = 10Q$ será nuestro divisor para construir el código $C(\chi, \mathcal{P}, D)$. Este tiene dimensión $k = 10 - 3 + 1 = 8$, longitud $n = 23$ distancia mínima $d \geq 23 - 10 = 13$. Notemos que $\text{grad}(D) = 10$ con lo cual $l(D) = 8$.

Ahora encontraremos una base para el espacio $L(D)$, y de esta manera daremos la construcción explícita del código. Comencemos por notar que los divisores correspondientes a las funciones ${}^x/_z$ y ${}^y/_z$ vienen dados por

$$\begin{aligned} ({}^x/_z) &= 3P_1 - P_2 - 2Q \\ ({}^y/_z) &= P_1 + 2P_2 - 3Q \end{aligned}$$

con $P_1 = (0, 0, 1)$ y $P_2(1, 0, 0)$. De ellos podemos deducir que las funciones $({}^x/_z)^i\,({}^y/_z)^j \in L(D)$ cuando se cumple

$$\begin{aligned} 0 &\leq 2i + 3j \leq 10 \\ 0 &\leq i \leq 2j \end{aligned}$$

Las soluciones a estas desigualdades arrojan un total de 8 funciones con polos en Q de órdenes 0, 3, 5, 6, 7, 8, 9 y 10 respectivamente, y como la dimensión de $L(D)$ es 8, las funciones encontradas forman una base para este espacio. Al sustituir las coordenadas de los puntos racionales de χ en estas funciones obtenemos una matriz generadora 8×23.

3.2. Hexacódigo

Para este ejemplo trabajaremos con el campo $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, con $\alpha^2 = \alpha + 1$, y la curva χ dada por la ecuación $x^2y + \alpha y^2z + \alpha z^2x = 0$, esta curva es de género $g = 1$ con lo que obtendremos un código $C(\chi, \mathcal{P}, D)$ con distancia mínima $d \geq n - k$, de hecho veremos que este es un código MDS.

Los puntos racionales de la curva χ sobre $\mathbb{F}_4$ vienen dador por la siguiente tabla, donde las filas representan las coordenadas de cada punto

$$\begin{pmatrix} & x & y & z \\ P_1 & 1 & 0 & 0 \\ P_2 & 0 & 1 & 0 \\ P_3 & 0 & 0 & 1 \\ P_4 & 1 & \alpha & \alpha^2 \\ P_5 & 1 & \alpha^2 & \alpha \\ P_6 & 1 & 1 & 1 \\ Q_1 & \alpha & 1 & 1 \\ Q_2 & 1 & \alpha & 1 \\ Q_3 & 1 & 1 & \alpha \end{pmatrix}$$

Definamos ahora $P = \sum_{i=1}^{6} P_i$ y $D = 2Q_1 + Q_2$ de grado 3. El espacio $L(D)$ tiene dimensión $l(D) = 3$ y una base para el son las funciones

$$\begin{aligned} f_1 &= \frac{x}{x + y + \alpha^2 z} \\ f_2 &= \frac{y}{x + y + \alpha^2 z} \\ f_3 &= \frac{\alpha^2 z}{x + y + \alpha^2 z} \end{aligned}$$

Esto se deduce a partir de que la función $x + y + \alpha^2 z$ es no cero en Q_1 y Q_2 además de que la ecuación $x + y + \alpha^2 z = 0$ corta a χ en Q_2 y es tangente a χ en Q_1. Este código tiene longitud $n = 6$, dimensión $k = 3$ y distancia mínima $d \geq 3$.

La matriz generadora de este código es

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & i & i \\ 0 & 1 & 0 & i & 1 & i \\ 0 & 0 & 1 & i & i & 1 \end{pmatrix}$$

de la cuál podemos ver que la distancia mínima, que es igual al peso mínimo de las palabras de nuestro código, es $d = 4$, con lo cual se cumple la igualdad de la cota de Singleton para estos parámetros y el código es MDS como habíamos planteado.

3.3. Reed-Solomon (8,3,5)

Tomemos la curva χ definida por $x^3 + y^3 + z^3 = 0$, sobre $\mathbb{F}_4$, que tiene 9 puntos racionales, a saber aquellos que tienen una coordenada cero, otra uno y la restante cualquier elemento de $\mathbb{F}_4$ distinto de cero, los cuales se presentan en la siguiente tabla

$$\begin{pmatrix} & x & y & z \\ Q & 0 & 1 & 1 \\ P & 0 & \alpha & 1 \\ P & 0 & \alpha^2 & 1 \\ P & 1 & 0 & 1 \\ P & \alpha & 0 & 1 \\ P & \alpha^2 & 0 & 1 \\ P & 1 & 1 & 0 \\ P & \alpha & 1 & 0 \\ P & \alpha^2 & 1 & 0 \end{pmatrix}$$

además la curva tiene genero $g = 1$. Definimos a $n = 8$ y tomemos $D = 3(0, 0, 1)$ y P la suma de los restantes puntos racionales. Una base para el espacio $L(D)$ viene dada por las funciones 1, $^{x}/_{(y+z)}$ y $^{y}/_{(y+z)}$ con lo que $k = 3$. Con estos datos podemos comprobar que la matriz generadora de nuestro código $C(\chi, \mathcal{P}, D)$ viene dada por

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha^2 & \alpha & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

de la cual podemos ver que la distancia mínima $d = 5$.

3.4. Código de Goppa clásico

Una manera de construir códigos de Goppa es la siguiente.

Sea $L = \{\alpha_1, ..., \alpha_n\}$ un conjunto de n elementos distintos de $\mathbb{F}_{q^m}$ y $g \in \mathbb{F}_{q^m}[x]$ un polinomio no cero en ningun punto de L. Definimos el código

de Goppa clásico $\Gamma(L, g)$ como

$$\Gamma(L, g) = \left\{ \mathbf{c} \in \mathbb{F}_{q^m} | \sum \frac{c_i}{x - \alpha_i} \equiv 0 \pmod{g} \right\}$$

Veamos ahora que este código puede definirse de la manera que presentamos en el capítulo anterior. Tomemos $P_i = (1, \alpha_i)$, $Q = (1, 0)$ y $P = \sum_{i=1}^{n} P_i$. Si definimos E como el divisor de los ceros de g sobre la linea proyectiva entonces $\Gamma(L, g) = C^*(P, E - Q)$, es decir

$$\mathbf{c} \in \Gamma(L, g) \iff \sum \frac{c_i}{x - \alpha_i} dx \in \Omega(E - Q - P)$$

La matriz generadora de el código $\Gamma(L, g)$ viene expresada en términos de los puntos α_i y el polinomio g como sigue

$$\begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \cdots & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{pmatrix}$$

donde r es el grado del pólinomio g. Al observar la matriz podemos ver el parecido que hay entre ésta y una matriz generadora de un código dual para el caso de códigos Reed-Solomon generalizados, lo que se justifica por el teorema 96.

Bibliografía

[1] William Fulton, Curvas algebráicas, ed.

[2] Judy L. Walker, Codes and curves, Student mathematical library. IAS/Park City mathematical subseries.

[3] T. Hohold, J. H. van Lind y Ruud Pellikaan, Algebraic geometry codes, Handbook of coding theory vol. 1 pp.871-961.

[4] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag.

[5] M. F. Atiyah y I. G. MacDonald, Introduction to commutative algebra, Addison Wesley Publishing Company.

[6] Athanasios Papaioannou, An algebraic aproach to the Riemann-Roch theorem and the arithmetic theory of funtions fields.

[7] D. A. Cox, J. Little and D. O´Shea, Using algebraic geometry, Springer.

[8] Varios, Topics in geometry, coding theory and cryptography, Springer.

[9] E. Brieskorn y Horst Körrer, Plane algebraic curves, Birkhäuser-Verlag.

[10] P. J. Mopandi, Error correcting codes and algebraic curves, Lecture notes.

[11] O. Pretzel, Error correcting codes and finite fields, Clarendon Press.

[12] A. Neubauer, J. Freudenberger y V. Kühn, Coding theory, John Wiley and sons.

[13] L. R. Vermani, Elements of algebraic coding theory, Chapman and Hall.