UNIVERSIDAD NACIONAL DE COLOMBIA

El Teorema de Riemman-Roch

Santiago Toro Oquendo

Universidad Nacional de Colombia
Facultad de Ciencias, Escuela de Matemáticas
Medellín, Colombia
2015

Agradecimientos a la Universidad Nacional de
Colombia sede Medellín y a la Escuela de
Matemáticas.

El Teorema de Riemman-Roch

Santiago Toro Oquendo

Trabajo de grado presentado como requisito parcial para optar al título de:
Matemático

Directora:
Margarita María Toro Villegas

Universidad Nacional de Colombia
Facultad de Ciencias, Escuela de Matemáticas
Medelllín, Colombia
2015

«El hecho de que yo exista prueba que el mundo no tiene sentido. ¿Qué sentido, en efecto, podría yo hallar en los suplicios de un hombre infinitamente atormentado y desgraciado para quien todo se reduce en última instancia a la nada y para quien el sufrimiento domina el mundo? Que el mundo haya permitido la existencia de un ser humano como yo prueba que las manchas sobre el sol de la vida son tan grandes que acabarán ocultando su luz».

E.M. Cioran / En las Cimas de la Desesperación.

Agradecimientos

Inicialmente deseo dar un agradecimiento infinito a mis padres Gilberto Toro Mira y Silvia María Oquendo quienes han puesto todo su empeño y apoyo para que yo lograra este objetivo, a ellos les debo todo lo que soy como persona. Su amor, comprensión y enseñanzas han logrado que día a día continue con entusiasmo en mi formación como profesional. Agradecezco también a mi hermana Laura Melisa Toro quien siempre ha sido un gran apoyo y un soporte familiar muy importante, de ella he aprendido muchas cosas y siempre me ha motivado y brindado buenos deseos en mi carrera profesional.

Agradezco sinceramente a la profesora Margarita Toro Villegas, quien fue mi asesora en este trabajo. A ella le profeso un gran respeto y admiración. Gracias por todo su esfuerzo y por la dedicación que brindó para este trabajo. Sus conocimientos, orientaciones y paciencia han sido de gran importancia para mi. Ella ha logrado contribuir de gran manera a mi formación como matemático.

Agradezco mucho a mis amigos, los «absurdos» de matemáticas quienes contribuyeron con mucho café, risas, cervezas y conocimiento. A ellos les debo su gran apoyo, muchos momentos indescriptibles y aquellos empujones que me daban en este duro camino cuando se tornaba todo cuesta arriba. También quiero agradecer profundamente a mis eternos amigos Yurani, Sebastian y Jaime y por supuesto a mis amigos ingenieros Linda, Camilo, Leidy, Santiago, Kelly y todos los demás. Ellos siempre han estado allí para decir las palabras adecuadas en momentos difíciles o para reír conmigo en los buenos.

Por último, agradezco a los profesores Carlos Augusto Veléz, José Manuel Gomez, Jhon Jader Mira, José Gregorio Rodriguez y Jhon Bayron Baena. De ellos no sólo he aprendido muchas matemáticas sino que me han brindado grandes consejos y enseñanzas que serán muy significativas para mi futuro como matemático y posteriormente investigador.

Resumen

En la década de 1850 se desarrolló un importante vinculo entre dos áreas de la matemática: el Análisis Complejo y la Geometría Algebraica. Esta herramienta, comúnmente utilizada en clasificación de curvas y superficies, se conoce hoy en día como el Teorema de Riemann-Roch. Éste vio la luz a causa de Riemann, el cual demostró inicialmente la desigualdad que lleva su nombre y mas tarde adquirió su forma mas conocida a causa de un gran estudiante de Riemann llamado Gustave Roch. En este trabajo se presenta una prueba detallada del teorema en su versión para curvas, usando técnicas de Geometría Algebraica y Teoría Algebraica de Números que fueron posteriores a Riemann.

Introducción

El Teorema de Riemann-Roch es una importante herramienta comúnmente utilizada en Variable Compleja y Geometría Algebraica, ya que varias de sus versiones sirven de apoyo en teoría de clasificación de curvas y superficies.
Se escribe este trabajo motivado por la importancia que posee la teoría de clasificación de superficies y lo interesante que se convierten las áreas que combinan distintas disciplinas y teorías en matemáticas. Además este teorema es un claro ejemplo en la historia de las matemáticas de una proposición que aún sigue vigente y puede verse desde distintos puntos de vista e interpretaciones.
En la presente monografía se tiene como objetivo presentar una prueba detallada del teorema en su versión para curvas. Inicialmente haremos un estudio general acerca de nociones básicas que se aprenden en un curso no graduado de Geometría Algebraica. Cuando entremos al terreno de las curvas vamos a ver como se relacionan los puntos en las curvas y las valuaciones de sus campos de funciones, particularmente, podremos observar la equivalencia que existe entre las nociones de divisor sobre una curva y divisor de un campo de funciones asociado a la curva. Esta equivalencia resulta ser muy importante, pues ese será nuestro punto de partida hacia la prueba del teorema. De esta manera, estudiaremos conceptos acerca de los campos de funciones y realizaremos la prueba del Teorema de Riemann-Roch usando técnicas muy comunes en Teoría Algebraica de Números.
Supondremos que el lector posee conocimientos básicos acerca de álgebra conmutativa y teoría de campos [2]. Antes de comenzar el trabajo, veamos un poco como surgió el teorema y quienes han contribuido de manera significante a este.

La historia del Teorema de Riemann-Roch inicia en la década de 1850, época en la cual Riemann puso en conjunto toda una teoría de funciones complejas definidas sobre un domi-nio 2-dimensional [5]. Riemann mostró cómo definir tales funciones complejas con polos sobre un camino usando su versión del Principio de Dirichlet. Posteriormente Riemann fue capaz de probar la existencia de funciones complejas sobre una superficie sin frontera gracias a la desigualdad que lleva su nombre, la cual fue su contribución al Teorema de Riemann-Roch. [5].
Gustav Roch fue un estudiante brillante de Riemann, el cual lamentablemente falleció de tuberculosis a tan solo 26 años de edad. Roch tuvo la habilidad de interpretar analíticamente ciertas cantidades en el trabajo de Riemann y juntos abrieron el camino para el estudio de las propiedades intrínsecas de curvas, independientemente de sus embebimientos en el plano. Después de la muerte de Riemann y Roch, ambas en el año 1866, el sucesor de Riemann en Göttingen fue Alfred Clebsch, quien se convertiría en el principal responsable de aplicar las ideas de Riemann a la Geometría y al Álgebra. La razón por la cual Clebsch busco otro camino que no fuese Variable Compleja se debió principalmente a que el trabajo de sus pre-

decesores era bastante complejo y difuso, debido a la naturaleza topológica de lo que es una superficie de Riemann. Además de ello, el uso del principio de Dirichlet se tornaba confuso en el trabajo de Roch, pues en aquella época Weierstrass encontró un contraejemplo a esta herramienta muy utilizada por Riemann y Roch en sus pruebas.

Ulteriormente, en el desarrollo del teorema se destacan ampliamente Alexander Von Brill y Max Noether quienes en 1874 fueron los primeros en llamar al teorema por el nombre con el que hoy le conocemos. Brill y Noether siguiendo las ideas de Clebsch y otros alemanes enuncian y prueban una version del Teorema de Riemann-Roch, la cual establecieron en términos de lo que llamaron familias especiales de curvas. A medida que se desarrollaron distintos resultados en Álgebra, muchos otros matemáticos publicaban sus versiones del teorema, algunas de estas en términos de superficies algebraicas en búsqueda de una mayor generalidad. Entre muchos, destacamos a Hensel y Landsberg los cuales, en 1898 [5], tomaron el estudio de curvas algebraicas y mediante los campos de funciones asociados a éstas dieron una nueva prueba del teorema.

Siguiendo este orden de ideas y pasados los años, un estudiante de Klein llamado Ernst Ritter brindó un buen aporte al teorema. Ritter, siguiendo una ruta desarrollada por Poincaré y Koebe en 1907, enunció lo que el llamó una versión extendida del Teorema de Riemann-Roch. Sin embargo, luego fue Hermann Weyl quien en su famoso artículo «*Die Idee der Riemannschen Fläche*», publicado en Leipzig en 1913, probó ambos, el teorema usual de Riemannn-Roch y la versión extendida del Teorema de Riemann-Roch dada a Ritter.

Por último es preciso mencionar a otros tres matemáticos que hicieron muy buenos aportes al teorema. Primero tenemos a William Osgood, quien fue el primero en dar una prueba del teorema utilizando el teorema de uniformización en 1927. Segundo está Friederich Hirzebruch quien, a principios de la década de 1950 demostró, mediante la teoría de clases características en Topología Algebraica, lo que hoy se conoce como el Teorema de Hirzebruch-Riemann-Roch, el cual es una generalización n-dimensional del teorema de Riemann y su estudiante. Todo el trabajo de Hirzebruch era una busqueda de los matemáticos de la época por establecer versiones del teorema en variedades algebraicas y dimensiones mas altas con el fin de generalizar el teorema. En consecuencia, en el año 1957, Alexander Grothendieck probó una version mucho mas general que la de Hirzebruch conocida hoy en día como el Teorema de Grothendieck-Riemann-Roch. Su trabajo se basó en reinterpretar el resultado de Riemann en el contexto de variedades y verlo mejor como un resultado acerca de un morfismo entre variedades. Las ideas geniales de Grothendieck son estudiadas ampliamente en la actualidad y constituyen una parte importante de la Geometría Algebraica moderna.

Índice general

Capítulo 1

Preliminares

«Every mathematician worthy of the name has experienced the state of lucid exaltation in which one thought succeeds another as if miraculously. This feeling may last for hours at a time, even for days. Once you have experienced it, you are eager to repeat it but unable to do it at will, unless perhaps by dogged work».

André Weil.

En este capítulo haremos una breve recopilación de la terminología y de los resultados necesarios para la lectura de capítulos posteriores. Supondremos que el lector está familiarizado con algunos conceptos de teoría básica de anillos conmutativos y conjuntos algebraicos afines. Para una mayor profundidad en algunos resultados de este capítulo recomendamos al lector visitar [4], esta obra junto con [12] han sido en gran parte la guía para este trabajo.

1.1. Conjuntos Algebraicos

Sea k un campo. Definimos el espacio afín, denotado por $\mathbb{A}^n(k)$, simplemente como el producto cartesiano de k consigo mismo n veces, es decir, $\mathbb{A}^n(k) = k^n$. $\mathbb{A}^n(k)$ suele llamarse el *espacio afín n-dimensional sobre k* y sus elementos son llamados *puntos*. Si $F \in k[x_1, ..., x_n]$, un punto $P = (a_1, ..., a_n) \in \mathbb{A}^n(k)$ es llamado un *cero* de F si $F(p) = F(a_1, ...a_n) = 0$. Si F no es constante, el conjunto de ceros de F es llamado una *hipersuperficie* definida por F y denotada por $V(F)$.

Más generalmente, si S es un conjunto de polinomios en $k[x_1, ..., x_n]$, definimos:

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

Si $S = \{F_1, ..., F_r\}$ usualmente escribimos $V(F_1, ..., F_r)$ en lugar de $V(\{F_1, ..., F_r\})$.

Definición 1.1. *Un subconjunto $X \subseteq \mathbb{A}^n(k)$ es un* ***conjunto algebraico afín*** *o simplemente* ***conjunto algebraico****, si $X = V(S)$ para algún $S \subseteq k[x_1, ..., x_n]$.*

De la anterior definición se deducen las siguientes propiedades:

(1) Si I es el ideal de $k[x_1, ..., x_n]$ generado por S, entonces $V(S) = V(I)$; así todo conjunto algebraico es igual a $V(I)$, para algún ideal I.

(2) Si $\{I_\alpha\}_{\alpha \in J}$ es cualquier colección de ideales de $k[x_1, ..., x_n]$, entonces:

$$V\left(\bigcup_{\alpha \in J} I_\alpha\right) = \bigcap_{\alpha \in J} V(I_\alpha);$$

así la intersección de cualquier colección de conjuntos algebraicos resulta ser un conjunto algebraico.

(3) Si $I \subseteq J$, entonces $V(I) \supseteq V(J)$.

(4) $V(FG) = V(F) \cup V(G)$ para cada par de polinomios $F, G \in k[x_1, ..., x_n]$. Además $V(I) \cup V(J) = V(\{FG \mid F \in I, G \in J\})$; luego la unión finita de conjuntos algebraicos es un conjunto algebraico.

(5) $V(0) = \mathbb{A}^n(k)$; $V(1) = \emptyset$ y $V(x_1 - a_1, ..., x_n - a_n) = \{(a_1, ..., a_n)\}$. Así cualesquier subconjunto finito de $\mathbb{A}^n(k)$ es un conjunto algebraico.

Estas propiedades dan lugar a una topología en el espacio afín $\mathbb{A}^n(k)$ denominada topología de Zariski, donde los cerrados de está topología están dados por los conjuntos algebraicos afines.

1.1.1. Ideal de un conjunto

Definición 1.2. *Sea $X \subseteq \mathbb{A}^n(k)$, los polinomios de $k[x_1, ..., x_n]$ que se anulan sobre X forman un ideal llamado el* ***ideal de*** *X, denotado por $I(X)$, explícitamente:*
$I(X) = \{F \in k[x_1, ..., x_n] \mid F(a_1, ..., a_n) = 0$ para todo $(a_1, ..., a_n) \in X\}$.

Definición 1.3 (Ideal radical)**.** *Sea R un anillo e I un ideal de R. Definimos el* ***radical*** *de I, denotado por $Rad(I)$, como el conjunto $\{a \in R \mid a^n \in I$ para algún entero $n > 0\}$. Resulta fácil probar que $Rad(I)$ es un ideal de R que contiene a I. Además un ideal es llamado* ***ideal radical*** *si $I = Rad(I)$.*

Las siguientes propiedades relacionan ideales y conjuntos algebraicos y se prueban fácilmente de la definición:

(6) Si $X \subseteq Y$ entonces $I(X) \supseteq I(Y)$.

(7) $I(\emptyset) = k[x_1, ..., x_n]$ e $I(\mathbb{A}^n(k)) = (0)$, siempre que k sea un campo infinito.

(8) $I(V(S)) \supseteq S$ para algún $S \subseteq k[x_1, ..., x_n]$. $V(I(X)) \supseteq X$ para algún $X \subseteq \mathbb{A}^n(k)$.

(9) $V(I(V(S))) = V(S)$ para algún $S \subseteq k[x_1, ..., x_n]$. $I(V(I(X))) = I(X)$ para algún $X \subseteq \mathbb{A}^n(k)$.
Por tanto si V es un conjunto algebraico, $V = V(I(V))$, y si I es el ideal de un conjunto algebraico $I(V(I)) = I$.

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

Proposición 1.4. *Sea k un campo, entonces para cada ideal I de $k[x_1, ..., x_n]$, $V(I) = V(Rad(I))$, y además $Rad(I) \subseteq I(V(I))$.*

Demostración. Veamos primero que $V(I) = V(Rad(I))$. Sea $x \in V(I)$, entonces $x \in \mathbb{A}^n(k)$ y $F(x) = 0$ para cada $F \in I$. Dado que $I \subseteq Rad(I)$, entonces $F(x) = 0$ para cada $F \in Rad(I)$, esto es, $x \in V(Rad(I))$ y por tanto $V(I) \subseteq V(Rad(I))$.
Ahora, notemos que de la Definición 1.3 tenemos que $I \subseteq Rad(I)$, y por tanto por la propiedad 3, se sigue que $V(I) \supseteq V(Rad(I))$. De lo anterior concluimos que $V(I) = V(Rad(I))$.

Veamos ahora que $Rad(I) \subseteq I(V(I))$. Sea $F \in Rad(I)$, entonces existe un entero $N > 0$ tal que $F^N \in I$, por lo tanto, para todo $p \in V(I)$ se sigue que $F^N(p) = 0 = (F(p))^N$ y en consecuencia $F(p) = 0$, con lo cual se concluye que $F \in I(V(I))$ y así $Rad(I) \subseteq I(V(I))$. □

Proposición 1.5. *Sea k un campo y sean $a_1, ..., a_n \in k$. Entonces el ideal:*

$$I = (x_1 - a_1, ..., x_n - a_n) \subseteq k[x_1, ..., x_n]$$

es un ideal maximal.

Demostración. Definamos:

$$\begin{aligned} \Phi : k[x_1, ..., x_n]/_I &\longrightarrow k \\ F + I &\longrightarrow F(a_1, ..., a_n) \end{aligned}$$

Resulta fácil notar que Φ esta bien definida y además es un isomorfismo de campos, por lo tanto I es un ideal maximal. □

1.1.2. Componentes irreducibles

Definición 1.6. *Un conjunto algebraico $V \subseteq \mathbb{A}^n(k)$ se dice **reducible** si $V = V_1 \cup V_2$, donde V_1, V_2 son conjuntos algebraicos en $\mathbb{A}^n(k)$ y $V_i \neq V$, i=1,2. En otro caso V se dice que es **irreducible**.*

La siguiente proposición nos permite caracterizar los conjuntos algebraicos irreducibles.

Proposición 1.7. *Un conjunto algebraico V es irreducible si y sólo si $I(V)$ es primo.*

Demostración. Supongamos que V es irreducible y razonando por el absurdo supongamos que $I(V)$ no es primo, luego tomemos $F, G \notin I(V)$ tales que $FG \in I(V)$. Entonces notemos que $(V \cap V(F)) \cup (V \cap V(G)) = V \cap (V(F) \cup V(G)) = V \cap (V(FG)) \subseteq V$.
Ahora si $p \in V$, dado que $FG \in I(V)$ entonces $FG(p) = 0$, con lo cual tenemos que $p \in V(FG)$ y así $p \in V \cap V(FG)$.
De lo anterior se sigue que $V = V \cap (V(FG)) = (V \cap V(F)) \cup (V \cap V(G))$ y además $V \cap V(F) \subsetneq V$ y $V \cap V(G) \subsetneq V$ (pues $F, G \notin I(V)$), con lo cual V es reducible pero esto contradice la hipótesis, luego $I(V)$ es primo.
Ahora, supongamos que $I(V)$ es primo y razonando nuevamente por el absurdo supongamos que V es reducible, es decir, $V = V_1 \cup V_2$ con $V_i \subsetneq V$, i=1,2. Entonces por propiedades $I(V_i) \supseteq I(V)$, luego existen $F_i \in I(V_i)$ tal que $F_i \notin I(V)$, se sigue entonces que $F_1 F_2 \in I(V)$, con lo cual $I(V)$ no sería primo. □

Teorema 1.8 (Teorema de descomposición)**.** *[11, págs 34-35]. Sea $V \subseteq \mathbb{A}^n(k)$ un conjunto algebraico afín. Entonces V puede expresarse de manera única como una unión de subconjuntos algebraicos irreducibles de V, esto es, existen $V_1, ..., V_m \subset V$ irreducibles tales que $V = \bigcup_{i=1}^{m} V_i$ y además $V_i \nsubseteq V_j$ para cada $i \neq j$.*

1.1.3. Teorema de los ceros de Hilbert

Un resultado importante de un curso básico de geometría algebraica es el Teorema de los ceros de Hilbert, éste permite establecer la relación exacta que hay entre ideales y conjuntos algebraicos. Para una reseña detallada de lo necesario para su prueba recomendamos consultar [3]. Aquí presentaremos sus dos versiones (fuerte y débil) y daremos la prueba de la version fuerte, la versión débil no ofrece una mayor dificultad y por ende recomendamos al lector consultarla en [7].

Definición 1.9. *Decimos que un anillo R es **Noetheriano** si cada ideal I de R es finitamente generado.*

Proposición 1.10. *[1, pág 80] R es un anillo Noetheriano si y sólo si toda cadena ascendente de ideales se estabiliza, es decir, si $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ es una cadena (arbitraria) de ideales de R, entonces existe un entero positivo m tal que, para cada $k \geq m$ se cumple que $I_k = I_m$.*

Teorema 1.11 (Teorema de la base de Hilbert)**.** *[3, págs 27-28]. Si R es un anillo Noetheriano entonces $R[x]$ también es Noetheriano.*

Gracias al teorema precedente, teniendo en cuenta que $K[x_1, ..., x_n] \cong K[x_1, ..., x_{n-1}][x_n]$ y utilizando un argumento inductivo se sigue inmediatamente la siguiente afirmación.

Corolario 1.12. *Sea K un campo, entonces $K[x_1, ..., x_n]$ es Noetheriano. Más aún, si K es un anillo Noetheriano entonces $K[x_1, ..., x_n]$ es Noetheriano.*

Teorema 1.13 (Nullstellensatz débil)**.** *Sea k un campo algebraicamente cerrado. Si I es un ideal propio de $k[x_1, ..., x_n]$, entonces $V(I) \neq \emptyset$.*

Demostración. Este teorema posee una versión equivalente que involucra extensiones de campo, recomendamos ver [7, págs 16-18]. □

Teorema 1.14 (Nullstellensatz fuerte)**.** *Sea k un campo algebraicamente cerrado y sea I un ideal en $k[x_1, ..., x_n]$, entonces $I(V(I)) = Rad(I)$.*

Demostración. Notemos que lo anterior nos dice que si $F_1, ..., F_r, G \in k[x_1, ..., x_n]$ y G se anula siempre que los $F_1, ..., F_r$ se anulen, entonces existe una ecuación dada por $G^N = A_1F_1 + \cdots + A_rF_r$ para algún $N > 0$ y algunos $A_i \in k[x_1, ..., x_n]$.

Recordemos que de la Proposición 1.4 , $Rad(I) \subseteq I(V(I))$. Ahora, por el teorema de la base de Hilbert 1.11, $k[x_1, ..., x_n]$ es Noetheriano, por ende existen $F_1, ..., F_r \in k[x_1, ..., x_n]$ tales que $I = (F_1, ..., F_r)$.
Supongamos que $G \in I(V(I))$ y definamos el ideal J por $J = (I, Gx_{n+1}-1) \subseteq k[x_1, ..., x_n, x_{n+1}]$.

Si $(a_1, ..., a_n, a_{n+1}) \in \mathbb{A}^{n+1}(k)$ es un cero de J, entonces $(a_1, ..., a_n) \in V(I)$, así que
$G(a_1, ..., a_n) \cdot a_{n+1} - 1 = -1$, pero $(a_1, ..., a_n, a_{n+1})$ es también un cero de $Gx_{n+1} - 1$ lo cual es absurdo y por lo tanto J no tiene ceros y en consecuencia por el Nullstellensatz débil se tiene que $V(J) = \emptyset$ y por lo tanto $1 \in J$. Así se tiene la siguiente ecuación:

$$1 = \sum_{i=1}^{r} R_iF_i + S(Gx_{n+1} - 1)$$

con $R_i, S \in k[x_1, ..., x_n, x_{n+1}]$ y $F_i \in I$ $(i = 1, ..., r)$.

Sea $\phi : k[x_1, ..., x_n, x_{n+1}] \longrightarrow k[x_1, ..., x_n]$ el k-homomorfismo dado por:

$$\phi(x_i) = x_i \text{ para cada } i = 1, ..., n \text{ y } \phi(x_{n+1}) = 1/G.$$

Entonces:

$$1 = \sum_{i=1}^{r} \phi(R_i)F_i \text{ y } \phi(R_i) = \frac{A_i}{G^{N_i}} \text{ con } A_i \in k[x_1, ..., x_n],\ N_i \in \mathbb{N}$$

Si $N := max\{N_i\}$ para $i = 1, ..., r$, entonces tenemos que:

$$G^N \in (F_1, ..., F_r) = I \Leftrightarrow G \in Rad(I).$$

□

Las siguientes son consecuencias inmediatas del teorema.

Corolario 1.15. *Si I es un ideal radical en $k[x_1, ..., x_n]$, entonces $I(V(I)) = I$. Luego existe una correspondencia uno a uno entre ideales radicales y conjuntos algebraicos.*

Corolario 1.16. *Si I es un ideal primo, entonces $V(I)$ es irreducible. Luego existe una correspondencia uno a uno entre ideales primos y conjuntos algebraicos irreducibles. Los ideales maximales se corresponden con puntos.*

1.2. Variedades Afines

En está sección observaremos propiedades locales de las variedades, podremos ver que diferentes propiedades locales se pueden capturar de manera algebraica usando distintas nociones como el anillo de coordenadas o el campo de funciones racionales.
A partir de ahora k denotará un campo algebraicamente cerrado. Además un conjunto algebraico en $\mathbb{A}^n(k)$ el cual es irreducible será llamado una **variedad afín** o simplemente **variedad** si se entiende en que espacio estamos trabajando. Por lo anterior si V es una variedad afín entonces gracias a la Proposición 1.7, $I(V)$ es un ideal primo.

1.2.1. Anillo de coordenadas y funciones regulares

Definición 1.17. *Sea $V \subseteq \mathbb{A}^n(k)$ una variedad afín no vacía. Definimos el anillo de coordenadas de V, usualmente denotado por $\Gamma(V)$, como el cociente:*

$$\frac{k[x_1, ..., x_n]}{I(V)}$$

Notemos que como el ideal $I(V)$ es primo entonces el anillo de coordenadas es un dominio.

Observación. *Dada una variedad no vacía $V \subset \mathbb{A}^n(k)$, denotaremos por $\mathcal{F}(V, k)$ al conjunto de todas las funciones de V en k. Este conjunto posee estructura de anillo de la manera usual (suma y producto usuales de funciones).*

Definición 1.18 (**Función polinomial**). *Sea $V \subset \mathbb{A}^n(k)$ una variedad. Una función $f \in \mathcal{F}(V, k)$ es llamada una **función polinomial o función regular** 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 $(a_1, ..., a_n) \in V$.*

Notemos que las funciones polinomiales forman un subanillo de $\mathcal{F}(V, k)$ el cual contiene a k (identificando k con el conjunto de funciones constantes).

Observación. *Dada una función regular $f \in \mathcal{F}(V, k)$, si existen dos polinomios $F, G \in k[x_1, ..., x_n]$ tales que ellos determinan a la misma función f, entonces para cada $(a_1, ..., a_n) \in V$:*

$$f(a_1, ..., a_n) = F(a_1, ..., a_n)$$
$$f(a_1, ..., a_n) = G(a_1, ..., a_n)$$

De donde;

$$F(a_1, ..., a_n) = G(a_1, ..., a_n)$$
$$(F - G)(a_1, ..., a_n) = 0$$

*Por lo tanto, $F - G \in I(V)$. De lo anterior podemos **identificar** al anillo de coordenadas, $\Gamma(V)$ con el conjunto que consiste de todas las funciones polinomiales sobre V.*

Mediante el anillo de coordenadas podremos identificar propiedades que son intrínsecas en las variedades, por ende nuestro siguiente objetivo será establecer cómo se definen las funciones entre variedades y que relación poseen con el anillo de coordenadas.

Definición 1.19. *Sean $V \subseteq \mathbb{A}^n(k)$ y $W \subseteq \mathbb{A}^m(k)$ variedades afines. Un mapeo $\varphi : V \longrightarrow W$ es llamado* ***morfismo*** *o* ***mapeo polinomial*** *si existen polinomios $F_1, ..., F_m \in k[x_1, ..., x_n]$ tales que para cada $(a_1, ..., a_n) \in V$ se cumple que:*

$$\varphi(a_1, ..., a_n) = (F_1(a_1, ..., a_n), ..., F_m(a_1, ..., a_n))$$

Observación. *Notemos que en particular, cualquier función regular $f : V \longrightarrow k = \mathbb{A}^1(k)$ es un morfismo.*

Ahora, dado un morfismo entre variedades, digamos, $\varphi : V \longrightarrow W$, podemos definir:

$$\begin{aligned} \widetilde{\varphi} : \mathcal{F}(W, k) &\longrightarrow \mathcal{F}(V, k) \\ f &\mapsto \widetilde{\varphi}(f) := f \circ \varphi \end{aligned}$$

Claramente $\widetilde{\varphi}$ esta bien definida y además resulta ser un homomorfismo de anillos inducido por φ. Además, dado que φ es un morfismo entonces si $f \in \Gamma(W)$, es decir, f es una función polinomial, se sigue que f es la $I(W)$-clase de algún polinomio $F \in k[x_1, ..., x_n]$, esto es, $f = F + I(W)$. Por definición $\widetilde{\varphi}(f) := f \circ \varphi$ y para todo $(a_1, ..., a_n) \in V$, tenemos que:

$$\begin{aligned} (f \circ \varphi)(a_1, ..., a_n) &= f(\varphi(a_1, ..., a_n)) \\ &= f(G_1(a_1, ..., a_n), ..., G_m(a_1, ..., a_n)) \\ &= F(G_1, ..., G_m)(a_1, ..., a_n) \end{aligned}$$

Donde $G_1, ..., G_m \in k[x_1, ..., x_n]$ son los correspondientes polinomios asociados a φ en la definición de morfismo.
Lo anterior nos dice que $\widetilde{\varphi}(f)$ es una función polinomial (regular) sobre V y por ende $\widetilde{\varphi}(f) \in \Gamma(V)$ y así $\widetilde{\varphi}(f)$ es la $I(V)$-clase del polinomio $F(G_1, ..., G_m)$.

Definición 1.20. *Un morfismo $\varphi : V \longrightarrow W$ se dice que es un* ***isomorfismo*** *si existe otro morfismo $\psi : W \longrightarrow V$ tal que $\psi \circ \varphi = Id_V$ y $\varphi \circ \psi = Id_W$.*

Ejemplo 1.21. *Sean $U = \mathbb{A}^1(k)$ y $W = V(x_1^3 - x_2^2) \subseteq \mathbb{A}^2(k)$ y definamos $\varphi : U \longrightarrow W$ de la siguiente manera: dado $v \in U$, $\varphi(v) = (v^2, v^3)$.*
Inicialmente notemos que claramente φ es un morfismo, pues para cada $v \in U$:

$$\varphi(v) = (F_1(v), F_2(v))$$

Donde $F_1(x), F_2(x) \in k[x]$ y están dados justo por $F_1(x) = x^2$ y $F_2(x) = x^3$.

Ahora, la pregunta interesante sería ¿Será φ un isomorfismo? la respuesta es no, pero con lo que tenemos hasta ahora es muy difícil justificar esa respuesta. Notemos que podemos definir $\psi : W \longrightarrow U$ por:

$$\psi(w_1, w_2) = \begin{cases} \dfrac{w_2}{w_1} & si\ (w_1, w_2) \neq (0,0) \\ 0 & si\ (w_1, w_2) = (0,0) \end{cases}$$

Un simple computo comprueba que $\varphi \circ \psi(w_1, w_2) = (w_1, w_2)$ y que $\psi \circ \varphi(v) = v$. Sin embargo, ψ no es un morfismo y por tanto φ no podría ser isomorfismo. Probar que ψ no es un morfismo resulta ser un problema difícil, así que motivados por este tipo de problemas es que presentamos el siguiente teorema, el cual nos va a permitir relacionar isomorfismos entre variedades con sus respectivos anillos de coordenadas.

Teorema 1.22. *Sean $V \subseteq \mathbb{A}^n(k)$, $W \subseteq \mathbb{A}^m(k)$ variedades afines. Entonces existe una correspondencia uno a uno entre los morfismos $\varphi : V \longrightarrow W$ y los homomorfismos $\widetilde{\varphi} : \Gamma(W) \longrightarrow \Gamma(V)$.*

Demostración. Sea $\varphi : V \longrightarrow W$ un morfismo, recordemos que, por la observación a la Definición 1.19, podemos definir $\widetilde{\varphi} : \Gamma(W) \longrightarrow \Gamma(V)$ dada por $\widetilde{\varphi}(f) = f \circ \varphi$ el cual resulta ser un homomorfismo de anillos.
Entonces la parte interesante a probar es, dado un homomorfismo $h : \Gamma(W) \longrightarrow \Gamma(V)$ existe un morfismo $\varphi : V \longrightarrow W$ tal que $h = \widetilde{\varphi}$. Consideremos entonces $T_1, ..., T_m \in \Gamma(W)$ funciones regulares de la siguiente manera, para cada $(w_1, ..., w_m) \in W$

$$T_j(w_1, ..., w_m) = w_j \qquad j = 1, ..., m.$$

Claramente son regulares pues coinciden con los polinomios $F_j(x_1, ..., x_m) = x_j$, $j = 1, ..., m$ respectivamente. Entonces $h(T_j) \in \Gamma(V)$, $j = 1, ..., m$. Definamos $\varphi : V \longrightarrow \mathbb{A}^m(k)$ de la siguiente manera, si $a = (a_1, ..., a_n) \in V$, entonces:

$$\varphi(a) = (h(T_1)(a), ..., h(T_m)(a))$$

Dado que para cada $j = 1, ..., m$, $h(T_j) \in \Gamma(V)$ entonces existen $F_1, ..., F_m \in k[x_1, ..., x_n]$ tales que:

$$\varphi(a) = (h(T_1)(a), ..., h(T_m)(a)) = (F_1(a), ..., F_m(a)).$$

En consecuencia, φ es un morfismo de V en $\mathbb{A}^m(k)$. Veamos que de hecho es un morfismo de V en W, es decir, veamos que para cada $a \in V$, $\varphi(a) \in W$. Lo anterior es equivalente a mostrar que:

$$\forall a \in V\ \forall g \in I(W) : \quad g(f(a)) = g(h(T_1)(a), ..., h(T_m)(a)) = 0.$$

Sin embargo, mediante el uso de las propiedades de homomorfismo y de polinomios puede verse que lo anterior es, a su vez, equivalente a:

$$\forall g \in I(W)\ \forall a \in V: \quad h(g(T_1, ..., T_m))(a) = 0.$$

Lo anterior es siempre cierto pues $g \in I(W)$ y h es homomorfismo (por ende envía $I(W)$ en $I(V)$), con lo cual φ es en efecto un morfismo entre V y W y además $\widetilde{\varphi} = h$. □

Observación. *Notemos que gracias al teorema anterior, dos variedades afines son isomorfas si y sólo si sus anillos de coordenadas son isomorfos (sobre k). Con lo cual volviendo al Ejemplo 1.21 para responder la pregunta de si φ era un isomorfismo entre V y W, basta considerar sus anillos de coordenadas y notar que estos en efecto no son isomorfos (es fácil verlo).*

1.2.2. Anillos locales y funciones racionales

Antes de comenzar el estudio algebraico de curvas planas, es preciso observar una serie de conceptos y hechos acerca del estudio local de variedades afines.

Sean $F_1, ..., F_m \in k[x_1, ..., x_n]$, si $F = (F_1, ..., F_m)$ es un mapeo polinomial de $\mathbb{A}^n(k)$ en $\mathbb{A}^m(k)$, y además G es un polinomio en $k[x_1, ..., x_m]$, denotaremos por G^F al polinomio $\widetilde{F}(G) = G(F_1, ..., F_m)$. Lo anterior motiva la siguiente definición:

Definición 1.23. *Sea $F = (F_1, ..., F_m)$. Para los ideales I y los conjuntos algebraicos V en $\mathbb{A}^m(k)$, definimos:*

$$I^F = \langle \{G^F\}_{G \in I} \rangle$$

Es decir, I^F denota el ideal de $k[x_1, ..., x_n]$ generado por el conjunto $\{G^F\}_{G \in I}$. Además, definimos V^F como el conjunto algebraico:

$$V^F = V(I^F)$$

Donde $I = I(V)$.

Definición 1.24. *Un **cambio de coordenadas afín** sobre $\mathbb{A}^n(k)$ es un mapeo polinomial $F = (F_1, ..., F_n) : \mathbb{A}^n(k) \longrightarrow \mathbb{A}^n(k)$ tal que cada F_i es polinomio de grado 1 y además F es biyectiva.*

Definición 1.25. *Sea V una variedad afín no vacía. El **campo de funciones racionales sobre** V, denotado por $k(V)$, se define como el campo de fracciones del anillo de coordenadas $\Gamma(V)$. Un elemento de $k(V)$ es llamado una **función racional** sobre V.*

*Ahora, si f es una función racional sobre V y $p = (a_1, ..., a_n) \in V$, decimos que f está **definida** en p si:*

$$f = \frac{a}{b}$$

Para algunos $a, b \in \Gamma(V)$ y donde $b(p) \neq 0$.

Notemos que en la Definición 1.25 la función f puede tener diferentes maneras de escribirse, sin embargo si se da el caso en el cual $\Gamma(V)$ es un D.F.U, existe una forma única de representar a f en el campo de funciones racionales.

Definición 1.26. *Sea V una variedad afín no vacía y sea $p \in V$. Definimos el* ***anillo local de*** *V* ***en*** *p, usualmente denotado por $\mathcal{O}_p(V)$, como el conjunto de todas las funciones racionales en V que están definidas en p.*
El conjunto de puntos $p \in V$ para los cuales una función racional f no está definida es llamado ***el conjunto de polos de*** *f.*

Observación. *Notemos que en la anterior definición el conjunto $\mathcal{O}_p(V)$ forma un subanillo del campo de funciones racionales $k(V)$ bajo la suma y producto usual de funciones, además $\mathcal{O}_p(V)$ contiene a $\Gamma(V)$. Note que el conjunto de polos de una función racional posee estructura de conjunto algebraico contenido en V.*

Proposición 1.27. *[4, pág 21]. Sea $V \subseteq \mathbb{A}^n(k)$ una variedad afín. Entonces:*

(1) *El conjunto de polos de una función racional en V es un subconjunto algebraico de V.*

(2) $\Gamma(V) = \bigcap_{p \in V} \mathcal{O}_p(V)$.

1.2.3. Subconjuntos algebraicos del plano

Justo como habíamos establecido antes, estamos interesados en curvas por ende en esta parte vamos a ver con mas detalle los subconjuntos algebraicos del plano afín $\mathbb{A}^2(k)$. Por el Teorema de descomposición basta sólo enfocarnos en los conjuntos irreducibles, de está manera vamos a determinar qué relaciones cumplen los conjuntos algebraicos irreducibles en el plano afín $\mathbb{A}^2(k)$.

Lema 1.28. *[8, págs 7-8]. Sea R un dominio de factorización única (DFU) con campo de fracciones K. Si $f, g \in R[x]$ son primos relativos, entonces ellos también son primos relativos en $K[x]$, además existe $d \in R[x] \setminus \{0\}$ tal que $d = af + bg$ para algunos polinomios $a, b \in R[x]$.*

Proposición 1.29. *Sean F, G polinomios no constantes en $k[x, y]$ tales que son primos relativos, con lo cual no poseen factores comunes. Entonces $V(F) \cap V(G) = V(F, G)$ es finito. En otras palabras, el sistema de ecuaciones:*

$$\begin{aligned} F(x, y) &= 0 \qquad (x, y) \in \mathbb{A}^2(k) \\ G(x, y) &= 0 \end{aligned}$$

posee sólo un numero finito de soluciones en $\mathbb{A}^2(k)$.

Demostración. Notemos que por el Lema 1.28, dado que F, G no poseen factores comunes en $k[x][y]$, entonces tampoco los tienen en $k(x)[y]$ (y en $k(y)[x]$), de donde tenemos las siguientes ecuaciones:

$$d_1 = a_1F + b_1G$$
$$d_2 = a_2F + b_2G$$

con $d_1 \in k[x] \setminus \{0\}$, $d_2 \in k[y] \setminus \{0\}$ y $a_i, b_i \in k[x, y]$ para $i = 1, 2$.
Si $(x, y) \in V(F) \cap V(G)$, entonces x es un cero de d_1 y y es un cero de d_2, sin embargo d_1, d_2 sólo tienen un número finito de ceros, luego hay sólo un número finito de puntos (x, y) tales que $(x, y) \in V(F) \cap V(G)$. □

Corolario 1.30. *Si F es un polinomio irreducible en $k[x, y]$ tal que $V(F)$ es infinito, entonces $I(V(F)) = \langle F \rangle$ y además $V(F)$ es irreducible.*

Demostración. Sea $G \in I(V(F))$, entonces $V(F, G) = V(F) \cap V(G)$ es infinito, luego por la Proposición 1.29, F debe dividir a G, de donde $G \in \langle F \rangle$. En consecuencia $I(V(F)) = \langle F \rangle$. Por propiedades se tiene claramente la otra inclusión.
Ahora, dado que F es irreducible y $k[x, y]$ es DFU, entonces todo elemento irreducible de $k[x, y]$ es primo, por consiguiente $\langle F \rangle$ es un ideal primo y así por la Proposición 1.7 se sigue que $V(\langle F \rangle) = V(F)$ es irreducible. □

Gracias a las afirmaciones precedentes podemos entonces determinar todos los conjuntos algebraicos irreducibles del plano afín $\mathbb{A}^2(k)$.

Corolario 1.31. *Supongamos que k es infinito. Entonces los subconjuntos algebraicos irreducibles de $\mathbb{A}^2(k)$ son $\mathbb{A}^2(k)$, $\emptyset$, puntos y curvas planas irreducibles, es decir, conjuntos de la forma $V(F)$ donde F es un polinomio irreducible y $V(F)$ es infinito.*

Demostración. Sea V un conjunto algebraico irreducible en $\mathbb{A}^2(k)$. Si V es finito o $I(V) = \langle 0 \rangle$, V es claramente de algún tipo de los anteriores en la afirmación. Ahora, en el caso en el cual $I(V) \neq \langle 0 \rangle$ entonces $I(V)$ contiene un polinomio F no constante y dado que $I(V)$ es primo (pues V es irreducible) entonces algún factor irreducible de F pertenece a $I(V)$. En consecuencia podemos asumir que F es irreducible.
Ahora, notemos que si existiese $G \in I(V)$ tal que $G \notin \langle F \rangle$ entonces $V \subseteq V(F, G)$ sería finito lo cual es absurdo, luego podemos concluir que $I(V) = \langle F \rangle$ lo cual finaliza la prueba. □

1.2.4. Propiedades locales de curvas planas

En lo que resta del capítulo comenzaremos nuestro camino en el estudio de curvas planas en el espacio afín, pondremos especial atención en multiplicidades y números de intersección entre curvas. Usaremos algunos resultados acerca de teoría de módulos y anillos de valuación discreta, esto último el lector lo puede encontrar en el anexo.

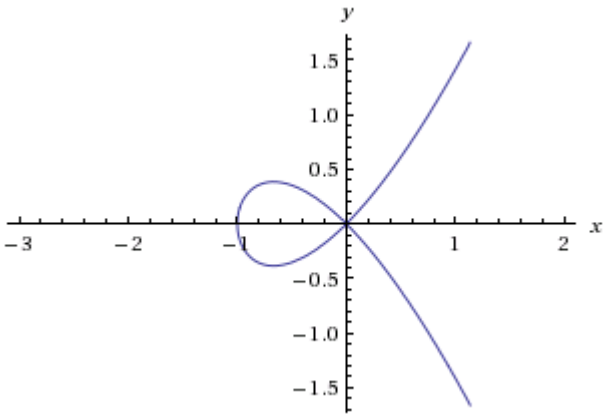
Hasta ahora habíamos hablado informalmente acerca de curvas planas afines como variedades afines de polinomios no constantes F en $k[x,y]$, es decir una curva plana afín consiste de los puntos $(a,b) \in \mathbb{A}^2(k)$ tales que satisfacen la ecuación $F(a,b) = 0$. Por simplicidad hablaremos de curvas refiriéndonos simplemente al polinomio que la define y supondremos siempre que estamos trabajando en el anillo $k[x,y]$, con k un campo algebraicamente cerrado. A continuación vamos a dar una definición un poco más precisa.

Definición 1.32. *Sean $F, G \in k[x,y]$ un par de polinomios. F y G se dice que son equivalentes si existe $\lambda \in k$ tal que $F = \lambda G$.*

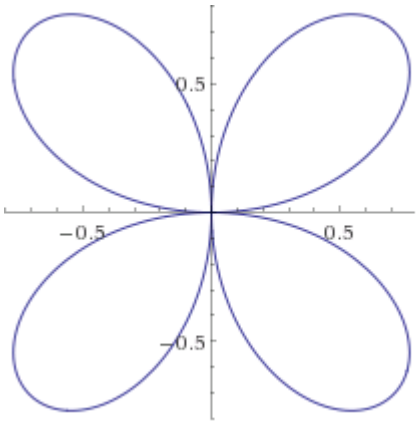
Resulta fácil probar que la anterior definición induce una relación de equivalencia $\sim$ dada por: dados $F, G \in k[x,y]$, entonces $F \sim G$ si y sólo si $F = \lambda G$ para algún $\lambda \in k$.
Definimos entonces una **curva plana afín** o simplemente **curva** (si se entiende el espacio en el que estamos trabajando), como una clase de equivalencia de polinomios no constantes bajo la relación de equivalencia anterior. Además el **grado** de una curva es el grado del polinomio que define a la curva. Una curva de grado 1 se dice que es una recta, una de grado 2 se dice que es una cónica y a una de grado 3 se le llama cubica.
Ahora, si el polinomio F que define una curva puede expresarse como $F = \prod_{i=1}^{m} F_i^{e_i}$, donde los polinomios F_i representan los factores irreducibles de F, diremos que los F_i son las *componentes* de F (i.e, las componentes de la curva definida por F) y que e_i es la *multiplicidad* de cada componente F_i.

Definición 1.33. *Sea F una curva plana afín y sea $p = (a,b) \in F$. El punto p es llamado un **punto simple** de F si, o bien la derivada parcial $F_x(p) \neq 0$ o $F_y(p) \neq 0$. En este caso la recta $F_x(p)(x-a) + F_y(p)(y-b) = 0$ es llamada la **recta tangente** a F en p.*
*Un punto que no es simple es llamado **múltiple** o **singular**. Una curva que solo posee puntos simples es llamada una **curva no singular**.*

Ejemplo 1.34. *Consideremos $k = \mathbb{C}$, sea $F_1 = x^3 + x^2 - y^2$ el polinomio que define una curva (Folium de Descartes) en $\mathbb{A}^2(\mathbb{C})$ y sea $p = (0,0)$. Para hacernos una pequeña imagen gráfica acerca de F_1, grafiquemos los puntos $\mathbb{R}-$racionales de F_1, estos son los puntos de la curva pero tomados sobre el campo $\mathbb{R} \subseteq \mathbb{C}$.*



A su vez, consideremos también $F_2 = (x^2 + y^2 - 4x^2y^2)$ *(flor de cuatro pétalos) y el punto y el mismo punto* $p = (0, 0)$.



Notemos que en ambos ejemplos anteriores un cálculo simple usando derivadas muestra que el punto $p = (0, 0)$ *es el único punto singular (múltiple).*

Definición 1.35. *Sea* F *una curva plana afín y sea* $p = (0, 0) \in \mathbb{A}^2(k)$. *Escribamos a* F *en la forma* $F = F_m + F_{m+1} + \cdots + F_n$, *donde cada* F_i *es una forma en* $k[x, y]$ *de grado* i *y además* $F_m \neq 0$ *(ver anexo A). Definimos la multiplicidad de* F *en* $p = (0, 0)$ *como el entero no negativo* m *en la escritura anterior de* F. *Dicha multiplicidad suele denotarse por* $m_p(F)$.

Observación. *En el contexto de la definición anterior:*

- $p = (0, 0) \in F$ *si y sólo si* $m_p(F) > 0$.
- *Usando las reglas básicas de derivación también puede verse que* $p = (0, 0)$ *es un punto simple de* F *si y sólo si* $m_p(F) = 1$. *En este caso,* F_1 *es exactamente la recta tangente a* F *en* p. *Si* $m = 2$, p *es llamado un punto doble, si* $m = 3$, p *es un punto triple, etc.*

Ahora, dado que una forma en dos variables, digamos F_m puede escribirse de la forma $F_m = \prod_i L_i^{r_i}$ donde los L_i son un número finito de rectas (ver Anexo A). Estas rectas son llamadas **rectas tangentes** a F en p y además los números r_i son llamados la **multiplicidad** de la tangente. Si $r_i = 1$ $(2, 3,$ etc), L_i es llamada un tangente simple (doble, triple, etc). Ahora si una curva F posee m tangentes (simples) distintas en $p = (0, 0)$,donde m denota la multiplicidad definida previamente. Decimos que p es un **punto múltiple ordinario** de F. En este sentido, un punto doble ordinario es llamado un **nodo**.

Capítulo 2

Variedades proyectivas

Al igual que en Geometría Diferencial, distinguir propiedades locales y globales de curvas resulta de vital importancia. Distintos teoremas globales pueden obtenerse mediante una «completación» de curvas algebraicas en el espacio afín agregando lo que se denomina «puntos en el infinito». En este capítulo nos enfocamos en este tipo de curvas. Inicialmente daremos una visión general de la teoría y posteriormente nos enfocamos en curvas en el plano proyectivo, allí vamos a ver un poco de dimensión en variedades, su relación con el campo de funciones racionales y algo de divisores de curvas. Lo anterior será para observar que clase de herramientas se usan en [4] para la prueba del Teorema de Riemann-Roch y así motivar la prueba que estudiamos en este trabajo.

Sea k un campo algebraicamente cerrado. Se define la *recta afín* como:

$$\mathbb{P}^1(k) := k \cup \{\infty\}$$

Más precisamente, en $k^2 \setminus \{(0,0)\}$ definimos la siguiente relación:

Dados $(a,b),(c,d) \in k^2 \setminus \{(0,0)\}$, decimos que $(a,b) \sim (c,d)$ si y sólo si existe $\lambda \in k \setminus \{0\}$ tal que $(c,d) = (\lambda a, \lambda b)$. Puede probarse fácilmente que $\sim$ es una relación de equivalencia. Al conjunto de clases de equivalencia determinadas por $\sim$ se le denota por:

$$\mathbb{P}^1(k) = \{[(a,b)] : (a,b) \in k^2 \setminus \{(0,0)\}\} = k^2 \setminus \{(0,0)\} /_{\sim}$$

En lugar de denotar la clase de un elemento (a,b) por $[(a,b)]$ usaremos el símbolo $(a:b) := [(a,b)]$.
Nótese que podemos identificar a $k = \mathbb{A}^1(k)$ con la clase de equivalencia en $\mathbb{P}^1(k)$ dada por: $\mathbb{A}^1_0(k) := \{(1:b) : b \in k\}$ pues la función:

$$\begin{aligned} \alpha : \ \mathbb{A}^1(k) &\to \mathbb{P}^1(k) \\ b &\mapsto (1:b) \end{aligned}$$

es una biyección. Por lo tanto $\mathbb{P}^1(k) = \underbrace{\mathbb{A}^1_0(k)}_{\text{"puntos afines"}} \cup \underbrace{\{(0:1)\}}_{\text{"puntos en el infinito"}}$.

En general, en $k^{n+1} \setminus \{(0,...,0)\}$ definimos la relación $\sim$ dada por:
$(a_0,...,a_n) \sim (b_0,...,b_n)$ si y sólo si existe $\lambda \in k \setminus \{0\}$ tal que $(b_0,...,b_n) = (\lambda a_0,...,\lambda a_n)$. Como en el caso anterior puede probarse que $\sim$ es una relación de equivalencia. Así pues, denotaremos por $\mathbb{P}^n(k)$ al conjunto de clases de equivalencia:

$$\mathbb{P}^n(k) := \{(a_0 : a_1 : \cdots : a_n) : \ (a_0,...,a_n) \in k^{n-1} \setminus \{(0,...,0)\}\}$$

2.1. Conjuntos algebraicos en el espacio proyectivo

Justo como hicimos en el caso afín podemos dotar al espacio $\mathbb{P}^n(k)$, llamado *espacio proyectivo n-dimensional*, de una topología también llamada Topología de Zariski. En está sección construiremos dicha topología y al igual que en el caso afín, observaremos la relación geométrica y algebraica en los cerrados mediante el Nullstellensatz proyectivo.

Definición 2.1. *Sea $f \in k[T_0,...,T_n]$ y $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$, decimos que $(a_0 : \cdots : a_n)$ es cero de f (o simplemente que $(a_0 : \cdots : a_n)$ es raíz de f en $\mathbb{P}^n(k)$) si para todo $\lambda \in k \setminus \{0\}$, $f(\lambda a_0,...,\lambda a_n) = 0$. Esto anterior lo denotaremos por $f(a_0 : \cdots : a_n) = 0$.*

Observación. *Notemos que en la definición anterior, si f es una forma de grado d, entonces $f(\lambda T_0,...,\lambda T_1) = \lambda^d f(T_0,...,T_n)$. De manera que si $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$ es tal que $f(a_0,...,a_n) = 0$ entonces $f(a_0 : \cdots : a_n) = 0$.*

Proposición 2.2. *Sea $f \in k[T_0,...,T_n]$ con $f \neq 0$ y sea $f = f_0 + \cdots f_d$ la descomposición de f como suma de formas o también llamados polinomios homogéneos (ver A) y sea $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$. Entonces $(a_0 : \cdots : a_n)$ es cero de f si y sólo si $f_i(a_0,...,a_n) = 0$ para todo $i = 0,...d$.*

Demostración. Supongamos que $(a_0 : \cdots : a_n)$ es un cero de f, entonces para cada $\lambda \in k \setminus \{0\}$ $f(\lambda a_0, \cdots, \lambda a_n) = 0$. Por consiguiente:

$$f(\lambda a_0, \cdots, \lambda a_n) = \lambda^0 f_0(a_1,...,a_n) + \lambda^1 f_1(a_0,...,a_n) + \cdots + \lambda^d f_d(a_0,...,a_n) = 0$$

Consideremos el polinomio $f_0(a_0,...,a_n) + T f_1(a_0,...,a_n) + \cdots + T^d f_d(a_0,...,a_n) \in k[T]$. Por lo anterior, todo $\lambda \in k$ tal que $\lambda \neq 0$ es raíz de este polinomio. Entonces, dado que k es infinito (pues es algebraicamente cerrado) el anterior polinomio posee infinitas raíces y por tal motivo debe ser el polinomio cero. De donde $f_i(a_0,...,a_n) = 0$ para todo $i = 0,...,d$. Recíprocamente, dado que cada f_i es una forma de grado i se sigue trivialmente que $f(a_0 : \cdots : a_n) = 0$. □

Definición 2.3. *Sea $S \subseteq k[T_0,...,T_n]$, definimos el conjunto de ceros de S en $\mathbb{P}^n(k)$ como $V_{\mathbb{P}}(S) := \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(k) : f(a_0 : \cdots : a_n) = 0, \ \forall f \in S\}$.*

La anterior definición argumenta entonces el poder definir una topología en $\mathbb{P}^n(k)$ considerando como cerrados a $V_{\mathbb{P}}(S)$ siendo $S \subseteq k[T_0, ..., T_n]$. Mas específicamente tenemos:

Proposición 2.4. *La colección* $\tau = \{\mathbb{P}^n(k) \setminus V_{\mathbb{P}}(S) : \ S \subseteq k[T_0, ..., T_n]\}$ *es una topología para* $\mathbb{P}^n(k)$ *llamada* ***Topología de Zariski*** *en* $\mathbb{P}^n(k)$*. A los cerrados de esta topología los llamamos* ***conjuntos algebraicos*** *en* $\mathbb{P}^n(k)$ *o simplemente* ***conjuntos algebraicos proyectivos****.*

Demostración. La prueba es bastante sencilla y análoga al caso afín. Dejamos los detalles como un ejercicio para el lector. □

Al igual que en el caso afín poseemos una aplicación reciproca a $V_{\mathbb{P}}(\cdot)$, mas precisamente: dado $Y \subseteq \mathbb{P}^n(k)$, se define el ideal asociado a Y como:

$$I_{\mathbb{P}}(Y) := \{f \in k[T_0, ..., T_n] : f(y_0 : \cdots : y_n) = 0 \ \ \forall (y_0 : \cdots : y_n) \in Y\}.$$

Definición 2.5. *(Ideal homogéneo) Sea* $\mathfrak{a}$ *un ideal de* $k[T_0, ..., T_n]$*. Decimos que* $\mathfrak{a}$ *es un* ***ideal homogéneo*** *de* $k[T_0, ..., T_n]$ *si para todo* $f \in \mathfrak{a}$*, las componentes homogéneas (formas asociadas a* f*)* f_i *de* f *también están en* $\mathfrak{a}$*.*

Proposición 2.6. *Sea* $Y \subseteq \mathbb{P}^n(k)$*. Entonces* $I_{\mathbb{P}}(Y)$ *es un ideal radical y homogéneo.*

Demostración. La prueba de que $I_{\mathbb{P}}(Y)$ es ideal y además ideal radical es similar a la del caso afín. Mostremos entonces que $I_{\mathbb{P}}(Y)$ es un ideal homogéneo.
Sea $f \in I_{\mathbb{P}}(Y)$, entonces justo como hicimos antes, consideremos la descomposición de f en formas, $f = f_0 + \cdots + f_m$. Mostremos que $f_i \in I_{\mathbb{P}}(Y)$. Sea $y = (y_0 : \cdots : y_n) \in Y$. Tenemos que $f(y) = 0$ (pues $f \in I_{\mathbb{P}}(Y)$). Por un argumento similar el de la Proposición 2.2 se sigue que $f_i(y_0, ..., y_n) = 0$ para todo $i = 0, ..., m$.
En consecuencia, para cada $\lambda \in k$ no nulo: $f_i(\lambda y_0, ..., \lambda y_n) = \lambda^i f_i(y_0, ..., y_n) = 0$. Esto es $f_i(y) = 0$ y por consiguiente $f_i \in I_{\mathbb{P}}(Y)$ para cada $i = 0, ..., m$. Así $I_{\mathbb{P}}(Y)$ es un ideal homogéneo. □

Observación. *De manera análoga al caso afín, puede probarse que:*

$$\begin{aligned} I_{\mathbb{P}}(\cdot) : \{Y : \ Y \subseteq \mathbb{P}^n(k)\} &\longrightarrow \{\mathfrak{a} : \ \mathfrak{a} \text{ es un ideal radical y homogeneo de } k[T_0, ..., T_n]\} \\ Y &\longmapsto \quad I_{\mathbb{P}}(Y) \end{aligned}$$

Es una aplicación antimonótona y además satisface que:

- $I_{\mathbb{P}}(Y_1 \cup Y_2) = I_{\mathbb{P}}(Y_1) \cap I_{\mathbb{P}}(Y_2)$.
- $I_{\mathbb{P}}\left(\bigcap_{i \in J} Y_i\right) = \sqrt{\sum_{j \in I} I_{\mathbb{P}}(Y_j)} := rad\left(\sum_{j \in I} I_{\mathbb{P}}(Y_j)\right)$.

Definición 2.7. *Sea $C \subseteq \mathbb{A}^{n+1}(k)$, decimos que C es un **cono** si para todo $x \in C$ y $\lambda \in k$ se cumple que $\lambda x \in C$.*

Podemos asociar a cada $Y \subseteq \mathbb{P}^n(k)$ un único cono en $\mathbb{A}^{n+1}(k)$ de la siguiente manera, inicialmente consideremos la proyección natural:

$$\begin{aligned} \pi : \mathbb{A}^{n+1}(k) \setminus \{0\} &\longrightarrow \mathbb{P}^n(k) \\ (a_0, ..., a_n) &\longmapsto (a_0 : \cdots : a_n) \end{aligned}$$

Definimos entonces:

$$\begin{aligned} \varphi : \{Y : \ Y \subseteq \mathbb{P}^n(k), Y \neq \emptyset\} &\longrightarrow \{C : C \subseteq \mathbb{A}^{n+1}(k), cono\} \\ Y &\longmapsto \varphi(Y) := \pi^{-1}(Y) \cup \{0\} \\ \emptyset &\longmapsto \varphi(\emptyset) := \emptyset \end{aligned}$$

Mostremos que φ es un función monótona y biyectiva, además su inversa es la función ψ definida por: para cada $C \subseteq \mathbb{A}^{n+1}(k)$, $C \neq \emptyset$, $\psi(C) := \pi(C \setminus \{0\})$.

Primero observemos que φ está bien definida. Sea $Y \subseteq \mathbb{P}^n(k)$, $Y \neq \emptyset$. Mostremos que $\pi^{-1}(Y) \cup \{0\}$ es un cono. En efecto, sea $p \in \pi^{-1}(Y) \cup \{0\}$ y $\lambda \in k$.
Si $p = 0$, trivialmente se sigue que $\lambda p \in \pi^{-1}(Y) \cup \{0\}$. Supongamos entonces que $p \neq 0$, digamos, $p = (a_0, ..., a_n)$, como $p \neq 0$ tenemos que $p \in \pi^{-1}(Y)$, luego $\pi(p) = (a_0 : \cdots : a_n) \in Y$, de manera que $\lambda p = (\lambda a_0, ..., \lambda a_n)$ y así $\pi(\lambda p) = (\lambda a_0 : ..., \lambda : a_n) = (a_0 : \cdots : a_n) \in Y$. Por consiguiente $\lambda p \in \pi^{-1}(Y)$.
En conclusión, $\pi^{-1}(Y) \cup \{0\}$ es un cono y así φ está bien definida. Además, resulta claro que $\varphi \circ \psi$ y $\psi \circ \varphi$ son las respectivas identidades, en consecuencia φ es una aplicación biyectiva.

Observación. *Sea $C \subseteq \mathbb{A}^{n+1}(k)$ tal que $C \neq \{0\}$. Entonces C es un cono y es cerrado (es decir conjunto algebraico) en $\mathbb{A}^{n+1}(k)$ si y sólo si $I(C)$ es homogéneo y es tal que $I(C) \neq \langle T_0, ..., T_n \rangle$.*
La prueba de este hecho es bastante fácil, de hecho, si se asume que C es cono cerrado basta reproducir un argumento similar a la Proposición 2.2. En la otra dirección es preciso considerar el Teorema de los ceros probado en la Sección 1.1.

Teorema 2.8. *(Nullstellensatz proyectivo) La aplicación:*

$$I_{\mathbb{P}}(\cdot) : \{Y : Y \subseteq \mathbb{P}^n(k), Y cerrado\} \longrightarrow \{\mathfrak{a} : \mathfrak{a} \lhd k[T_0, ..., T_n], homogeneo, \ radical \ y \ \mathfrak{a} \neq \langle T_0, ..., T_n \rangle\}$$

es biyectiva y su inversa es $V_{\mathbb{P}}(\cdot)$. Es decir, para todo ideal homogéneo $\mathfrak{a}$, $\mathfrak{a} \neq \langle T_0, ..., T_n \rangle$, se cumple que: $I_{\mathbb{P}}(V_{\mathbb{P}}(\mathfrak{a})) = rad(\mathfrak{a})$. Además, para todo $Y \subseteq \mathbb{P}^n(k)$, $\overline{Y} = V_{\mathbb{P}}(I_{\mathbb{P}}(Y))$.

Demostración. Restringiendo la función φ considerada previamente a el conjunto $\{Y : \ Y \subseteq \mathbb{P}^n(k), Y \ cerrado\}$, obtenemos que:

$$\begin{aligned} \varphi : \{Y : Y \subseteq \mathbb{P}^n(k), \ Y \ cerrado\} &\longrightarrow \{C : C \subseteq \mathbb{A}^{n+1}(k), \ C \neq \{0\}, \ C \ cono \ cerrado \ de \ \mathbb{A}^{n+1}(k)\} \\ Y &\longmapsto \pi^{-1}(Y) \cup \{0\} \end{aligned}$$

es una función biyectiva. En efecto, sea C un cono cerrado de $\mathbb{A}^{n+1}(k)$ con $C \neq \{0\}$, veamos que existe $Y \subseteq \mathbb{P}^n(k)$ cerrado tal que $\varphi(Y) = C$, es decir, $\pi^{-1}(Y) \cup \{0\} = C$. Tomemos $Y = \psi(C) = \pi(C \setminus \{0\})$, mostremos que Y es un cerrado de $\mathbb{P}^n(k)$. Como C es un cerrado de $\mathbb{A}^{n+1}(k)$, $C = V(I(C))$.
Afirmamos que $Y = V_{\mathbb{P}}(I(C))$. En efecto, sea $y = (y_0 : \cdots : y_n) \in Y$ y sea $f \in I(C)$. Dado que $f \in I(C)$, para todo $p \in C$, $f(p) = 0$. Dado que $y \in Y$ entonces existe $p \in C \setminus \{0\}$ tal que $\pi(p) = y$, esto es, $y = (y_0 : \cdots : y_n) = (p_0 : \cdots : p_n)$ con $p = (p_0 : \cdots : p_n) \in C \setminus \{0\}$.
Luego $f(p) = 0$, pero C es un cono, luego $f(\lambda p) = f(\lambda p_0, ..., \lambda p_n) = 0$ para todo $\lambda \in k \setminus \{0\}$.
Ahora, tenemos que $(y_0, ..., y_n) = (\alpha p_0, ..., \alpha p_n)$ para algún $\alpha \in k \setminus \{0\}$. Entonces:

$$f(\lambda y_0, ..., \lambda y_n) = (\alpha\lambda p_0, ..., \alpha\lambda p_n) = 0$$

así, $f(y) = 0$, i.e, $y \in V_{\mathbb{P}}(I(C))$.
Ahora, sea $z \in V_{\mathbb{P}}(I(C))$, mostremos que $z \in Y := \pi(C \setminus \{0\})$. Tenemos que $z = (z_0 : \cdots : z_n)$ con $(z_0, ..., z_n) \in \mathbb{A}^{n+1}(k) \setminus \{0\}$, mostremos que $p = (z_0, ..., z_n) \in C \setminus \{0\}$. Notemos que $\pi(p) = z$ y sea $f \in I(C)$, veamos que $f(p) = 0$. Dado que $z \in V_{\mathbb{P}}(I(C))$ y $f \in I(C)$ entonces $f(z) = 0$. De manera que $\forall \lambda \in k \setminus \{0\}$, $f(\lambda z_0, ..., \lambda z_n) = 0$. En particular, si $\lambda = 1$ se sigue que $f(p) = 0$ y por ende $p \in V(I(C)) = C$.

En virtud de la observación anterior, tenemos biyecciones de la siguiente manera:

$$\big\{Y : \ Y \subseteq \mathbb{P}^n(k), \ Y \ \textit{cerrado}\big\}$$

$$\downarrow \varphi$$

$$\big\{C : \ C \subseteq \mathbb{A}^{n+1}(k) \setminus \{0\}, \ C \ \textit{cono}, \ \textit{cerrado}\big\}$$

$$\downarrow I(\cdot)$$

$$\big\{\mathfrak{a} : \mathfrak{a} \ \textit{ideal homogeneo}, \ \textit{radical tal que } \mathfrak{a} \neq \langle T_0, ..., T_n\rangle \ \textit{de } k[T_0, ..., T_n]\big\}$$

Lo anterior garantiza que $I_{\mathbb{P}} = I \circ \varphi$ es biyectiva y por tanto $I_{\mathbb{P}}(Y) = I(\pi^{-1} \cup \{0\})$. La otra parte que resta por probar se sigue de la misma manera que en el caso afín, recomendamos ver [11]. □

Como consecuencia inmediata del teorema anterior tenemos que:

Corolario 2.9. *(Nullstellensatz débil) Sea $\mathfrak{a}$ un ideal homogéneo de $k[T_0, ..., T_n]$. Entonces, $V_{\mathbb{P}}(\mathfrak{a}) = \emptyset$ si y sólo si $rad(\mathfrak{a}) = k[T_0, ..., T_n]$ ó $rad(\mathfrak{a}) = \langle T_0, ..., T_n\rangle$.*

Observación. *Al igual que en el caso afín dado $Y \subseteq \mathbb{P}^n(k)$. Entonces Y es irreducible si y sólo si $I_{\mathbb{P}}(Y)$ es ideal primo. La prueba de esté hecho se sigue de manera similar al caso afín pero teniendo en cuenta que un ideal homogéneo P en $k[T_0, ..., T_n]$ es primo si y sólo si para cada par de polinomios homogéneos $A, B \in k[T_0, ..., T_n]$, si $AB \in P$ entonces $A \in P$ ó $B \in P$.*

Proposición 2.10. *El conjunto* $\mathbb{A}^n_0(k) := \{(1 : x_1 : \cdots : x_n) \in \mathbb{P}^n(k) : \ (x_1, ..., x_n) \in \mathbb{A}^n(k)\}$ *es un abierto de* $\mathbb{P}^n(k)$*. Además, la función:*

$$\begin{aligned} \alpha : \ \mathbb{A}^n(k) &\longrightarrow \mathbb{A}^n_0(k) \\ (x_1, ..., x_n) &\longmapsto (1 : x_1 : \cdots : x_n) \end{aligned}$$

es un homeomorfismo entre $\mathbb{A}^n(k)$ *con la Topología de Zariski y* $\mathbb{A}^n_0(k)$ *con la Topología de Zariski en* $\mathbb{P}^n(k)$*.*

Demostración. Notemos inicialmente que $\mathbb{A}^n_0(k) = \mathbb{P}^n(k) \setminus V_{\mathbb{P}}(T_0)$, de manera que $\mathbb{A}^n_0(k)$ es un abierto de $\mathbb{P}^n(k)$. Ahora, resulta claro que α es una función biyectiva, veamos que es continua y que posee inversa continua.
Sea $Z \subseteq \mathbb{A}^n_0(k)$ un cerrado, mostremos que $\alpha^{-1}(Z)$ es cerrado en $\mathbb{A}^n(k)$. Como Z es un cerrado de *Acero*, existe Y cerrado en $\mathbb{P}^n(k)$ tal que $Z = Y \cap \mathbb{A}^n_0(k)$, de donde por el Teorema 2.8 existen polinomios homogéneos $H_1, ..., H_m \in k[T_0, ..., T_n]$ tales que $Y = V_{\mathbb{P}}(H_1, ..., H_m)$.
Consideremos los polinomios $h_1, ..., h_m$ definidos por: para cada $i = 1, ..., m$:

$$h_i = H_i(1, T_1, ..., T_n)$$

Notemos entonces que $\alpha^{-1}(Z) = V(h_1, ..., h_m)$, por consiguiente es un cerrado en $\mathbb{A}^n(k)$ y en consecuencia α es continua.
Ahora, sea $X \subseteq \mathbb{A}^n(k)$ un cerrado, mostremos que $\alpha(X)$ es cerrado en $\mathbb{A}^n_0(k)$. Notemos que:

$$\begin{aligned} \alpha^{-1} \ : \ \mathbb{A}^n_0(k) &\longrightarrow \mathbb{A}^n(k) \\ (x_0 : \cdots : x_n) &\longmapsto \left(\frac{x_1}{x_0} : \cdots \frac{x_n}{x_0}\right), \quad x_0 \neq 0 \\ (1 : y_1 : \cdots : y_n) &\longmapsto (y_1 : \cdots y_n) \end{aligned}$$

Entonces, mostremos que $\alpha(X) = \mathbb{A}^n_0(k) \cap Y$, para algún $Y \subseteq \mathbb{P}^n(k)$ cerrado. Como X es un cerrado de $\mathbb{A}^n(k)$, entonces $X = V(I(X))$. Sea $Y = V_{\mathbb{P}}(\{f^* : \ f \in I(X)\})$. Donde f^* indica la homogenización de f (ver A). Afirmamos que $\alpha(X) = \mathbb{A}^n_0(k) \cap Y$.
En efecto, sea $(1 : x_1 : \cdots : x_n) \in \alpha(X)$, con $(x_1, ..., x_n) \in X$ y sea $f \in I(X)$, luego $f(x_1, ..., x_n) = 0$. Entonces:

$$f^*(1 : x_1 : \cdots : x_n) = 1^{deg(f)} f(x_1, ..., x_n) = 0$$

Por lo tanto $(1 : x_1 : \cdots x_n) \in Y$. Ahora, sea $(y_0 : \cdots : y_n) \in \mathbb{A}^n_0(k) \cap Y$, entonces $y_0 \neq 0$ y así:

$$(y_0 : \cdots : y_n) = \left(1 : \frac{y_1}{y_0} : \cdots : \frac{y_n}{y_0}\right) = \alpha\left(\frac{y_1}{y_0}, ..., \frac{y_n}{y_0}\right)$$

Nos resta mostrar entonces que $\left(\frac{y_1}{y_0}, ..., \frac{y_n}{y_0}\right) \in X$. Sea $f \in I(X)$, entonces:

$$f\left(\frac{y_1}{y_0}, ..., \frac{y_n}{y_0}\right) = y_0^{def(f)} f^*(y_1, ..., y_n) = 0$$

Luego $\left(\frac{y_1}{y_0}, ..., \frac{y_n}{y_0}\right) \in X$ y así concluimos que $\alpha(X) = \mathbb{A}_0^n(k) \cap Y$. □

El siguiente teorema nos va a permitir caracterizar la clausura de una hipersuperficie afín en el espacio proyectivo $\mathbb{P}^n(k)$. Lo anterior tiene sentido gracias a la identificación que podemos hacer mediante la función α de la proposición anterior.

Teorema 2.11. *Sea $X = V(f)$ con $f \in k[T_1, ..., T_n]$. Entonces, $\overline{\alpha(X)} = V_{\mathbb{P}}(f^*)$, es decir:*

$$\overline{\alpha(X)} = V_{\mathbb{P}}(f^*) = \left\{(y_0 : \cdots : y_n) \in \mathbb{P}^n(k) : \ f^*(y_0 : \cdots : y_n) = 0\right\}$$

donde,

$$f^* = T_0^{deg(f)} f\left(\frac{T_1}{T_0}, ..., \frac{T_n}{T_0}\right).$$

Demostración. En general, para todo $Z \subseteq \mathbb{P}^n(k)$, $\overline{Z} = V_{\mathbb{P}}(I_{\mathbb{P}}(Z))$. En particular, $\overline{\alpha(X)} = V_{\mathbb{P}}(I_{\mathbb{P}}(\alpha(X)))$. Mostremos entonces que $\overline{\alpha(X)} = V_{\mathbb{P}}(I_{\mathbb{P}}(\alpha(X))) = V_{\mathbb{P}}(f^*)$.
Sea $(y_0 : \cdots : y_n) \in \overline{\alpha(X)}$, luego para todo $F \in I_{\mathbb{P}}(\alpha(X))$, $F(y_0 : \cdots : y_n) = 0$. Mostremos que $f^* \in I_{\mathbb{P}}(\alpha(X))$. Sea $(1 : x_1 : \cdots : x_n) \in \alpha(X)$, con $(x_1, ..., x_n) \in X = V(f)$. Veamos que $f^*(1 : x_1 : \cdots : x_n) = 0$.
Como f^* es homogéneo, es suficiente mostrar que $f^*(1, x_1, ..., x_n) = 0$. En efecto:

$$f^*(1, x_1, ..., x_n) = 1^{deg(f)} f(x_1, ..., x_n) = 0$$

Por tanto $f^* \in I_{\mathbb{P}}(\alpha(X))$. En particular, $f^*(y_1 : \cdots : y_n) = 0$ y por ende $\overline{\alpha(X)} \subseteq V_{\mathbb{P}}(f^*)$.

Ahora, sea $(y_0 : \cdots : y_n) \in V_{\mathbb{P}}(f^*)$, es decir, $f^*(y_0 : \cdots : y_n) = 0$. Mostremos que $(y_0 : \cdots : y_n) \in \overline{\alpha(X)} = V_{\mathbb{P}}(I_{\mathbb{P}}(\alpha(X)))$. Sea $g \in I_{\mathbb{P}}(\alpha(X))$, veamos entonces que $g(y_0 : \cdots : y_n) = 0$. Sea $\lambda \in k \setminus \{0\}$, probemos que $g(\lambda y_0, ..., \lambda y_n) = 0$. Como

$$f^*(y_0 : \cdots : y_n) = 0$$

Se sigue que

$$f^*(\lambda y_0, ..., \lambda y_n) = 0$$

Esto es:

$$\lambda^{deg(f)} f^*(y_0, ..., y_n) = 0$$

De donde

$$f^*(y_0, ..., y_n) = 0$$

Ahora, como $g \in I_{\mathbb{P}}(\alpha(X))$, para todo $(1 : x_1 : \cdots : x_n) \in \alpha(X)$, entonces $g(1 : x_1 : \cdots : x_n) = 0$. En particular, para cada $(x_1, ..., x_n) \in X$ tenemos que $g(1, x_1, ..., x_n) = 0$. Así:

$$h = g(1, T_1, ..., T_n) \in I(X)$$

pero, $X = V(f)$, de donde $I(X) = rad(f)$. Por consiguiente $g(1, T_1, ..., T_n) \in rad(f)$, esto es, $(g(1, T_1, ..., , T_n))^m = qf$ para algún $q \in k[T_1, ..., T_n]$ y algún m entero positivo.
Homogeneizando y teniendo en cuenta las propiedades de este procedimiento (A) :

$$(h^*)^m = q^* f^*.$$

Ahora, si g es homogéneo entonces $h = g_*$ y así $((g_*)^*)^m = q^* f^*$. De manera que:

$$T_0^{(deg(g)-deg(g_*))m} ((g_*)^*)^m = T_0^{(deg(g)-deg(g_*))m} q^* f^*$$
$$g^m = T_0^{(deg(g)-deg(g_*))m} q^* f^*$$

Por tanto:

$$g^m(y_0, ..., y_n) = y_0^{(deg(g)-deg(g_*))m} q^*(y_0, ..., y_n) f^*(y_0, ..., y_n)$$

En consecuencia $g^m(y_0, ..., y_n) = 0$ y por ende $g(y_0, ..., y_n) = 0$. Esto permite concluir que $V_{\mathbb{P}}(f^*) \subseteq \overline{\alpha(X)}$.
Ahora, en el caso en que g no sea homogéneo, podemos descomponer a g en sus componentes homogéneas $g_0 + \cdots + g_l$ con g_i homogéneo de grado i y $g_i \in I_{\mathbb{P}}(\alpha(X))$. Aplicando el mismo procedimiento anterior a cada una de las componentes homogéneas g_i de de g concluimos que $g_i(y_0, ..., y_n) = 0$. □

2.2. Curvas algebraicas proyectivas

A lo largo de esta sección y las siguientes del capítulo, k denotará un campo algebraicamente cerrado.

Definición 2.12. *Sea $X \subseteq \mathbb{P}_k^2$, X es llamado una **curva algebraica proyectiva** si existe un polinomio homogéneo de grado mayor que cero, $F \in k[T_0, T_1, T_2]$ tal que $X = V(F)$. Un polinomio de grado mínimo que satisfaga lo anterior es llamado polinomio minimal para X y su grado es el **grado** que le asociaremos a la curva. Curvas de grado 1,2 y 3 serán llamadas lineas, cónicas y cubicas, respectivamente.*

Sea $X \subseteq \mathbb{A}^2(k)$ una curva algebraica con polinomio minimal $f \in k[X, Y]$ y sea f^* la homogenización de f. Entonces, gracias al Teorema 2.11, la clausura proyectiva de X es la curva algebraica proyectiva dada por $X^* = V(f^*)$. Además puede probarse fácilmente que $X = X^* \cap \mathbb{A}^2(k)$.

Teorema 2.13. *Sea X una curva algebraica proyectiva, tal que $X = V(F)$, y sea $Y = X \cap \mathbb{A}^2(k)$. Entonces*

(a) Si X no es una linea en el infinito, entonces X es una curva algebraica afín.

(b) Si X no contiene una linea al infinito, entonces la deshomogenización F_* de F es un polinomio minimal de Y y $X = \overline{Y}$, la clausura proyectiva de Y.

Demostración:

(a) Por hipótesis tenemos que la deshomogenización de F, no es constante y además se sigue que $Y = V(F_*)$.

(b) Sea $F_* = cf_1^{\alpha_1} \cdots f_n^{\alpha_n}$ la descomposición de F_* en factores irreducibles, donde $c \in k^*$, $\alpha_i \in \mathbb{N}$ y f_i es irreducible con $i = 1, ..., n$. Si deshomogenizamos con respeto a la primera variable T_0, notamos que T_0 no es un factor de F, de manera que, por propiedades A:

$$F = c(f_1^*)^{\alpha_1} \cdots (f_n^*)^{\alpha_n}$$

Pero como F es el polinomio minimal de X, debe cumplirse que $\alpha_1 = \cdots \alpha_n = 1$. Además, por la definición de la clausura proyectiva se sigue que $X = \overline{Y}$.

□

Corolario 2.14. *Existe una correspondencia uno a uno entre las curvas algebraicas afines y las curvas algebraicas proyectivas que no contienen la linea al infinito, h_∞ dada por $T_0 = 0$.*

Corolario 2.15. *Toda curva proyectiva X posee infinitos puntos, además $\mathbb{P}^2(k) \setminus X$ es infinito.*

A continuación vamos a resumir unos cuantos resultados que ya hemos visto en el caso general $\mathbb{P}^n(k)$, de igual manera recomendamos visitar [8, págs 18-19] para una reseña mas completa.

Teorema 2.16. *Sea $k[T_0, T_1, T_2]$ el anillo de polinomios, entonces:*

(a) Los ideales principales $\langle F \rangle$, donde $F \in k[T_0, T_1, T_2]$ es un polinomio no nulo homogéneo e irreducible, son primos y homogéneos. Estos ideales se corresponden de manera inyectiva con las curvas irreducibles en $\mathbb{P}^2(k)$.

(b) Los ideales $\langle aT_1 - bT_0, aT_2 - cT_0, bT_2 - cT_1 \rangle$, donde $P = (a, b, c) \in \mathbb{P}^2(k)$, son ideales homogéneos y maximal, además existe una correspondencia uno a uno entre esta clase de ideales y los puntos de $\mathbb{P}^2(k)$.

(c) El ideal cero y el ideal maximal $\langle T_0, T_1, T_2 \rangle$ son ideales primos y homogéneos.

Algunos conceptos que observamos en el capitulo anterior para curvas en el plano afín pueden reproducirse también en el caso proyectivo, veamos:

Definición 2.17. *Sea F un polinomio homogeneo en $k[T_0, T_1, T_2]$ que define una curva en $\mathbb{P}^2(k)$, usualmente nos vamos a referir a la curva por el polinomio que la define, es este caso F. El cociente $k[F] := \frac{k[T_0,T_1,T_2]}{\langle F \rangle}$ es llamado el anillo de coordenadas de la curva F.*

El anillo de funciones racionales de una curva F en $\mathbb{P}^2(k)$ se define de manera análoga como en el caso afín, es decir $k(F) = Fr(k[F])$, además el anillo local en un punto P de la curva, $\mathcal{O}_P(F)$, no es más que el conjunto de funciones racionales $\in k(F)$ que están definidas en P. Notemos que, cuando $P = (x : y : 1)$, entonces $\mathcal{O}_P(F)$ es isomorfo a $\mathcal{O}_{(x,y)}(F_*)$, donde F_* es la correspondiente curva definida por el polinomio F_*, la deshomogenización de F.

2.3. Campos algebraicos de funciones

Sea K una extensión de campos de F. Recordemos que el grado de trascendencia de una extensión K sobre F, denotado por $degtras(K|F)$, se define como el menor entero n tal que para algunos $x_1, ..., x_n \in K$, K es algebraica sobre $F(x_1, ..., x_n)$. En este caso, vamos a decir que K es un campo algebraico de funciones en n variables sobre F. Este concepto resulta muy importante pues vamos a restringir el estudio geométrico de las curvas al estudio algebraico de campos de este estilo y mediante el uso de ésta y otras herramientas estudiaremos el Teorema de Riemann-Roch.

Proposición 2.18. *Sea K un campo algebraico de funciones en una variable sobre un campo F, con F algebraicamente cerrado y sea $x \in K \setminus F$. Entonces:*

(1) K es algebraica sobre $F(x)$.

(2) Si $char(F) = 0$, existe un elemento $y \in K$ tal que $K = F(x, y)$.

(3) Si R es un dominio entero tal que $K = Fr(R)$, $F \subseteq R$ y $\mathfrak{p}$ es un ideal primo de R, entonces el homomorfismo natural de F en $R/\mathfrak{p}$ dado por $f \mapsto f + \mathfrak{p}$ es un isomorfismo.

Demostración. Veamos la prueba de (3), la prueba de (1) la veremos en el siguiente capítulo cuando hagamos un estudio más detallado de los campos algebraicos de funciones y sus propiedades. La prueba de (2) es una aplicación inmediata del Teorema del Elemento Primitivo [10, pág 55].

(3) Supongamos que existe $x \in R$ tal que $\overline{x} = x + \mathfrak{p} \notin F$ y sea $y \in \mathfrak{p}$ tal que $y \neq 0$. Tomemos $F = \sum a_i(X)Y^i \in F[X, Y]$ tal que $F(x, y) = 0$. Si tomamos F de grado minimal tal que lo anterior suceda, entonces $a_0(X) \neq 0$. De manera que $a_0(x) \in \mathfrak{p}$, en consecuencia $a_0(\overline{x}) = 0$. Sin embargo $\overline{x}$ no es un elemento algebraico sobre F de manera que no puede existir tal elemento x. Lo anterior permite concluir que tal homomorfismo es sobre, lo demás es inmediato pues F es un campo y por tanto el homomorfismo es inyectivo.

□

Supongamos ahora que X es una variedad proyectiva, es decir, es un conjunto algebraico proyectivo irreducible. La **dimensión** de X la definimos como $degtras(F(X)|F)$, donde

$F(X)$ indica el campo de funciones racionales de X. Una variedad de dimensión uno es llamada una curva y además, esta definición de curva coincide con la definición que habíamos dado anteriormente gracias a la siguiente proposición, dejaremos su prueba como lectura personal en [4, pág 76]

Proposición 2.19. *Sea X una variedad proyectiva. Entonces:*

- *Si U es una subvariedad abierta de X, entonces $dim(U) = dim(X)$.*
- *Si V^* es la clausura proyectiva de una variedad afín V, entonces $dim(V) = dim(V^*)$.*
- *Una variedad tiene dimensión cero si y sólo si es un punto.*
- *Toda subvariedad cerrada de una curva es un punto.*
- *Una subvariedad cerrada de $\mathbb{A}^2(k)$ ($\mathbb{P}^2(k)$) tiene dimensión uno si y sólo si es una curva plana afín (proyectiva).*

Curvas no singulares y sus campos de funciones

En esta sección vamos simplemente a estudiar unos cuantos resultados que nos hablan acerca de las correspondencias que existen entre los campos algebraicos de funciones y las curvas no singulares, no entraremos en muchos detalles pues nuestro objetivo radica en observar la correspondencia para comenzar, desde este punto de partida, un estudio profundo de los campos algebraicos de funciones y así estudiar la prueba del teorema en cuestión.

Definición 2.20. *Sea C una curva arbitraria y sea P un punto de C. Diremos que P es un punto **no singular** de C si el anillo local asociado, $\mathcal{O}_P(C)$ es un anillo de valuación discreto.*
Una curva C se dice que es no singular si todo punto de C es no singular.

A continuación resumiremos los resultados más destacados, dejaremos sus justificaciones como lectura personal para el lector en [4, Capítulo 7].

Teorema 2.21. *Dos curvas no singulares son isomorfas si y sólo si sus campos algebraicos de funciones asociados son isomorfos.*

Teorema 2.22. *Sea C una curva proyectiva no singular, $K = k(C)$. Entonces existe una correspondencia uno a uno entre los puntos de la curva C y los anillos de valuación discretos de K. Si $P \in C$, $\mathcal{O}_P(C)$ es el correspondiente anillo de valuación discreto de P.*

Teorema 2.23. *Sea C una curva proyectiva. Entonces existe una curva proyectiva no singular X y un morfismo birracional $f : X \to C$, es decir, un morfismo tal que existen abiertos densos de X y C de tal manera que f es un isomorfismo entre dichos abiertos densos. Además si $f' : X' \to C$ es otro morfismo birracional, entonces existe un único isomorfismo $g : X \to X'$ tal que $f' \circ g = f$.*

Teorema 2.24. *Existe una correspondencia uno a uno entre curvas proyectivas no singulares X y campos algebraicos de funciones en una variable K sobre k, a saber, $K = k(X)$.*

2.4. Hacia el Teorema de Riemann-Roch

Para el estudio del Teorema de Riemann-Roch, debemos utilizar un concepto denominado *divisor* de una curva. Veamos que dice dicho concepto y como se relaciona con el campo de funciones.
Dada una curva proyectiva irreducible C, por el Teorema 2.23, existe un morfismo birracional $f : X \to C$, donde X es una curva proyectiva no singular. En lo que resta del capítulo vamos a adoptar esta notación.
Un **divisor sobre X** es una suma formal $D = \sum_{P \in X} n_P P$, donde $n_P \in \mathbb{Z}$ y $n_P = 0$ para todos, excepto para un número finito de elementos $P \in X$. Los divisores sobre X forman un grupo abeliano, a saber, es el grupo abeliano libre sobre la curva no singular X.
Sin embargo, como la curva X es no singular, por el Teorema 2.24 a la curva se le corresponde un campo algebraico de funciones en una variable, $k(X)$, y de igual manera por el Teorema 2.22 cada uno de los puntos de la curva X se corresponde con un anillo de valuación discreto de $k(X)$, lo anterior se cumple salvo equivalencia birracional entre curvas.
De manera que el concepto de divisor puede reinterpretarse usando las respectivas correspondencias y simplemente escribir:

$$D = \sum_{P} n_P P$$

donde P es la valuación asociada al anillo de valuación discreto $\mathcal{O}_P(k) \subseteq k(X)$ (ver Anexo B, B.5). En consecuencia, podemos estudiar las valuaciones y sus anillos de valuación discretos asociados, en el contexto de campos algebraicos de funciones y dejar de lado el contexto geométrico que aparece en el estudio de las curvas. En esta sección simplemente vamos a ver que clase de herramientas se usan para la prueba clásica atribuida a Brill y Noether y en el siguiente capítulo daremos la prueba con todo detalle usando los campos de funciones.

Definición 2.25. *El **grado** de un divisor $D = \sum_{P \in X} n_P P$, denotado por $deg(D)$, se define por $\sum_{P \in X} n_P$. Además diremos que un divisor es **efectivo** (o positivo) si para cada $P \in X$, $n_P \geq 0$.*

Observación. *Mediante la definición anterior puede probarse que, dados dos divisores sobre X, D y E entonces $deg(D + E) = deg(D) + deg(E)$. Esto lo vamos a probar en el siguiente capítulo en el contexto de divisores asociados al campo de funciones de la curva.*

Notemos también que podemos definir un orden en el grupo de divisores. Si $D = \sum_{P \in X} n_P P$ y $E = \sum_{P \in X} m_P P$ entonces $D \geq E$ si y sólo si $n_P \geq m_P$ para cada $P \in X$.

Recordemos que como X es nosingular, para cada $P \in X$, $\mathcal{O}_P(X)$ es un anillo de valuación discreto. A la valuación de la cual proviene $\mathcal{O}_P(X)$ (ver Anexo B) la denotaremos por ord_P.

Definición 2.26. *Supongamos que $K = k(X) \simeq k(C)$, es el campo de funciones racionales de la curva nosingular X. Sea $z \in K$, definimos el divisor de z por:*

$$div(z) = \sum_{P \in X} ord_P(z)P.$$

Como z posee sólo un número finito de ceros y polos, $div(z)$ está bien definido. Definimos también,

$$div_0(z) = \sum_{P \in X} ord_P(z)P, \quad \text{para los puntos P tales que } ord_P(z) > 0$$
$$div_\infty(z) = \sum_{P \in X} -ord_P(z)P, \quad \text{para los puntos P tales que } \ ord_P(z) < 0$$

Estos son llamados, el divisor de ceros de z y el divisor de polos, respectivamente. Nótese que $div(z) = div_0(z) - div_\infty(z)$.
En el siguiente capítulo vamos a mostrar otras propiedades interesantes, particularmente se tiene que, para cada par de elementos $z, w \in K$ se cumple que, $div(zw) = div(z) + div(w)$ y además, $div(z^{-1}) = -div(z)$.

Proposición 2.27. *Para todo $z \in K$ no nulo, $div(z)$ es un divisor de grado cero.*

Demostración. Nuevamente, la prueba de esta clase de propiedades las vamos a hacer en el contexto de campos algebraicos de funciones, ver Teorema 3.18. □

Corolario 2.28. *Sea $z \in K$, tal que $z \neq 0$. Entonces, las siguientes afirmaciones son equivalentes:*

(1) $div(z) \geq 0$.

(2) $z \in K$.

(3) $div(z) = 0$.

Demostración. Supongamos que $div(z) \geq 0$, entonces para cada $P \in X$, $ord_P(z) \geq 0$, por tanto $z \in \mathcal{O}_P(X)$. Si $z(P_0) = \lambda_0$, para algún $P_0 \in X$, se sigue que $div(z - \lambda_0) \geq 0$ y $deg(div(z - \lambda_0)) > 0$, lo cual nos lleva a una contradicción. En consecuencia, $z \in K$.
Ahora, si $z \in K$, se sigue que para cada $P \in X$, $ord_P(z) = 0$ luego $div(z) = 0$. La otra implicación para cerrar el ciclo es inmediata. □

Corolario 2.29. *Sean $z, w \in K$ no nulos. Entonces $div(z) = div(w)$ si y sólo si $w = \lambda z$, para algún $\lambda \in K$.*

Demostración. Supongamos que $div(z) = div(w)$, entonces $div(z) - div(w) = 0$ lo cual implica que $div(\frac{z}{w}) = 0$ y así, por la proposición anterior, existe $\lambda \in K$ tal que $z = \lambda w$. La implicación de derecha a izquierda se sigue fácilmente por las definiciones y propiedades mencionadas anteriormente. □

Definición 2.30. *Sean D y E dos divisores sobre X. Decimos que D y E son linealmente equivalentes si existe $z \in K$ tal que $E = D + div(z)$. En este caso escribiremos $D \equiv E$.*

La relación anterior resulta ser una relación de equivalencia, además dicha relación posee propiedades muy interesantes que resumiremos a continuación.

Proposición 2.31. *Sean D,E,D' y E' divisores sobre la curva X, entonces:*

(1) $D \equiv 0$ si y sólo si, para algún $z \in K$ se cumple que $D = div(z)$.

(2) Si $D \equiv E$ entonces $deg(D) = deg(E)$.

(3) Si $D \equiv D'$ y $E \equiv E'$ entonces $D + E \equiv D' + E'$.

Demostración. La prueba de (1) es una aplicación inmediata de la definición de equivalencia de divisores, (2) se sigue gracias a la Proposición 2.27 y al Corolario 2.28.
Para probar (3), si $D \equiv D'$ y $E \equiv E'$, entonces existen z y w en K tales que:

$$D' = D + div(z) E' = E + div(w)$$

De manera que, $D' + E' = D + E + div(z) + div(w)$, pero $div(z) + div(w) = div(zw)$, con lo cual se sigue la propiedad (3). □

La Desigualdad de Riemann

Supongamos que $D = \sum_{P \in X}$ es un divisor sobre la curva X. Notemos que cada divisor D de cierta manera toma un número finito de puntos en la curva y les asigna números enteros. Queremos precisar cuando existe una función racional con polos sólo en los puntos escogidos y de tal manera que los polos no posean orden no mayor a n_P en cada uno de los puntos que se escogieron en la curva X. De ser cierto lo anterior, la pregunta es ¿cuántas funciones existen con esta propiedad? Lo anterior es básicamente uno de los interrogantes que pudo haberse hecho Riemann en el contexto de Variable Compleja. Su respuesta radica precisamente en el teorema que ha sido el tópico principal de este trabajo. A continuación vamos a ver ciertas nociones en el contexto de divisores de curvas que son necesarias para responder la pregunta.

Definición 2.32. *Sea D un divisor sobre la curva X. Definimos un espacio asociado al divisor D por:*

$$L(D) := \{f \in K \ : \ ord_P(f) \geq -n_P \ \forall P \in X\}$$

De manera que, por la definición anterior, una función racional $f \in L(D)$ si $div(f) + D \geq 0$ o si $f = 0$. Además $L(D)$ posee estructura de espacio vectorial sobre k, denotaremos su dimensión por $l(D)$.
Gracias a las correspondencias observadas en la Sección 2.3 y al análogo que existe entre las definiciones de divisor sobre una curva y divisor sobre un campo de funciones, podemos observar que la definición anterior puede reinterpretarse usando esta ultima noción y notar que básicamente la definición de $L(D)$ depende solamente del campo de funciones asociado.

Así pues, para resolver la pregunta formulada anteriormente, simplemente podemos hacer un estudio profundo de las extensiones de campo que poseen grado de trascendencia uno, pues dicha característica la poseen todos los campos asociados a las curvas (salvo equivalencia birracional). Para finalizar este capítulo, veamos qué propiedades posee el espacio $L(D)$ asociado a un divisor y posteriormente veremos que existe un cierto entero g de tal manera que para cada divisor D asociado a la curva X, $l(D) \geq deg(D) + 1 - g$. Esta afirmación fue el aporte de Riemannn al teorema y constituye un paso importante para computar la dimensión de $L(D)$ que será nuestro objetivo final.

Proposición 2.33. *Sean D y D' divisores sobre la curva X. Entonces:*

(1) Si $D \leq D'$ entonces $L(D) \subseteq L(D')$ y

$$dim_k\left(L(D')/L(D)\right) \geq deg(D' - D).$$

(2) $L(0) = k$ y $L(D) = 0$ siempre que $deg(D) < 0$.

(3) $L(D)$ es finito dimensional.

(4) Si $deg(D) \geq 0$ entonces $l(D) \leq deg(D) + 1$.

(5) Si $D \equiv D'$ entonces $l(D) = l(D')$.

Demostración:

(1) Como $D \leq D'$, se sigue que existen $P_1, ..., P_s \in X$ tales que $D' = D + P_1 + P_2 + \cdots + P_s$ por lo tanto

$$L(D) \subseteq L(D + P_1) \subseteq L(D + P_1 + P_2) \subset L(D + P_1 + P_2 + \cdots + P_s) = L(D').$$

En este caso, $deg(D' - D) = deg(P_1 + \cdots + P_s) = s$, luego es suficiente mostrar que para todo $P \in X$,

$$dim_k\left(L(D + P)/L(D)\right) \leq 1.$$

La prueba de este último hecho se basa en las mismas ideas del Teorema 3.23 que veremos en el siguiente capítulo.

(2) Por el Corolario 2.28 se sigue que:

$$L(0) = \{f \in K \ : \ div(f) + 0 \geq 0\} \cup \{0\} = K.$$

La otra parte se sigue gracias a la Proposición 2.31 parte (2). Las pruebas de (3) y (4) las haremos en el siguiente capítulo en el contexto de campos de funciones, de igual manera no requieren gran esfuerzo, recomendamos visitar [4, pág 99-100].

(5) Supongamos que $D \equiv D'$, entonces $D' = D + div(g)$ para algún $g \in K$. Definamos:

$$\begin{aligned} \psi : & L(D) \longrightarrow L(D') \\ & f \longmapsto fg \end{aligned}$$

Basta notar que ψ es un isomorfismo de k-espacios vectoriales y por tanto $l(D) = l(D')$.

□

Finalmente vamos a enunciar el Teorema de Riemann, nuestro siguiente objetivo será, como ya hemos mencionado, recopilar toda la información vista en esta sección en el contexto de campos algebraicos de funciones y probar, tanto el Teorema de Riemann como el Teorema de Riemann-Roch.

Teorema 2.34. *Sea D un divisor sobre la curva X, entonces existe un entero g tal que $l(D) \geq deg(D) + 1 - g$. El entero más pequeño g que satisface lo anterior es llamado el género de la curva X.*

Capítulo 3

El Teorema de Riemann-Roch

En este capítulo del trabajo estudiaremos la prueba del Teorema de Riemann-Roch siguiendo las ideas y métodos de Andre Weil [12]. Este capítulo constituye el corazón del trabajo, para el estudio de dicha prueba, introduciremos nuevamente el concepto de *campo algebraico de funciones* que vimos en la Sección 2.3. Como vimos, esta noción posee una amplia relación con el campo de funciones racionales de una curva, de manera que en este punto del trabajo nos alejaremos del estudio geométrico de las curvas que veníamos haciendo anteriormente y haremos un estudio algebraico principalmente enfocado a estudiar los campos algebraicos de funciones y sus «sitios».

3.1. Generalidades

Antes de comenzar con la prueba vamos a introducir diferentes conceptos que constituyen los pilares para estudiar la prueba del Teorema de Riemann y posteriormente el Teorema de Riemann-Roch.

3.1.1. Campos algebraicos de funciones

Definición 3.1. *Sea F un campo. Un* ***campo algebraico de funciones*** *o simplemente* ***campo de funciones*** *es una extensión de campos K de F, tal que el grado de trascendencia de K sobre F es uno, esto es, $degtras(K/F) = 1$.*

Ejemplo 3.2. *Sea F un campo, entonces el campo de funcionales racionales $F(x)$ con x un elemento trascendente sobre F es un campo de funciones sobre F.*

Notemos ahora que si K es un campo de funciones sobre F entonces para todo $x \in K \setminus F$ se cumple que [10, pág 179]:

$$degtras(K/F) = degtras(K/F(x)) + degtras(F(x)/F)$$

Pero $degtras(K/F) = degtras(F(x)/F) = 1$, de manera que $degtras(K/F(x)) = 0$. En consecuencia K es una extensión algebraica sobre $F(x)$, además si K es una extensión finitamente generada sobre F se tiene que para todo $x \in K \setminus F$: [10, pág 177]:

$$[K : F(x)] < \infty$$

A continuación vamos a introducir un concepto que jugará un papel importante en el desarrollo posterior de esta capítulo, el lector podrá leer de manera mas detallada varios resultados básicos acerca de valuaciones en el Anexo B.

Definición 3.3. *Una **valuación discreta** sobre un campo K es una función sobreyectiva ν de $K^* \twoheadrightarrow \mathbb{Z}$ (donde $K^* = K - \{0\}$ es el grupo multiplicativo asociado a K) tal que para todos $x, y \in K^*$:*

- $\nu(xy) = \nu(x) + \nu(y)$, *i.e, ν es un homomorfismo.*
- $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$.

Usualmente extendemos ν a todo K definiendo $\nu(0) = \infty$, por lo tanto, para cada $x \in K^*$ se cumple que $\nu(0) > \nu(x)$.

Para toda valuación discreta ν sobre K se tiene un **anillo de valuación discreto**, $\mathcal{O}_\nu$, definido por:

$$\mathcal{O}_\nu := \{x \in K : \ \nu(x) \geq 0\}$$

Este anillo resulta ser un anillo local (ver Anexo B) y su único ideal maximal $\mathfrak{m}_\nu$ es:

$$\mathfrak{m}_\nu := \{x \in K : \ \nu(x) \geq 1\}$$

Un importante resultado cuya prueba puede observarse en el Apéndice B dice que el ideal maximal asociado al anillo de valuación discreto $\mathcal{O}_\nu$, es principal. Es decir, $\mathfrak{m}_\nu$ está generado por sólo un elemento. Además si t es un generador para $\mathfrak{m}_\nu$, dicho generador es llamado **parámetro de uniformización**.

Ejemplo 3.4. *Consideremos el campo $\mathbb{Q}$ y sea p un número primo fijo. Vamos a ver como construir una valuación para este campo. Inicialmente, dado que $\mathbb{Z}$ es un Dominio de factorización única, todo entero no nulo n puede escribirse como un producto de primos, digamos, $n = \pm p_1^{e_1} \cdots p_k^{e_k}$.*
De manera que para un primo fijo p, definimos:

$$ord_p{}^{\mathbb{Z}}(n) = \begin{cases} e_i & si \ p = p_i \\ 0 & si \ p \neq p_1, ..., p_k \end{cases}$$

Ahora, definamos

$$\begin{aligned} ord_p{}^{\mathbb{Q}} : \mathbb{Q}^* &\longrightarrow \mathbb{Z} \\ \frac{n}{m} &\longmapsto ord_p{}^{\mathbb{Q}}\left(\frac{n}{m}\right) = ord_p{}^{\mathbb{Z}}(n) - ord_p{}^{\mathbb{Z}}(m) \end{aligned}$$

Gracias a lo anterior y haciendo un fácil computo se muestra que $ord_p{}^{\mathbb{Q}}(\cdot)$ está bien definida. Además, $ord_p{}^{\mathbb{Q}}(\cdot)$ resulta ser una valuación para el campo $\mathbb{Q}$.

Todo lo anterior nos sirve para motivar un ejemplo de valuaciones en el campo $\mathbb{C}(x)$. En vista que $\mathbb{C}$ es algebraicamente cerrado, dada $f \in \mathbb{C}[x]$ no nula, f descompone como un producto finito de polinomios lineales, es decir, podemos escribir:

$$f(x) = c(x - a_1)^{e_1} \cdots (x - a_k)^{e_k}$$

De esta manera, para $a \in \mathbb{C}$, definimos:

$$\begin{aligned} ord_{x-a} : \ \mathbb{C}[x] &\longrightarrow \mathbb{Z} \\ f(x) &\longmapsto ord_{x-a}(f(x)) = \begin{cases} e_i & si\ a = a_i \\ 0 & si\ a \neq a_1, ..., a_k \end{cases} \end{aligned}$$

De la misma manera que hicimos con $\mathbb{Q}$, podemos extender ord_{x-a} a $\mathbb{C}(x)^*$ produciendo valuaciones sobre $\mathbb{C}(x)$. Además cabe resaltar que los polinomios lineales son exactamente los elementos irreducibles (primos) de $\mathbb{C}[x]$.

Definición 3.5. *Sea K un campo de funciones sobre un campo algebraicamente cerrado F. Un **sitio** de K sobre F es una valuación discreta $\nu : K \longrightarrow \mathbb{Z}$ que es trivial sobre F, es decir, $\nu(F^*) = 0$.*

Observación. *Notemos que por el Ejemplo 3.4 y lo visto en la Sección 2.4, las valuaciones se corresponden con puntos, de manera que usualmente vamos a escribir las valuaciones sobre un campo de funciones K como P, donde la valuación de P en un elemento $f \in K$ se denota por $ord_P(f)$.*
*En este contexto, si $ord_P(f) > 0$ diremos que f tiene un **cero** de orden $ord_P(f)$ y si $ord_P(f) < 0$, diremos que f tiene un **polo** de orden $-ord_P(f)$ en P. Adicionalmente, a $|ord_P(f)|$ lo llamaremos la **multiplicidad** de f en P.*

Ejemplo 3.6. *Las valuaciones consideradas en el Ejemplo 3.4 son todas triviales sobre $\mathbb{C}$, de manera que, dichas valuaciones son sitios sobre $\mathbb{C}(x)$. Además, si*

$$r(x) = \frac{f(x)}{g(x)} \in \mathbb{C}(x)$$

con $f(x), g(x) \in \mathbb{C}(x)$, notemos que

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0 \quad si\ y\ sólo\ si\ deg(f(x)) < deg(g(x)).$$

Pero esto último es equivalente a que $-deg(f(x)) + deg(g(x)) = ord_\infty(r(x)) > 0$. *En consecuencia,* ord_∞ *mide el orden en que* $r(x)$ *toma el valor cero en el punto infinito de la esfera de Riemann.*

El siguiente teorema nos va a permitir describir los sitios de un campo de funciones K, su prueba puede consultarse en [12, págs 4-6].

Teorema 3.7. *([12, págs 4-6]) Sea* K *un campo algebraico de funciones sobre un campo* F *y sea* $x \in K \setminus F$. *Entonces los sitios del campo* K *que no se anulan en* x *se corresponden con los primos de la clausura entera de* $F[x]$ *en* K, *denotada por* R_x. *En particular, para un sitio* P *y su correspondiente primo* $\mathfrak{P}$, *si denotamos por* $(R_x)_{\mathfrak{P}}$ *a la localización de la clausura entera de* $F[x]$ *en* K *sobre el conjunto multiplicativo determinado por el complemento de* $\mathfrak{P}$. *Entonces, se cumple que* $(R_x)_{\mathfrak{P}} = \mathcal{O}_P$.

Lema 3.8. *Sea* K *un campo de funciones sobre* F *y sea* P *un sitio de* K. *Entonces*

$$[\mathcal{O}_P \,/_{\mathfrak{m}_P} \ : \ F] < \infty$$

En particular, si F *es algebraicamente cerrado,* $\mathcal{O}_P \,/_{\mathfrak{m}_P} \simeq F$

Demostración. Inicialmente notemos que como $ord_P : K^* \longrightarrow \mathbb{Z}$ es trivial sobre F^* se sigue que $F^* \subseteq \mathcal{O}_P^*$. Además $F \hookrightarrow \mathcal{O}_P \,/_{\mathfrak{m}_P}$, pues todo homomorfismo de anillos desde un campo es inyectivo. Veamos entonces que esta extensión anterior es finita.
Fijemos $x \in K \setminus F$, tal que $x \in \mathfrak{m}_P$. Entonces $ord_P(x) \geq 1$. Recordemos que la extensión $K/F(x)$ es finita. Sean $\{e_1, ..., e_n\}$ elementos de $\mathcal{O}_P$ cuyas clases módulo $\mathfrak{m}_P$ son linealmente independientes sobre F. Mostremos que $n \leq [K : F(x)]$.
Razonemos por contradicción y supongamos que $n > [K : F(x)]$, entonces tenemos un conjunto de funciones racionales $\{f_1(x), ..., f_n\} \subseteq F(x)$, no todas cero y tales que:

$$f_1(x)e_1 + \cdots + f_n(x)e_n = 0 \tag{3-1}$$

Multiplicando por un factor común (es decir, quitando los denominadores) podemos tomar a las funciones $f_i(x) \in F[x] \subseteq \mathcal{O}_P$, no todas cero.
Ahora, si ninguna de las funciones f_i posee termino constante cero, dividamos a ambos lados de (3-1) por x hasta que al menos uno de los f_i tenga termino constante no nulo. Sea c_i el termino constante de $f_i(x)$. Recordemos que $ord_P(x) \geq 1$, entonces si tomamos clase módulo $\mathfrak{m}_P$, todas las x se anulan y tenemos la ecuación:

$$c_1\overline{e_1} + \cdots c_n\overline{e_n} = 0$$

Lo anterior es en $\mathcal{O}_P \,/_{\mathfrak{m}_P}$, lo cual es absurdo pues el conjunto $\{\overline{e_1}, ..., \overline{e_n}\}$ es linealmente independiente en $\mathcal{O}_P \,/_{\mathfrak{m}_P}$. Así :

$$dim_F\left(\mathcal{O}_P \,/_{\mathfrak{m}_P}\right) \leq n \leq [K : F(x)]$$

□

Teorema 3.9. *[12, págs 7-8] Sea K un campo de funciones sobre F. Si $x \in K \setminus F$, entonces:*

$$[K : F(x)] = \sum_P max(ord_P(x), 0)[\mathcal{O}_P \,/_{\mathfrak{m}_P} : F]$$

.

Observación. Todo el estudio anterior acerca de campos algebraicos de funciones juega un papel muy importante para la prueba del Teorema de Riemann-Roch. Cuando el campo F es algebraicamente cerrado podemos reinterpretar a $f \in K$ como una función con valores de F definida sobre todos, excepto por un número finito de sitios de P, i.e, $f(P) = a$ si $ord_P(f) \geq 0$, es decir, $a \in F$, $ord_P(f - a) \geq 1$.
Notemos que si F no fuese algebraicamente cerrado, el valor de f podría no estar en F, pero si en una extensión de campo de F, a saber, $[\mathcal{O}_P \,/_{\mathfrak{m}_P} : F]$.

3.1.2. Divisores y adeles

Ahora vamos a introducir nuevos conceptos que nos van a permitir trazar la ruta hacia el objetivo de Riemann-Roch. En adelante a menos que se diga lo contrario K denotará un campo algebraico de funciones sobre F, esté último se considera algebraicamente cerrado.

Definición 3.10. *Definimos el grupo de divisores de un campo de funciones K/F, usualmente denotado por D_K, como el grupo libre abeliano considerado sobre los sitios de K. Es decir:*

$$D_K = \bigoplus_P \mathbb{Z}P = \{\sum_P n_P P \quad : n_P = 0 \quad \textit{excepto para un número finito de sitios } P\}$$

*A los elementos de D_K los llamaremos **divisores**.*

Observación. *Para referirnos a un elemento arbitrario de D_K, usaremos la notación $\sum_P n_P P$, es decir, no especificamos, a menos que sea necesario, en que sitios P se cumple que $n_P = 0$. Además, en la anterior definición la operación de grupo está definida componente a componente:*

$$\sum_P n_P P + \sum_P m_P P = \sum_P (n_P + m_P)P$$

Ejemplo 3.11. *Para todo campo de funciones K, el **divisor cero** de K está definido como $\sum_P n_P P$ donde $n_P = 0$ para todo sitio P de K. Se suele denotar por $\mathbf{0}$.*

Ejemplo 3.12. *Sea F un campo algebraicamente cerrado. Consideremos el campo de funciones $F(x)$ sobre F. Notemos que gracias a los ejemplos vistos anteriormente, podemos determinar los sitios de $F(x)$, a saber, están dados por $F \cup \{\infty\}$. Ahora, ord_P es, o bien ord_{x-a} para algún $a \in F$ o ord_∞.*
De esta manera si tomamos $F = \mathbb{C}$, se sigue que $7(i) - 3(\infty) + 4(1 - i)$ es un ejemplo de un divisor en $\mathbb{C}(x)$.

Definición 3.13. *Para un divisor $D = \sum_P n_P P$ definimos el **grado** del divisor, denotado por $deg(D)$, como:*

$$deg(D) = \sum_P n_P \in \mathbb{Z}$$

*Claramente por la definición de D_K, la anterior suma es finita. Además definimos el **soporte** del divisor, denotado por $supp(D)$, como el conjunto de sitios P en los cuales $n_P \neq 0$.*

Ejemplo 3.14. *En el contexto del Ejemplo 3.12, el grado del divisor $7(i) - 3(\infty) + 4(1-i)$ es $7 - 3 + 4 = 8$. Además su soporte está dado por $supp(D) = \{i, \infty, (1-i)\}$.*

Definición 3.15. *Sea $f \in K^*$. Definimos el divisor, $div(f)$, asociado a f como $\sum_P ord_P(f)P$. Nótese que $div(f)$ está bien definido en virtud del Teorema 3.9.*

Definición 3.16. *Sea $f \in K$. En la anterior definición podemos descomponer a $div(f)$ de la siguiente manera:*

$$div(f) = div_0(f) - div_\infty(f)$$

donde

$$div_0(f) = \sum_P max(ord_P(f), 0)P$$

y

$$div_\infty(f) = \sum_P -min(ord_p(f), 0).$$

*Además, $div_0(f)$ será llamado el **divisor de ceros** de f y a su vez div_∞ será llamado el **divisor de polos** de f.*

Lema 3.17. *Sea $f \in K \setminus F$. Entonces:*

$$deg(div_0(f)) = deg(div_\infty(f)) = [K : F(f)].$$

Demostración. Por el Teorema 3.9, tenemos que:

$$[K : F(f)] = \sum_P max(ord_P(f)), 0)[\mathcal{O}_P \,/\, \mathfrak{m}_P : F]$$

pero F es algebraicamente cerrado, luego $[\mathcal{O}_P \,/\, \mathfrak{m}_P : F] = 1$. De manera que

$$[K : F(f)] = \sum_P max(ord_P(f)), 0)[\mathcal{O}_P \,/\, \mathfrak{m}_P : F] = \sum_P max(ord_P(f)), 0) = deg(div_0(f)).$$

Ahora, si reemplazamos f por $1/f$ tenemos que $div_0(1/f) = div_\infty(f)$ pues $F(f) = F(1/f)$, por lo tanto, $deg(div_\infty(f)) = [K : F(f)]$. □

Teorema 3.18. *Sean $E = \sum_P n_P P$ y $D = \sum_P m_P P$ divisores arbitrarios de D_K. Entonces para cada $f, g \in K^*$ se cumple que:*

- $deg(E + D) = deg(E) + deg(D)$.
- $div(fg) = div(f) + div(g)$.
- $deg(div(f)) = 0$.

Demostración:

- Tenemos que:

$$deg(E + D) = deg\left(\sum_P n_P P + \sum_P m_P P\right) = deg\left(\sum_P (n_P + m_P)P\right)$$
$$= \sum_P (n_P + m_P) = deg(E) + deg(D).$$

- Recordemos que $ord_P(\cdot)$ es una valuación sobre K^*, luego para todos $f, g \in K^*$ y para todo sitio P de K:
$$ord_P(fg) = ord_P(f) + ord_P(g)$$
luego,
$$\sum_P ord_P(fg) = \sum_P (ord_P(f) + ord_P(g))$$
en consecuencia,
$$\sum_P ord_P(fg)P = \sum_P (ord_P(f) + ord_P(g))P$$
es decir,
$$div(fg) = div(f) + div(g).$$

- Ahora, como la valuación ord_P es trivial sobre F tenemos que para todo $a \in F^*$ se cumple que:
$$deg(div(a)) = \sum_P 0 = 0$$
donde $div(a) = \sum_P ord_P(a)P$. Además, para $x \in K \setminus F$, por el Lema 3.17:
$$deg(div(x)) = deg(div_0(x)) - deg(div_\infty(x)) = 0.$$

□

Una aplicación directa del teorema anterior nos permite concluir lo siguiente.

Corolario 3.19. *Sea D un divisor de D_K y sea $f \in K^*$, entonces*

$$deg(D + div(f)) = deg(D).$$

Observación. *Podemos definir un orden parcial en D_K de la siguiente manera: dados dos divisores $\sum_P n_P P$, $\sum_P m_P P$, decimos que $\sum_P n_P P \geq \sum_P m_P P$ si y sólo si para cada sitio P, $n_P \geq m_P$, donde este último es el orden usual en $\mathbb{Z}$.*

Definición 3.20. *Sea D un divisor. Definimos un espacio asociado a D, denotado por $L(D)$, como $L(D) := \{f \in K^* \ : \ div(f) + D \geq \mathbf{0}\} \cup \{0\}$.*

Este espacio $L(D)$ resulta ser un espacio vectorial sobre F. Cuando $L(D)$ es un espacio finito-dimensional sobre F, denotamos por $l(D) := dim_F(L(D))$.
En lo que sigue vamos a estudiar distintas herramientas para demostrar que el espacio definido anteriormente, $L(D)$, resulta ser un F-espacio vectorial finito-dimensional, esté resultado es muy importante pues de hecho el objetivo del Teorema de Riemann-Roch es computar la dimensión de $L(D)$, es decir, $l(D)$.

Definición 3.21. *Un divisor $\sum_P n_P P$ es llamado **efectivo** en un sitio P si $n_P \geq 0$. Además un divisor se dice que es **efectivo** si es efectivo en cada punto P.*

Observación. *Notemos que por definición, para $f \in K \setminus F$, los divisores de ceros y polos de f son efectivos.*
Ahora, sea $D = \sum_P n_P P$ entonces:

$$\begin{aligned} f \in L(D) &\Leftrightarrow div(f) + D \geq \mathbf{0} \\ &\Leftrightarrow \sum_P (ord_P(f) + n_P)P \geq \mathbf{0} \\ &\Leftrightarrow ord_P(f) + n_P \geq 0 \ \Leftrightarrow \ ord_P(f) \geq -n_P \end{aligned}$$

Corolario 3.22. *Sea D un divisor tal que $dim_F(L(D)) < \infty$ y sea $g \in K$. Entonces*

$$L(D + div(g)) = L(D).$$

En consecuencia, $l(D + div(g)) = l(D)$.

Demostración. Por definición tenemos que $L(D) = \{f \in K^* \ : \ div(f) + D \geq \mathbf{0}\} \cup \{0\}$. Además:

$$\begin{aligned} L(D + div(g)) &= \{f \in K^* \ : \ div(f) + div(g) + D \geq \mathbf{0}\} \cup \{0\} \\ &= \{f \in K^* \ : \ div(fg) + D \geq \mathbf{0}\} \cup \{0\} \\ &= \{h \in K^* \ : \ div(h) + D \geq \mathbf{0}\} \cup \{0\} \\ &= L(D) \end{aligned}$$

□

Teorema 3.23. *Sea D un divisor del grupo de divisores asociado a K tal que $l(D)$ está definida. Entonces, para sitio P de K se cumple que:*

$$l(D + P) \leq l(D) + 1.$$

Demostración. Sea $D = n_P P + \sum_{Q \neq P} n_Q Q$ un divisor de D_K tal que $l(D)$ está definida, es decir, $L(D)$ es finito-dimensional sobre F. Por una observación anterior, tenemos que para cada $f \in L(D+P)$, $ord_P(f) \geq -n_P - 1$.
Ahora, si adicionalmente suponemos que $f \notin L(D)$ entonces se sigue que para algún sitio Q, $ord_Q(f) + n_Q < 0$. Sin embargo, como $f \in L(D+P)$, lo anterior sólo puede suceder para el sitio $Q = P$, en cuyo caso $ord_P(f) + n_P = -1$.
Sea $m := n_P + 1$. Entonces $ord_P(f) = -n_P - 1 = -m$, por consiguiente cada $f \in L(D + P) \setminus L(D)$ tiene orden $-m$ en P. Si tal f no existiese, tendríamos que $L(D+P) = L(D)$ y por tanto tendríamos lo que se quiere probar.
Motivados por lo anterior, supongamos que existe $f \in L(D+P)$ tal que f tiene exactamente orden $-m$ en el sitio P. Recordemos que P es una valuación discreta, la cual tiene asociado un anillo de valuación discreto y que por la Proposición B.3 y el Lema B.6 dicho anillo posee un único ideal maximal, esté último resulta ser principal. Entonces, sea $t \in K$ un parámetro de uniformización para P tal que $ord_P(t) = 1$. Como $ord_P(f) = -m$ y $ord_P(t^m) = m \cdot ord_P(t) = m$. Entonces:

$$ord_P(t^m f) = ord_P(t^m) + ord_P(f) = m - m = 0$$

en consecuencia, $t^m f \in \mathcal{O}_P \big/ \mathfrak{m}_P$. Ahora, como F es algebraicamente cerrado se sigue que $\mathcal{O}_P \big/ \mathfrak{m}_P \simeq F$. Lo anterior permite deducir que existe un $a \in F^*$ tal que:

$$t^m f \equiv a \ mod \ \mathfrak{m}_P.$$

De manera que $t^m f - a \in \mathfrak{m}_P$, es decir, para algún $x \in \mathcal{O}_P$ tenemos que $t^m f = a + xt$.
Supongamos ahora que g es otro elemento de $L(D+P)$ de orden $-m$ en P. Entonces, de manera análoga a como hicimos con f, existen $b \in F^*$ y $y \in \mathcal{O}_P$ tales que $t^m g = b + yt$. Así:

$$f = at^{-m} + xt^{-m+1} \ , \ g = bt^{-m} + yt^{-m+1}$$

luego

$$g - \frac{b}{a} f = (bt^{-m} + yt^{-m+1}) - (bt^{-m} + \frac{b}{a} x t^{-m+1}) = \left(y - \frac{b}{a} x \right) t^{-m+1}.$$

Entonces:

$$ord_P \left(g - \frac{b}{a} f \right) = ord_P \underbrace{\left(y - \frac{b}{a} x \right)}_{\in \mathcal{O}_P} + ord_P(t^{-m+1})$$
$$\geq 0 + (-m+1) = -n_P$$

Lo anterior permite concluir que $g - \frac{b}{a} f \in L(D)$ y por lo tanto, cualesquier par de elementos no nulos de $L(D+P) \setminus L(D)$ son linealmente dependientes.
Así pues,

$$dim_F \left(L(D+P) \Big/ L(D) \right) = 1$$

y por ende,

$$dim_F(L(D+P)) \leq 1 + dim_F(L(D))$$

es decir,

$$l(D+P) \leq 1 + l(D).$$

□

Corolario 3.24. *[12, pág 12] Para todo divisor D de K se cumple que, $l(D) \leq deg(D) + 1$ ó $l(D) = 0$.*

Una consecuencia interesante del corolario anterior es que la cota que hemos encontrado para $l(D)$ es óptima, más específicamente tenemos:

Corolario 3.25. *Para cualquier campo de funciones K, la desigualdad $l(D) \leq deg(D) + 1$ es óptima, es decir, la igualdad se satisface para al menos un divisor D asociado al campo de funciones K.*

Demostración. Sea K un campo algebraico de funciones y consideremos el divisor cero $\mathbf{0}$. Sea $f \in K^*$, por definición $f \in L(\mathbf{0})$ si y sólo si $\sum_P ord_P(f)P \geq \mathbf{0}$, esto es, para cada sitio P, $ord_P(f) \geq 0$. Sin embargo, por el Teorema 3.9 tenemos:

$$[K : F(f)] = \sum_P max(ord_P(f), 0) = \sum_P ord_P(f) = deg(div(f)) = 0.$$

Por lo tanto, $K = F(f)$ y así $f \in F$. En consecuencia, $l(\mathbf{0}) = 1$. □

Hasta el momento hemos establecido una cota superior óptima para $l(D)$ que depende sólo del grado del divisor D. En lo que sigue vamos a estudiar como encontrar una cota inferior para $l(D)$ que dependa de D. Más específicamente, deseamos encontrar una constante g que depende de K tal que $l(D) \geq deg(D) + 1 - g$ de ta manera que la anterior desigualdad también sea óptima.
Para realizar lo anterior, introduciremos un concepto que proviene de Teoría Algebraica de Números, denominado espacio adele del campo K.

Definición 3.26. *Definimos el **anillo adele** $\mathbb{A}_K$, asociado a un campo de funciones K, como el producto directo restringido de K con respecto a $\mathcal{O}_P$ indexado sobre los sitios P de K, mas específicamente, $\mathbb{A}_K$ es un subconjunto de $\prod_P K$ tal que para cada $\prod_p x_P \in \prod_P K$, se cumple que $x_P \in \mathcal{O}_P$ excepto para un número finito de sitios P.*
*Usualmente a los elementos del anillo adele los llamaremos **adeles** y además a un adele que es de la forma $\prod_P x_P$ lo denotaremos por (x_P).*

Observación. *Podemos identificar al campo K con un subconjunto del anillo adele de manera natural bajo el embebimiento diagonal*

$$K \hookrightarrow \mathbb{A}_K$$
$$x \mapsto (x)$$

Definición 3.27. *Sea K un campo de funciones y sea D un divisor de la forma $\sum_P n_P P$. Definimos el* ***espacio adele*** *asociado a D, denotado por $A_K(D)$, como el conjunto de todos los adeles (x_P) tales que para cada sitio P:*

$$ord_P(x_P) + n_P \geq 0 \quad ó \quad x_P = 0.$$

Además, como $n_P = 0$ para todo P excepto para un número finito, entonces para cada divisor D se sigue que $A_K(D) \subseteq \mathbb{A}_K$.

Lema 3.28. *Sean $E = \sum_P m_P P$ y $D = \sum_P n_P P$ divisores asociados a K. Entonces:*

1. *Si $D \leq E$ entonces $A_K(D) \subseteq A_K(E)$.*
2. *Si $min\{E, D\} = \sum_P min\{m_P, n_P\}P$ entonces $A_K(min\{E, D\}) = A_K(E) \cap A_K(D)$.*
3. *Si $max\{E, D\} = \sum_P max\{m_P, n_P\}P$ entonces $A_K(max\{E, D\}) = A_K(E) + A_K(D)$.*
4. *Identificando a K mediante el embebimiento diagonal, $K \cap A_K(D) = L(D)$.*

Demostración:

1. Supongamos que $E \leq D$, entonces para cada P, $m_P \leq n_P$, además si $(x_P) \in A_K(E)$ entonces para cada P tal que $x_P \neq 0$ tenemos

$$ord_P(x_P) + m_P \geq 0 \Rightarrow ord_P(x_P) + n_P \geq 0$$

Luego, $ord_P(x_P) + n_P \geq ord_P(x_P) + m_P \geq 0$. En consecuencia $(x_P) \in A_K(D)$.

2. Por el literal anterior se sigue que $A_K(min\{E, D\}) \subseteq A_K(E) \cap A_K(D)$. Ahora, sea $(x_P \in A_K(E) \cap A_K(D)$. Entonces para cada P tal que $x_P \neq 0$,

$$ord_P(x_P) + n_P \geq 0$$
$$ord_P(x_P) + m_P \geq 0$$

Por lo tanto, $ord_P(x_P) + min\{m_P, n_P\} \geq 0$ y así

$$A_K(E) \cap A_K(D) = A_K(min\{E, D\}).$$

3. Sean $(x_P) \in A_K(D)$ y $(y_P) \in A_K(E)$ entonces para los sitios P tales que $x_P + y_P = 0$ se cumple trivialmente que $(x_P) + (y_P) \in A_K(max\{E, D\})$.
Ahora, si al menos uno de x_P, y_P es no nulo, entonces, supongamos sin pérdida de generalidad que x_P es cero y que y_P es no nulo. De manera que,

$$ord_P(x_P + y_P) \geq min\{ord_P(x_P), ord_P(y_P)\}.$$

Por ende, para todo sitio P:

$$ord_P(x_P + y_P) + \text{máx}\{n_P, m_P\} \geq \text{mín}\{ord_P(x_P), ord_P(y_P)\} + \text{máx}\{n_P, m_P\}$$

y por hipótesis

$$\text{mín}\{ord_P(x_P), ord_P(y_P)\} + \text{máx}\{n_P, m_P\} \geq 0.$$

En consecuencia, $x_P + y_P \in A_K(\text{máx}\{D, E\})$.

4. Recordemos que $L(D) = \{f \in K^* \ : \ div(f) + D \geq \mathbf{0}\}$ donde $div(f) = \sum_P ord_P(f)P$. De manera que por las definiciones de $L(D)$ y $A_K(D)$ se sigue fácilmente que $K \cap A_K(D) = L(D)$. □

3.2. Desigualdad de Riemann

El concepto de adele resulta ser una herramienta importante pues nos va a permitir establecer el Teorema (desiguladad) de Riemann, primero observaremos un par de lemas y posteriormente vamos a establecer una cota superior para $deg(D) - l(D)$ para cualquier divisor D asociado al campo K. Dicha cota superior involucra un concepto muy usado en superficies de Riemann denominado **género**.

Lema 3.29. *Sean E, D divisores de K tales que $D \leq E$. Entonces*

$$dim_F\left(\frac{A_K(E)}{A_K(D)}\right) = deg(E) - deg(D).$$

Demostración. Procedamos por inducción sobre $deg(E) - deg(D)$. Consideremos varios casos:

- Si $deg(E) - deg(D) = 0$ entonces, como $D \leq E$ debe cumplirse que $E = D$. Así que $A_K(E) = A_K(D)$ y por tanto
$$\frac{A_K(E)}{A_K(D)} = \{0\}.$$
Se sigue entonces que $dim_F\left(\frac{A_K(E)}{A_K(D)}\right) = 0$.

- Si $deg(E) - deg(D) = 1$ y $D \leq E$ entonces $E = D + P$ para algún sitio P. De esta manera, probar que el teorema se cumple si $deg(E) - deg(D) = 1$ es lo mismo que mostrar que, para cada divisor D y todo sitio P,
$$dim_F\left(\frac{A_K(D+P)}{A_K(D)}\right) = 1.$$
Entonces, sea $D = \sum_P n_P P$ arbitrario y sea P un sitio de K. Consideremos las siguientes aplicaciones:
$$A_K(D+P) \xrightarrow{\pi} \mathfrak{m}_P^{-n_P-1} \xrightarrow{\varphi} \mathfrak{m}_P^{-n_P-1} \Big/ \mathfrak{m}_P^{-n_P}$$
$$(x_Q) \equiv \left(\prod_{Q \neq P} x_Q\right) \times x_P \longmapsto x_P \longmapsto x_P + \mathfrak{m}_P^{-n_P}$$
Notemos que π es sobreyectiva, pues si $f \in \mathfrak{m}_P^{-n_P-1}$, basta tomar $(x_Q) \in A_K(D+P)$ y considerar
$$f \times \prod_{Q \neq P} x_Q \in A_K(D+P)$$

entonces, $\pi(f \times \prod x_Q) = f$. Además φ claramente también es sobre. De manera que la composición $\pi \circ \varphi$ es sobreyectiva.

Ahora, si $(x_Q) \in A_K(D+P)$ y $(x_Q) \in ker(\pi \circ \varphi)$ entonces $x_P \in \mathfrak{m}_P^{-n_P}$ en cuyo caso $ord(x_P) \geq -n_P$ ó $x_P = 0$.
Sin embargo, como $(x_Q) \in A_K(D+P)$, para $Q \neq P$:

$$ord_Q(x_Q) \geq -n_Q \ \text{ y } \ (x_Q) \in A_K(D).$$

En consecuencia, $ker(\pi \circ \varphi) = A_K(D)$. Aplicando el primer Teorema de Isomorfismos [2];

$$\left(\frac{A_K(D+P)}{A_K(D)}\right) \simeq \left(\frac{\mathfrak{m}_P^{-n_P-1}}{\mathfrak{m}_P^{-n_P}}\right).$$

Recordemos que el ideal $\mathfrak{m}_P$ es principal, entonces existe t parámetro uniformizador (generador) tal que $\mathfrak{m}_P = \langle t \rangle = t\mathcal{O}_P$. Con base en lo anterior, definamos:

$$\begin{aligned} \psi \ : \mathcal{O}_P &\longrightarrow \frac{\mathfrak{m}_P^{-n_P-1}}{\mathfrak{m}_P^{-n_P}} \\ f &\longmapsto f \cdot t^{-n_P-1} + \mathfrak{m}_P^{-n_P} \end{aligned}$$

Puede notarse que la aplicación anterior es sobreyectiva y además,

$$\begin{aligned} ker(\psi) &= \{f \in \mathcal{O}_P \ : \ f \cdot t^{-n_P-1} + \mathfrak{m}_P^{-n_P} = 0 + \mathfrak{m}_P^{-n_P}\} \\ &= \{f \in \mathcal{O}_P \ : \ f \cdot t^{-n_P-1} \in \mathfrak{m}_P^{-n_P}\} \\ &= \{f \in \mathcal{O}_P \ : \ ord_P(f \cdot t^{-n_P-1}) \geq -n_P\} \\ &= \{f \in \mathcal{O}_P \ : \ ord_P(f) + ord_P(t^{-n_P-1}) \geq -n_P\} \\ &= \{f \in \mathcal{O}_P \ : \ ord_P(f) \geq -n_P - ord_P(t^{-n_P-1})\} \\ &= \{f \in \mathcal{O}_P \ : \ ord_P(f) \geq -n_P - ((-n_P-1)ord_P(t))\} \\ &= \{f \in \mathcal{O}_P \ : \ ord_P(f) \geq -n_P - ((-n_P-1)\cdot 1) = 1\} = \mathfrak{m}_P \end{aligned}$$

por ende ψ es sobreyectiva y nuevamente por el primer Teorema de Isomorfismos, se sigue que

$$\mathcal{O}_P \,/\mathfrak{m}_P \simeq \frac{\mathfrak{m}_P^{-n_P-1}}{\mathfrak{m}_P^{-n_P}}.$$

Entonces,

$$\frac{A_K(D+P)}{A_K(D)} \simeq \mathcal{O}_P \,/\mathfrak{m}_P$$

pero, en virtud del Lema 3.8 tenemos que $dim_F(\mathcal{O}_P \,/\mathfrak{m}_P) = dim_F(F) = 1$. Así,

$$dim_F\left(\frac{A_K(D+P)}{A_K(D)}\right) = 1.$$

- Supongamos ahora que para algún $n \geq 1$, $deg(E) - deg(D) = n$ y que el resultado se cumple para todos los divisores $E \geq D$ tales que $dim_F(\frac{A_K(E)}{A_K(D)}) < n$. Dado que $E \geq D$, podemos encontrar un divisor E' tal que $E \geq E' \geq D$ y que satisface lo siguiente:

$$\begin{aligned} deg(E) - deg(E') &= 1 \\ deg(E') - deg(D) &= n. \end{aligned}$$

Entonces, como $A_K(D) \subseteq A_K(E') \subseteq A_K(E)$, luego aplicando la hipótesis de inducción se sigue que:

$$\begin{aligned} dim_F\left(\frac{A_K(E)}{A_K(D)}\right) &= dim_F\left(\frac{A_K(E)}{A_K(E')}\right) + dim_F\left(\frac{A_K(E')}{A_K(D)}\right) \\ &= deg(E) - deg(E') + deg(E') - deg(D) \\ &= deg(E) - deg(D). \end{aligned}$$

□

Lema 3.30. *Sean E, D divisores de K, entonces si consideramos a K mediante su identificación en $\mathbb{A}_K$ bajo el emebebimiento diagonal se tiene que*

$$dim_F\left(\frac{A_K(E) + K}{A_K(D) + K}\right) = (deg(E) - l(E)) - (deg(D) - l(D)).$$

Demostración. Definamos

$$\begin{aligned} A_K(E) &\xrightarrow{\varphi} A_K(E) + K \\ (x_P) &\longmapsto (x_P) + 0 \end{aligned}$$

$$\begin{aligned} A_K(E) &\xrightarrow{\psi} \frac{A_K(E) + K}{A_K(D) + K} \\ (x_P) + (x) &\longmapsto (x_P) + (x) + (A_K(D) + K) \end{aligned}$$

Notemos que la composición $\varphi \circ \psi$ es sobreyextiva y además,

$$\begin{aligned} ker(\psi \circ \varphi) &= \{(x_P) \in A_K(E) \ : \ (x_P) \in A_K(D) + K\} \\ &= A_K(E) \cap (A_K(D) + K). \end{aligned}$$

Luego,

$$\frac{A_K(E)}{A_K(E) \cap (A_K(D) + K)} \simeq \frac{A_K(E) + K}{A_K(D) + K}$$

Sin embargo, $D \leq E$, $A_K(E) \cap K = L(E)$ y $A_K(min\{D, E\}) = A_K(D) = A_K(E) \cap A_K(D)$. De manera que:

$$\frac{A_K(E)}{A_K(E) \cap (A_K(D) + K)} = \frac{A_K(E)}{A_K(D) \cap A_K(E) + A_K(E) \cap K} = \frac{A_K(E)}{A_K(D) + L(E)}.$$

Además, por teoremas de isomorfismos;

$$\frac{A_K(E)}{A_K(D)+L(E)} \simeq \frac{\frac{A_K(E)}{A_K(D)}}{\frac{A_K(D)+L(E)}{A_K(D)}}.$$

En consecuencia y por el Lema 3.29,

$$dim_F\left(\frac{A_K(E)+K}{A_K(D)+K}\right) = deg(E) - deg(D) - dim_F\left(\frac{A_K(D)+L(E)}{A_K(D)}\right).$$

Ahora, como $\frac{A_K(D)+L(E)}{A_K(D)} \simeq \frac{L(E)}{A_K(D)+L(E)}$, para concluir el resultado queremos entonces que $A_K(D)+L(E) = L(D)$. Lo anterior es válido, pues $E \geq D \Rightarrow L(D) \subseteq L(E)$ y por tanto:

$$L(D) = K \cap A_K(D) \subseteq L(E) \subseteq K \text{ y además } L(E) \subseteq K,$$

esta serie de inclusiones implica que $A_K(D) \cap L(E) = L(D)$ y así,

$$\left(\frac{A_K(D)+L(E)}{A_K(D)}\right) \simeq \frac{L(E)}{L(D)} \text{ y } dim_F\left(\frac{L(E)}{L(D)}\right) = l(E) - l(D).$$

Con lo cual se sigue lo que se quería probar. □

Notación. En adelante denotaremos por $r(D)$ a $deg(D) - l(D)$.

Como consecuencia del lema anterior y las definiciones introducidas a lo largo de esté capítulo, puede probarse fácilmente el siguiente lema.

Lema 3.31. *Si $f \in K^*$ y E, D son dos divisores de K, entonces la aplicación $r : D_K \to \mathbb{Z}$ satisface:*

- *Si $D \geq E$ entonces $r(D) \geq r(E)$.*
- *Para todo divisor D, $r(div(f) + D) = r(D)$.*

Teorema 3.32 (Riemann)**.** *Sea K un campo de funciones sobre F. Entonces, para todo divisor D, $r(D)$ está acotado superiormente.*

Demostración. Sea $x \in K \setminus F$. Por el Lema 3.17, $deg(div_\infty) = [K : F(x)]$. Denotemos por n a $[K : F(x)]$.
Sea $y \in R_x$, donde R_x denota la clausura entera de $F[x]$ en K, i.e,

$$R_x = \{z \in K \ : \ z \text{ es entero sobre } F[x]\}.$$

Notemos que si para un sitio P, $ord_P(x) \geq 0$ entonces $x \in \mathcal{O}_P$ en cuyo caso $F[x] \subseteq \mathcal{O}_P$. Lo anterior nos permite concluir que y es entero sobre $\mathcal{O}_P$, pues y satisface un polinomio

en $F[x]$, el cual es también un polinomio de $\mathcal{O}_P[x] = \mathcal{O}_P$. Ahora, como $\mathcal{O}_P$ es un anillo de valuación discreto es integralmente cerrado (ver Anexo B) y por ende $y \in \mathcal{O}_P$, es decir, $ord_P(y) \geq 0$. Esto último es equivalente a que si $ord_P(y) < 0$ entonces $ord_P(x) < 0$, es decir, «todo polo de y es un polo de x».
Si recordamos la Definición 3.13, lo anterior puede reescribirse en términos de divisores como $supp(div_\infty(y)) \subseteq supp(div_\infty(x))$. Recordemos que el divisor de polos de un elemento de K es efectivo, luego para cada $f \in K^*$, existe $k \in \mathbb{Z}^+$ suficientemente grande tal que:

$$0 \leq div_\infty(y) \leq kdiv_\infty(x).$$

Recordemos también que $div_\infty(y) = div_0(y) - div(y)$, luego

$$kdiv_\infty(x) + div(y) \geq div_0(y) \geq 0.$$

Así, para cada $y \in R_x$, $y \in L(kdiv_\infty(x))$ para algún k que depende de y suficientemente grande. Como $[K : F(x)] = n$, existe $\{y_1, ..., y_n\} \subseteq R_x$ base para K como $F(x)$-espacio vectorial. Además, como $y_i \in R_x$ para cada $i = 1, ..., n$, tenemos que $y_i \in L(k_i div_\infty(x))$ para algunos enteros k_i, $i = 1, ..., n$.
Sea, $k := \text{máx}\{k_1, ..., k_n\}$, entonces para cada $i = 1, ..., n$ se cumple que $y_i \in L(kdiv_\infty(x))$. Sea $m \geq k$ y sea $G = \{x^i y_j \ : \ 1 \geq j \geq n \ , \ 0 \geq i \geq m-k\}$, mostremos que G es un conjunto linealmente independiente sobre F. Consideremos la combinación lineal:

$$\alpha_{01}x^0y_1+\alpha_{02}x^0y_2+\cdots+\alpha_{0n}x^0y_n+\alpha_{11}x^1y_1+\cdots+\alpha_{1n}x^1y_n+\cdots+\alpha_{ij}x^iy_j+\cdots+\alpha_{m-k,n}x^{m-k}y_n = 0$$

equivalentemente

$$(\alpha_{01}x^0+\alpha_{11}x^1+\alpha_{21}x^2+\cdots+\alpha_{m-k,1}x^{m-k})y_1+\cdots+(\alpha_{0n}x^0+\alpha_{1n}x^1+\alpha_{2n}x^2+\cdots+\alpha_{m-k,n}x^{m-k})y_n = 0$$

pero los y_i son linealmente independientes, entonces, para cada $j = 1, ..., n$:

$$\alpha_{0j}x^0 + \alpha_{1j}x^1 + \alpha_{2j}x^2 + \cdots + \alpha_{m-k,j}x^{m-k} = 0$$

y como x es trascendente sobre F, se sigue que:

$$\alpha_{01} = \alpha_{02} = \cdots = \alpha_{11} = \cdots = \alpha_{m--k,n} = 0.$$

Entonces, G es un conjunto linealmente independiente y además los elementos de G están en $L(mdiv_\infty(x))$, por tanto, $l(mdiv_\infty(x)) \geq n((m-k)+1)$.

Recordemos ahora que $r(D) = deg(D) - l(D)$ y notemos que por el Lema 3.31, si $E \geq D$ entonces $r(E) \geq r(D)$. Luego:

$$\begin{aligned} r(mdiv_\infty(x)) &= deg(mdiv_\infty(x)) - l(mdiv_\infty(x)) \\ &\leq (mn) - (n(m-k+1)) \\ &= nk - n. \end{aligned}$$

En virtud del Lema 3.30, $\{r(mdiv_\infty(x))\}_{m\in\mathbb{Z}}$ es una sucesión creciente de enteros y por lo mostrado anteriormente está acotada superiormente, de manera que dicha sucesión debe ser eventualmente constante. Definamos está sucesión eventualmente constante como $g-1$, (escribimos $g-1$ en lugar de g para asegurarnos que g es no negativa, pues si tomamos $m=0$ entonces $mdiv_\infty(x)=\mathbf{0}$ y $r(\mathbf{0})=-1$). Esta constante que hemos exhibido es nuestro candidato para que $r(D)\leq g-1$ para todo divisor D. Ya hemos visto que esta desigualdad anterior se cumple para los divisores $mdiv_\infty(x)$.
Para un divisor arbitrario D, podemos dividir el soporte del divisor en los sitios donde x no tiene polos y los sitios donde x posee polos, es decir:

$$D = D_1 + D_2$$

donde D_1 indica la parte del divisor D donde x no tiene polos y D_2 la parte en la cual x posee polos. Además, se tiene que

$$\begin{aligned} supp(D_1)\cap supp(div_\infty(x) &= \emptyset \\ supp(D_2) &\subseteq supp(div_\infty(x)). \end{aligned}$$

Consideremos cualquier sitio P en el cual D_1 no es efectivo. Entonces x no posee polos en P en cuyo caso $F[x]\subseteq\mathcal{O}_P$. Adicionalmente, $F[x]\cap\mathfrak{m}_P\neq\{0\}$, luego $F[x]\cap\mathfrak{m}_P$ es un ideal primo de $F[x]$.
Sea $t_P(x)$ un elemento no nulo irreducible tal que genera a $\mathfrak{m}_P\cap F[x]$. Entonces para algún entero $m_P\geq 1$, $div(t_P(x)^{m_P})+D_1$ es efectivo en P. Además, como $F[x]\subseteq R_x$, se sigue que $supp(div_\infty(t_P(x)))\subseteq supp(div_\infty(x))$ y así $supp(div_\infty(t_P(x)))\cap D_1=\emptyset$. En consecuencia $div_\infty(t_P(x)^{m_P})+D_1$ sólo posee coeficientes enteros negativos en los sitios de $supp(div_\infty(x))$.

Si hacemos lo anterior para cada sitio P donde D_1 no es efectivo, entonces si definimos $f(x):=\prod_P t_P(x)^{m_P}\in F[x]$, luego $div(f(x))+D_1$ es efectivo excepto en los sitios en los cuales x posee polos. También tenemos que D_2 es efectivo en todo sitio excepto en los cuales x tiene polos, pues $supp(D_2)\subseteq supp(div_\infty(x))$. En consecuencia $div(f(x))+D_1+D_2=div(f(x))-D$ es efectivo sobre el complemento del soporte de $div_\infty(x)$. Si escogemos un $m\in\mathbb{Z}$ suficientemente grande, el divisor:

$$div(f(x)) - D + mdiv_\infty(x)$$

resulta ser efectivo, por lo tanto $div(f(x))+mdiv_\infty(x)\geq D$, así por el Lema 3.31:

$$r(div(f(x))+mdiv_\infty(x)) = r(mdiv_\infty(x))\geq r(D).$$

Si m es suficientemente grande, $r(mdiv_\infty(x))=g-1$, por lo que $r(D)\leq g-1$. □

Definición 3.33. *Definimos el* ***genero*** *de un campo de funciones K/F como el entero $g\geq 0$ tal que:*

$$\begin{aligned} g &:= 1+\max_D r(D) \\ &= 1+\max_{m\geq 0}\ r(mdiv_\infty(x)). \end{aligned}$$

Donde $x \in K \setminus F$.

Corolario 3.34. *[Riemann] Para cada divisor D de un campo de funciones K/F de genero g, se tiene que*

$$l(D) \geq deg(D) - g + 1.$$

Demostración. Notemos que $r(D) := deg(D) - l(D)$ y por el teorema anterior $r(D) \geq g - 1$ para todo divisor D, de manera que $deg(D) - l(D) \geq g - 1$ y reorganizando se sigue el resultado. □

Observación. El corolario anterior es lo que se conoce como Teorema de Riemann, a continuación veremos un ejemplo que muestra que la cota hallada en el Teorema 3.32 es óptima.

Ejemplo 3.35. *Sea D un divisor del campo de funciones $K = F(x)$, donde F es un campo algebraicamente cerrado y $x \in K$ es trascendente sobre F. Supongamos que el divisor D es tal que $deg(D) \geq 0$, entonces por el Corolario 3.24 se tiene que $l(D) \leq deg(D) + 1$. Dado que $F(x)$ posee genero 0, entonces por el Corolario 3.34 tenemos:*

$$l(D) \geq deg(D) - g + 1 = deg(D) + 1.$$

En consecuencia, si D es un divisor de $F(x)$, o bien $l(D) = deg(D) + 1$ ó $l(D) = 0$.

Veamos que la cota encontrada para $l(D)$ en 3.34 no sólo es óptima para $K = F(x)$ como en el ejemplo anterior, sino que también lo es para cualquier campo de funciones K.

Corolario 3.36. *Sea D un divisor asociado a K. Entonces existe una constante c de tal manera que si $deg(D) \geq c$ entonces*

$$l(D) = deg(D) - g + 1.$$

Demostración. Justo como en la prueba al Teorema de Riemann, tomemos $x \in K \setminus F$ arbitrario y m suficientemente grande tal que $r(mdiv_\infty(x)) = g-1$ y sea $c = m \cdot [K : F(x)] + g$. Si D es un divisor de K tal que $deg(D) \geq c$, entonces:

$$deg(D - m \cdot div_\infty(x)) = deg(D) - m \cdot deg(div_\infty(x)) \geq (m \cdot [K : F(x)] + g - m \cdot [K : F(x)]) = g.$$

Por ende, por el Corolario 3.34,

$$l(D - m \cdot div_\infty(x)) \geq deg(D - m \cdot div_\infty(x)) - g + 1 \geq g - g + 1 = 1.$$

Luego $L(D - m \cdot div_\infty(x)) \neq \{0\}$. Ahora, sea $y \in L(D - m \cdot div_\infty(x))$ distinto de cero, por definición,

$$div(y) + D - m \cdot div_\infty(x) \geq \mathbf{0}$$

equivalentemente

$$div(y) + D \geq m \cdot div_\infty(x).$$

Por el lema 3.31,

$$r(D) = r(div(y) + D) \geq r(m \cdot div_\infty(x)) = g - 1$$

pero teníamos que $r(D) \geq g - 1$, luego

$$r(D) = deg(D) - l(D) = g - 1.$$

□

Corolario 3.37. *Sea D un divisor de K tal que $deg(D) \geq c$, donde c es la constante del Corolario 3.36. Entonces, $A_K(D) + K = \mathbb{A}_K$.*

Demostración. Sea E un divisor de K tal que $E \geq D$. Entonces, por el Lema 3.30:

$$dim_F \left(\frac{A_K(E) + K}{A_K(D) + K} \right) = r(E) - r(D).$$

Además, como $deg(D) \geq c$ se sigue por el corolario anterior que $r(D) = g - 1$, de manera que si $deg(E) \geq c$ y $deg(D) \geq c$, entonces:

$$dim_F \left(\frac{A_K(E) + K}{A_K(D) + K} \right) = (g - 1) - (g - 1) = 0$$

y por tanto, $A_K(E) + K = A_K(D) + K$. Supongamos que $D = \sum_P n_P P$ con $deg(D) \geq c$ y sea (ϕ_P) un adele. Definamos $E = \text{máx}\{D, -div((\phi_P))\}$. Notemos que $E \geq D$, y como $deg(D) \geq c$, lo anterior implica que $\mathbb{A}_K(D) + K = A_K(E) + K$.
También tenemos que

$$(\phi_P) \in A_K(-div((\phi_P)) \subseteq A_K(E) \subseteq A_K(E) + K = A_K(D) + K.$$

por lo tanto, si D posee un grado suficientemente grande cualesquier adele de $\mathbb{A}_K$ pertenece a $A_K(D) + K$. De lo anterior y gracias a que $A_K(D) + K$ es subconjunto de $\mathbb{A}_K$ se sigue lo que se quería probar. □

3.3. Teorema de Riemann-Roch

Finalmente vamos a estudiar el Teorema de Riemman-Roch. Para ello, introduciremos el concepto de diferencial de Weil y de espacio de diferenciales de Weil. Vamos a mostrar que el espacio de diferenciales de Weil es un K-espacio vectorial finito dimensional, este resultado es de vital importancia pues esto implica que $l(D) = deg(D) - g + 1 + l(div(\omega) - D)$.

Al igual que en la sección anterior, en esta parte K denotará un campo de funciones sobre un campo F con F algebraicamente cerrado.

Definición 3.38. *Un **diferencial de Weil** de K o simplemente **diferencial**, si se entiende el contexto en el cual estamos hablando, se define como una función $\omega : \mathbb{A}_K \to F$ tal que ω es lineal sobre F y además se anula en K y en $A_K(D)$ para algún divisor D. Es decir,*

- $\omega(A_K(D)) = 0$, *para algún divisor D de K.*
- $\omega(K) = 0$.

Notación. El espacio de diferenciales de K, i.e, el conjunto de funciones $\omega : \mathbb{A}_K \to F$ que satisfacen las dos condiciones anteriores será denotado por Ω_K. Además, el espacio de diferenciales que se anulan sobre $A_K(D)$ para algún divisor fijo D será denotado por $\Omega_K(D)$.

Notemos que para cada $a \in F$ y $\omega \in \Omega_K$, $a \cdot \omega$ es también una función F-lineal de $\mathbb{A}_K$ en F. Además notemos que si ω se anula sobre $A_K(D)$ para algún divisor D, entonces $a \cdot \omega$ también se anula sobre $A_K(D)$.
Lo anterior permite dotar a Ω_K y $\Omega_K(D)$ de estructura de F-espacios vectoriales, pues

$$\Omega_K(D) = Hom_F\left(\frac{\mathbb{A}_K}{A_K(D) + K}, F\right).$$

Teorema 3.39. *Sea D un divisor de K. Entonces $\Omega_K(D)$ es un F-espacio finito dimensional y $l(D) = deg(D) - g + 1 + dim_F(\Omega_K(D))$.*

Demostración. Sea E un divisor de K tal que $E \geq D$ y su grado es suficientemente grande de tal manera que por el Corolario 3.37, $A_K = A_K(E) + K$. Entonces

$$\Omega_K(D) = Hom_F\left(\frac{\mathbb{A}_K}{A_K(D) + K}, F\right) = Hom_F\left(\frac{A_K(E) + K}{A_K(D) + K}, F\right).$$

Además, por el Lema 3.30,

$$dim_F\left(\frac{A_K(E) + K}{A_K(D) + K}\right) = r(E) - r(D) < \infty$$

de manera que $\Omega_K(D)$ es finito-dimensional y $dim_F(\Omega_K(D)) = dim_F\left(\frac{\mathbb{A}_K}{A_K(D)+K}\right)$. En particular, como $r(E) = g - 1$ y $A_K(E) + K = \mathbb{A}_K$, para cada divisor E de grado suficientemente grande, tenemos:

$$dim_F(\Omega_K(D)) = g - 1 - (deg(D) - l(D)).$$

□

Corolario 3.40. *El genero g de un campo de funciones K está dado por, $g = dim_F(\Omega_K(\mathbf{0}))$.*

Demostración. Por el teorema anterior,

$$\begin{aligned} l(\mathbf{0}) &= deg(\mathbf{0}) - g + 1 + dim_F(\Omega_K(\mathbf{0})) \\ 1 &= 0 - g + 1 + dim_F(\Omega_K(\mathbf{0})) \end{aligned}$$

luego, $dim_F(\Omega_K(\mathbf{0})) = g$. □

Teorema 3.41. *Sea ω un diferencial de Weil no nulo. Entonces existe un divisor D tal que ω se anula sobre $A_K(E)$ si y sólo si $E \geq D$.*

Demostración. Sea $S_\omega = \{E \in D_K \ : \ \omega(A_K(E)) = 0\}$. El Corolario 3.37 nos dice que para un divisor E, existe una constante c tal que si $deg(E) \geq c$ entonces $A_K(E) + K = \mathbb{A}_K$; equivalentemente, si $\mathbb{A}_K \neq A_K(E) + K$ entonces $deg(E) < c$.
Como ω es un diferencial no nulo, existe algún adele $\phi \in \mathbb{A}_K$ tal que $\omega(\phi) \neq 0$. Por tanto, si $E \in S_\omega$ entonces $A_K(E) + K \neq \mathbb{A}_K$, luego tenemos una cota, que depende del divisor, para el grado de los divisores en S_ω.
Como $deg(\cdot) : D_K \to \mathbb{Z}$, podemos fijar en S_ω un divisor de grado máximo, este divisor es único pues si existiese otro divisor $E \in S_\omega$, por definición de S_ω se tiene que ω se anula en $A_K(E)$ y $A_K(D)$. Por lo tanto, ω se anula en:

$$A_K(E) + A_K(D) = A_K(\text{máx}\{E, D\}).$$

De manera que $\text{máx}\{E, D\} \in S_\omega$. Ahora, por definición $\text{máx}\{E, D\} \geq D$, luego

$$deg(\text{máx}\{E, D\}) \geq deg(D).$$

Como D tiene grado maximal en S_ω, se sigue que $deg(D) = deg(\text{máx}\{E, D\})$ y entonces debe cumplirse que $D = \text{máx}\{E, D\}$ y así $D \geq E$. □

Definición 3.42. *El divisor D de mayor grado en el Teorema 3.41 tal que ω se anula sobre $A_K(D)$ es denotado por $div(\omega)$.*

Lema 3.43. *Sea $\omega \in \Omega_K$ y $\alpha \in K^*$, entonces*

$$div(\alpha \cdot \omega) = div(\alpha) + div(\omega).$$

Demostración. Sea $(\phi_P) \in \mathbb{A}_K$, $D = \sum_P n_P P$ y $\alpha \in K^*$. Notemos que para todo P,

$$\begin{aligned} \alpha(\phi_P) \in A_K(D) &\Leftrightarrow ord_P(\alpha\phi_P) + n_P \geq 0 \text{ ó } \phi_P = 0 \\ &\Leftrightarrow ord_P(\phi_P) + (ord_P(\alpha) + n_P) \geq 0 \text{ ó } \phi_P = 0 \\ &\Leftrightarrow \phi \in A_K(div(\alpha) + D). \end{aligned}$$

Luego, si ω se anula sobre $A_K(D)$ entonces $\alpha \cdot \omega$ se anula sobre $A_K(div(\alpha) + D)$ y viceversa. Por lo tanto

$$\omega \in \Omega_K(D) \Leftrightarrow \alpha \cdot \omega \in \Omega_K(div(\alpha) + D).$$

Ahora, claramente $\omega \in \Omega_K(div(\omega))$ y así $div(\alpha) + div(\omega) \in S_{\alpha\cdot\omega}$ donde $S_{\alpha\cdot\omega}$ es el mismo conjunto considerado en 3.41.
Gracias a lo anterior, si $D = div(\alpha \cdot \omega)$, entonces $D \geq div(\alpha) + div(\omega)$. Tenemos entonces que

$$\alpha \cdot \omega \in \Omega_K(D) = \Omega_K(div(\alpha) + (D - div(\alpha)))$$

luego, por la equivalencia anterior, $\omega \in \Omega_K(D - div(\alpha))$. Sin embargo, por la definición de $div(\omega)$,

$$div(\omega) \geq D - div(\alpha).$$

Luego $D \leq div(\omega) + div(\alpha)$, lo cual completa la prueba. □

Lema 3.44. *Sean $\omega \in \Omega_K$ no nulo y D un divisor de K, entonces*

$$L(div(\omega) - D)\omega \subseteq \Omega_K(D).$$

Más aún, $L(E\omega) \subseteq \Omega_K(D)$ si y sólo si $E \leq div(\omega) - D$.

Demostración. Dado $\alpha \in K^*$, entonces por el Lema 3.43,

$$\alpha \in L(div(\omega) - D) \Leftrightarrow div(\omega) + div(\alpha) = div(\alpha\omega) \geq D.$$

Lo anterior implica que $A_K(div(\alpha\omega)) \supseteq A_K(D)$. Como $\alpha\omega$ se anula sobre $A_K(div(\alpha\omega))$ también se anula sobre $A_K(D)$. □

Hemos visto que el espacio de diferenciales de Weil es un F-espacio vectorial de dimensión finita, nuestro siguiente objetivo es mostrar que también es un K-espacio vectorial, pero en esté caso resulta ser unidimensional.

Teorema 3.45. *El espacio de diferenciales de Weil es un K-espacio vectorial unidimensional.*

Demostración. Por el Lema 3.44 sabemos que, para cada par de diferenciales no nulos ω y η y cualquier divisor D,

$$L(div(\omega) - D)\omega \subseteq \Omega_K(D)$$
$$L(div(\eta) - D)\eta \subseteq \Omega_K(D).$$

Ahora, si existiese un elemento digamos, ρ, en la intersección de los espacios del lado izquierdo en la proposición anterior, entonces para α y β en K elementos no nulos tenemos:

$$\rho = \alpha\omega = \beta\eta$$

Por lo tanto tendríamos que ω y η serían linealmente dependientes sobre K.
Como $\Omega_K(D)$, $L(div(\omega) - D)\omega$ y $L(div(\eta) - D)\eta$ son F-espacios vectoriales, se sigue que

$$L(div(\omega) - D)\omega \subseteq \Omega_K(D)$$
$$L(div(\eta) - D)\eta \subseteq \Omega_K(D)$$

vistos como F-espacios vectoriales. Razonemos por el absurdo y supongamos que $L(div(\omega) - D)\omega \cap L(div(\eta) - D)\eta = \{0\}$, por tanto como ambos son subespacios vectoriales se sigue que

$\Omega_K(D)$ debe contener a $L(div(\omega) - D)\omega \oplus L(div(\eta) - D)\eta$.
En consecuencia, tenemos que

$$dim_F(\Omega_K(D)) \geq l(div(\omega) - D) + l(div(\eta) - D)\eta. \tag{3-2}$$

Lo anterior es válido para cualquier divisor D, de manera que nuestro paso a seguir es construir un divisor tal que lo anterior no pueda suceder.
Sea $n \geq 1$ y sea P un sitio. Si fijamos $D = -nP$, por el Teorema 3.39 tenemos

$$dim_F(\Omega_K(-nP) = l(-nP) - deg(-nP) + g - 1.$$

Ahora, como $L(-nP) = \{f \in K^* \ : \ div(f) - nP \geq \mathbf{0}\} \cup \{0\}$. Entonces, $f \in L(-nP)$, si y sólo si $\sum_P ord_P(f)P - nP \geq \mathbf{0}$, equivalentemente, para todo sitio P, $ord_P(f) \geq n$, pero $n \geq 1$. Luego siguiendo un argumento similar al usado en el Corolario 3.25, se tiene que lo anterior es imposible para $f \in K$ no nula, luego $l(-nP) = 0$. Por lo tanto

$$dim_F(\Omega_K(-nP)) = n + g - 1.$$

Ahora, por el Teorema 3.32 tenemos:

$$\begin{aligned} g - 1 &\geq l(div(\omega) + nP) - deg(div(\omega) + deg(nP)) \\ l(div(\omega) + nP) &\geq deg(div(\omega)) + deg(nP) - g + 1 \\ &= deg(div(\omega)) + n - g + 1 \end{aligned}$$

además,

$$\begin{aligned} l(div(\eta) + nP) &\geq deg(div(\eta)) + deg(nP) - g + 1 \\ &= deg(div(\eta) + n - g + 1. \end{aligned}$$

Luego si $L(div(\omega) - D)\omega \cap L(div(\eta) - D)\eta = \{0\}$, por (3-2) tenemos que

$$\begin{aligned} n + g - 1 &\geq 2n - 2g + 2 + deg(div(\omega)) + deg(div(\eta)) \\ n &\leq 3g - 3 - deg(div(\omega)) + deg(div(\eta)). \end{aligned}$$

De manera que, como $n \geq 1$ era arbitrario, si escogemos un n suficientemente grande la anterior desigualdad no se cumple, es decir, para $D = -nP$,

$$L(div(\omega) - D)\omega \cap L(div(\eta) - D)\eta \neq \{0\}.$$

Lo anterior nos permite entonces concluir que cualesquier par de diferenciales son linealmente dependientes sobre K. □

Corolario 3.46. *Sea D un divisor, entonces para todo diferencial $\omega \in \Omega_K(D)$, $L(div(\omega) - D) \simeq \Omega_K(D)$ vistos como F-espacios vectoriales.*

Demostración. Por el Lema 3.44, la función

$$\begin{aligned} \varphi \ : K &\hookrightarrow \Omega_K(D) \\ \alpha &\mapsto \alpha \cdot \omega \end{aligned}$$

mapea $L(div(\omega) - D)$ en $\Omega_K(D)$ y como K es un campo, está función es inyectiva. Así, por el Teorema 3.45, todo diferencial no nulo η puede escribirse como $\beta \cdot \omega$ para algún $\beta \in K^*$. Queremos ver que $\beta \in L(div(\omega) - D)$ o equivalentemente que

$$div(\beta) + div(\omega) = div(\beta \cdot \omega) \geq D.$$

Razonemos por el absurdo y supongamos que lo anterior es falso, es decir, $\beta \notin L(div(\omega) - D)$, entonces $div(\beta \cdot \omega) < D$ y en particular

$$\begin{aligned} deg(div(\beta \cdot \omega)) &= deg(div(\beta)) + deg(div(\omega)) \\ &= 0 + deg(div(\omega)) < deg(D). \end{aligned}$$

Sin embargo, como $\omega \in \Omega_K(D)$ entonces en virtud del Teorema 3.41 se sigue que $div(\omega) \geq D$, luego

$$deg(div(\omega)) \geq deg(D).$$

Lo cual es absurdo por lo anterior, de manera que $\beta \in L(div(\omega) - D)$ y la función $\alpha \mapsto \alpha \cdot \omega$ es entonces un isomorfismo. □

Teorema 3.47 (Riemann-Roch)**.** *Sea D un divisor y ω un diferencial no nulo, entonces*

$$l(D) = deg(D) - g + 1 + l(div(\omega) - D).$$

Demostración. Por el corolario anterior, para todo divisor D y todo diferencial ω no nulo se tiene que $dim_F(\omega_K(D)) = l(div(\omega) - D)$. En consecuencia, por el Teorema 3.39:

$$\begin{aligned} l(D) &= deg(D) - g + 1 + dim_F(\Omega_K(D)) \\ &= deg(D) - g + 1 + l(div(\omega) - D). \end{aligned}$$

□

Estudios posteriores

La presente monografía es el fruto de un estudio preliminar en Geometría algebraica y el Teorema de Riemann-Roch representa un primer paso en dicho estudio.
Existen diferentes versiones y generalizaciones del teorema que estudiamos, muchas de estas involucran un lenguaje y conceptos modernos que, como mencionamos en la introducción, fueron influenciados gracias al trabajo de Grothendieck. Así pues, un posible paso a seguir en este momento es estudiar dichas generalizaciones del teorema usando herramientas modernas que involucran nociones tales como esquemas, sheaves y cohomología. Para este nuevo objetivo, recomendamos las siguientes fuentes:

Hartshorne, R. *Algebraic Geometry*, Springer Science & Business Media, 1977.

Qing,L. *Algebraic Geometry and Arithmetic Curves*, OUP Oxford, 2006.

Apéndice A

Formas

El uso de polinomios homogéneos o formas y el proceso de homogenizar y deshomogenizar un polinomio fue usado ampliamente en el Capítulo 2. A continuación daremos unos cuantos detalles acerca de en que consisten estos procesos y algunas propiedades asociadas a las formas y sus homogenizaciones.
A lo largo de este anexo, R denotará un anillo conmutativo con unidad. Recordemos que en el anillo de polinomios en $n-$variables, $R[x_1, ..., x_n]$, los *monomios* son polinomios de la forma $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ con $i_1, ..., i_n$ enteros no negativos. El *grado de un monomio* de este estilo es $i_1 + \cdots i_n$.
Recordemos también que $F \in R[x_1, ...x_n]$ tiene una única escritura en la forma:

$$F = \sum_{(i)} a_{(i)} x^{(i)}.$$

Aquí (i) denota el multi-indice dado por $(i) = i_1, i_2, ..., i_n$, de manera que $x^{(i)}$ denota el monomio $x_1^{i_1} \cdots x_n^{i_n}$. Además cada $a_{(i)} \in R$.

Definición A.1. *Sea $F \in R[x_1, ..., x_n]$, decimos que F es **homogeneo** o es una **forma de grado d**, si todos los coeficientes $a_{(i)}$ son cero excepto para monomios de grado d.*

Observación. *De la definición anterior y la escritura de polinomios como suma de monomios podemos notar que todo polinomio $F \in R[x_1, ..., x_n]$ posee una única expresión en la forma:*

$$F = F_0 + F_1 + \cdots F_d$$

donde para cada $i = 1, ..., d$, se cumple que F_i es una forma de grado i. Con lo cual si $F_d \neq 0$, d es el grado del polinomio F denotado por $deg(F)$.

Existe un proceso para «homogeneizar» o «deshomogeneizar» polinomios con respecto a una variable. Para ello, consideremos ahora R como un dominio entero. Si $F \in R[x_1, ..., x_{n+1}]$ es

una forma, definimos $F_* \in R[x_1, ..., x_n]$ (deshomogenizar) como el polinomio:

$$F_* = F(x_1, ..., x_n, 1).$$

De manera reciproca, para cada polinomio $f \in R[x_1, ..., x_n]$ de grado d, escribamos $f = f_0 + \cdots + f_d$ (donde cada f_i es una forma de grado i). Definimos $f^* \in R[x_1, ..., x_{n+1}]$ (homogenizar) como:

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

f^* es entonces una forma de grado d.

Proposición A.2. *Sean $F, G \in R[x_1, ..., x_{n+1}]$ y sean $f, g \in R[x_1, ..., x_n]$. Entonces:*

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

(2) $(F + G)_* = F_* + G_*$ y $x_{n+1}^t (f + g)^* = x_{n+1}^r f^* + x_{n+1}^s g^*$ donde $r = deg(g)$, $s = deg(f)$ y $t = r + s - deg(f + g)$.

(3) Si F es homogeneo entonces $(F_*)^* \cdot x_{n+1}^{deg(F) - deg(F_*)} = F$.

Demostración. (1) y (2) son simples cómputos y se siguen fácilmente. Mostremos (3). Notemos que:

$$F_*(x_1, ..., x_n) = F(x_1, ..., x_n, 1).$$

Luego

$$(F_*)^* = x_{n+1}^{deg(F_*)} F\left(\frac{x_1}{x_{n+1}}, ..., \frac{x_n}{x_{n+1}}, 1\right).$$

Por otro lado

$$\begin{aligned} F(x_1, ..., x_{n+1}) &= x_{n+1}^{deg(F)} F\left(\frac{x_1}{x_{n+1}}, ..., \frac{x_n}{x_{n+1}}, 1\right) \\ &= x_{n+1}^{(deg(F) - deg(F_*)} (F_*)^*. \end{aligned}$$

□

Apéndice B

Anillos de valuación discretos

Un concepto de vital importancia en álgebra conmutativa es el de *valuación discreta*. En este anexo daremos una breve reseña de este concepto junto con el de *dominio de Dedekind* con el fin de fundamentar su uso en la Sección 3.1.1. Para el lector que desee una mayor profundidad en dichos conceptos recomendamos visitar [1, 6], estas fuentes han sido la guía para este anexo.
A lo largo de este apéndice supondremos que todos los anillos son conmutativos y poseen identidad multiplicativa denotada por 1.

Definición B.1. *Sea R un dominio entero y denotemos por A a su campo de fracciones. Decimos que R es un* ***anillo de valuación*** *de A si, para cada $x \in A \setminus \{0\}$ se cumple que $x \in R$ o $x^{-1} \in R$.*

Lema B.2. *Sea R un anillo y $\mathfrak{m} \neq \langle 1 \rangle$ un ideal de R tal que todo $x \in R \setminus \mathfrak{m}$ es unidad. Entonces el anillo R es local, esto es, posee un único ideal maximal el cual es $\mathfrak{m}$.*

Demostración. Notemos que si un ideal $\mathfrak{b}$ de R contiene una unidad se sigue inmediatamente que $\mathfrak{b} = \langle 1 \rangle = R$. luego todo ideal $\mathfrak{b}$ de R consiste de no-unidades y por consiguiente en virtud de la hipótesis del lema se sigue que $\mathfrak{b} \subseteq \mathfrak{m}$ y así el anillo R es local y $\mathfrak{m}$ es su único ideal maximal. □

Proposición B.3. *Sea R un anillo de valuación de $A = Fr(R)$. Entonces:*

(i) *R es un anillo local.*

(ii) *R es integralmente cerrado en A.*

Demostración. ***(i)*** Sea $\mathfrak{m}$ el conjunto de no-unidades en R, notemos que si $\mathfrak{m}$ fuese un ideal de R, por el lema anterior podríamos concluir que R es local con ideal maximal $\mathfrak{m}$. Notemos que, $x \in \mathfrak{m}$ si y sólo si $x = 0$ o $x^{-1} \notin R$, ahora dado $a \in R$ tenemos que en cualquier caso $ax \in \mathfrak{m}$ pues si $x = 0$ trivialmente se sigue que $ax \in \mathfrak{m}$. Ahora, en el otro caso, si $ax \notin \mathfrak{m}$ entonces $(ax)^{-1} \in R$ y por tanto $x^{-1} = a \cdot (ax)^{-1} \in R$, lo cual es absurdo.

Ahora, sean $x, y \in \mathfrak{m}$ no nulos. Entonces, o bien $xy^{-1} \in R$ o $x^{-1}y \in R$. Si $xy^{-1} \in R$ entonces $x + y = (1 + xy^{-1})y \in R\mathfrak{m} \subseteq \mathfrak{m}$, de manera similar se sigue que $x + y \in \mathfrak{m}$ si $x^{-1}y \in R$. En consecuencia $\mathfrak{m}$ es un ideal y por tanto el anillo R es local.

(ii) Sea $x \in A$ un elemento entero sobre R. Entonces tenemos que existe un polinomio mónico con coeficientes en R tal que:

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

con $b_i \in R$, para $i = 1, ..., n$. Notemos que si $x \in R$ no habría nada que probar, de lo contrario, es decir, si $x \notin R$ entonces por hipótesis $x^{-1} \in R$, de tal manera que:

$$x = -(b_1 + b_2 x^{-1} + \cdots + b_n x^{1-n}) \in R$$

□

Definición B.4. *Sea k un campo. Una **valuación discreta** sobre k es un mapeo ν de k^* sobre $\mathbb{Z}$ (donde $k^* = k - \{0\}$ es el grupo multiplicativo asociado a k), tal que, para todos $x, y \in k^*$:*

- $\nu(xy) = \nu(x) + \nu(y)$, *i.e, ν es un homomorfismo.*
- $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$.

*El conjunto que consiste de 0 y de todos $x \in k^*$ tales que $\nu(x) \geq 0$ es un anillo, el cual es llamado el **anillo de valuación** de ν. Resulta apropiado en ciertos casos extender el mapeo ν a todo k haciendo $\nu(0) = +\infty$.*

Definición B.5. *Sea R un dominio entero. R se dice que es un **anillo de valuación discreto** (DVR) si existe una valuación discreta ν de $k = Fr(R)$ en $\mathbb{Z}$ tal que R es el anillo de valuación de ν.*

Lema B.6. *Sea R un DVR. Gracias a la Proposición B.3, R es local, por lo tanto sea $\mathfrak{b}$ su único ideal maximal. Entonces $\mathfrak{b}$ es principal.*

Demostración. Dado que R es un anillo de valuación discreto, existe una valuación discreta $\nu : Fr(R)^* \longrightarrow \mathbb{Z}$, tal que:

$$R = \{x \in Fr(R)^* \ : \ \nu(x) \geq 0\}$$

Afirmamos que $\mathfrak{b} = \{x \in Fr(R)^* \ : \ \nu(x) \geq 1\} \equiv H$.
En efecto, sea $x \in \mathfrak{b}$ y supongamos además que $x \notin H$, entonces $\nu(x) < 1$, es decir, $\nu(x) = 0$. Ahora, notemos que:

$$\nu(1) = \nu(x \cdot x^{-1}) = \nu(x) + \nu(x^{-1}) = \nu(x^{-1})$$

De manera que $\nu(x^{-1}) = \nu(1) \geq 0$ (pues $1 \in R$). Lo anterior nos dice que $x^{-1} \in R$ y por consiguiente x es una unidad en R, de esta manera $1 = (x \cdot x^{-1}) \in \mathfrak{b}$, lo cual es absurdo pues $\mathfrak{b} \subsetneq R$.
Ahora, gracias a las propiedades que satisfacen las valuaciones, fácilmente puede verse que H es un ideal de R, de manera que $\mathfrak{b} \subseteq H$, pero $\mathfrak{b}$ es ideal maximal, luego necesariamente $\mathfrak{b} = H$.
De esta manera hemos caracterizado el ideal asociado a un anillo de valuación discreto. Mostremos que dicho ideal es en efecto principal. Sea $t \in R$ tal que $\nu(t) = 1$. Claramente $\langle t \rangle \subseteq \mathfrak{b}$ pues si $y \in R$ entonces $\nu(ty) = \nu(t) + \nu(y) = 1 + \nu(y) \geq 0$.
Consideremos $x \in \mathfrak{b}$, entonces $\nu(x) = k \geq 1$ para algún $k \in \mathbb{Z}$ y además $\nu(\frac{x}{t}) = k - 1 \geq 1 - 1 = 0$. De esta manera $\frac{x}{t} \in R$ y por tanto $x = t\left(\frac{x}{t}\right) \in \langle t \rangle$. □

Las siguientes son propiedades que satisfacen los anillos de valuación discretos, sus pruebas no requieren herramientas sofisticadas y por tanto dejamos la fuente en la cual pueden verse [6, pág 8].

Propiedades (DVR)**.** *Sea R un anillo de valuación discreto. Como vimos antes R es local, denotemos por $\mathfrak{b}$ su único ideal maximal, el cual, por el Lema B.6, es principal. Sea t un generador para $\mathfrak{b}$, entonces*

(i) R es Noetheriano.

(ii) Todo elemento no nulo de R posee la forma ut^k para algún entero no negativo k y alguna unidad u en R.

(iii) Todo ideal no trivial de R posee la forma $\langle t^k \rangle$ para algún k.

(iv) R posee solo un ideal primo no trivial.

(v) R es integralmente cerrado.

A continuación presentaremos algunos resultados importantes que combinan los conceptos de *Dominios de Dedekind* e *Ideales Fraccionarios*. Para una lectura detallada de esta parte recomendamos visitar [9].

Definición B.7. *Sea R un anillo y sea $K = Fr(R)$. Un **ideal fraccionario** de R en K es un R-módulo $\mathfrak{a}$ contenido en K y es tal que existe un elemento $c \neq 0$ en R para el cual $c\mathfrak{a} \subseteq R$. Si R es Noetheriano se sigue que $c\mathfrak{a}$ y por tanto $\mathfrak{a}$ son finitamente generados.*

Teorema B.8. *[9, págs 18-20]. Sea R un anillo Noetheriano, integralmente cerrado y tal que todo ideal primo no trivial es maximal. Entonces todo ideal de R se puede expresar de manera única como un producto (factorizar) de ideales primos y los ideales fraccionarios no nulos forman un grupo bajo la multiplicación.*

Definición B.9. *Un anillo R que satisface las propiedades del Teorema B.8 es llamado un* ***Dominio de Dedekind****.*

Observación. *Sea R un Dominio de Dedekind y sea $\mathfrak{a}$ un ideal fraccionario. Tenemos una factorización para $\mathfrak{a}$ de la forma:*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}}$$

Donde todos, excepto un numero finito de enteros $r_{\mathfrak{p}}$, son cero. Diremos que $r_{\mathfrak{p}}$ es el orden de $\mathfrak{a}$ en $\mathfrak{p}$. Si $r_{\mathfrak{p}} > 0$ diremos que $\mathfrak{a}$ posee un ***cero*** *en $\mathfrak{p}$, de lo contrario si $r_{\mathfrak{p}} < 0$, diremos que $\mathfrak{a}$ tiene un* ***polo*** *en $\mathfrak{p}$.*
Ahora, sea x un elemento no nulo del campo de fracciones de R, $A = Fr(R)$. Entonces podemos formar un ideal fraccionario dado por $\langle x \rangle = Ax$ y es posible aplicar todas las nociones anteriores de orden, cero y polo a x.

Finalizaremos esta sección con un par de resultados que satisfacen los Dominios de Dedekind, sus pruebas no ofrecen mayor dificultad y las dejamos como lectura personal.

Proposición B.10. *[9, pág 21]. Sea $\mathfrak{A}$ un Dominio de Dedekind con sólo un numero finito de ideales primos no triviales. Entonces $\mathfrak{A}$ es un dominio de ideales principales.*

Proposición B.11. *[9, pág 21]. Sea A un Dominio de Dedekind y sea S un subconjunto multiplicativo de A. Entonces $S^{-1}A$ (la localización de A en S) es un Dominio de Dedekind. Además el mapeo:*

$$\varphi(\mathfrak{a}) \mapsto S^{-1}\mathfrak{a}$$

es un homomorfismo sobreyectivo del grupo de ideales fraccionarios de A en el grupo de ideales fraccionarios de $S^{-1}A$.

Bibliografía

[1] Atiyah, M.: *Introduction To Commutative Algebra*. Westview Press, 1994 (Addison-Wesley series in mathematics). – ISBN 9780813345444

[2] Dummit, D.S. ; Foote, R.M.: *Abstract Algebra*. Wiley, 2004. – ISBN 9780471452348

[3] Eisenbud, D.: *Commutative Algebra: With a View Toward Algebraic Geometry*. Springer, 1995 (Graduate Texts in Mathematics). – ISBN 9780387942698

[4] Fulton, W.: *Algebraic Curves ; An introduction to Algebraic Geometry*. W. A. Benjamin; 1st edition, 1969. – ISBN 978–0805330823

[5] Gray, Jeremy J.: The Riemann-Roch Theorem and Geometry, 1854-1914. En: *Proceedings of the International Congress of Mathematicians* Vol. 3, 1998, p. 811–822

[6] Janusz, G.: *Algebraic Number Fields*. American Mathematical Soc., 1995. – ISBN 9780821872437

[7] Kunz, E.: *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 2012 (Modern Birkhäuser Classics). – ISBN 9781461459873

[8] Kunz, E. ; Belshoff, R.G.: *Introduction to Plane Algebraic Curves*. Birkhäuser Boston, 2007. – ISBN 9780817644437

[9] Lang, S.: *Algebraic Number Theory*. Springer New York, 2013 (Graduate Texts in Mathematics). – ISBN 9781461208532

[10] Morandi, P.: *Field and Galois Theory*. Springer, 1996 (Graduate Texts in Mathematics). – ISBN 9780387947532

[11] Shafarevich, I.R. ; Reid, M.: *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer, 2013 (SpringerLink : Bücher v. 1). – ISBN 9783642379567

[12] Stankewicz, J.: The Riemann-Roch Theorem. (2007)

Lista de Símbolos

(x_P) Elemento del anillo adele, pág 42

$\Gamma(V)$ Anillo de coordenadas de una variedad V, pág 8

$\mathbb{A}^n(k)$ Espacio afín n-dimensional, pág 3

$\mathbb{A}_K$ Anillo adele sobre el campo K, pág 42

$\mathbb{P}^n k$ Espacio proyectivo n-dimensional sobre el campo k, pág 18

$\mathcal{F}(V,k)$ Conjunto de todas las funciones de la variedad V en el campo k, pág 8

$\mathcal{O}_p(V)$ Anillo local de V en el punto p, pág 12

D_K Grupo de divisores de un campo de funciones K, pág 37

$l(D)$ Dimensión del espacio vectorial $L(D)$, pág 40

$\Omega_K(D)$ Espacio de diferenciales de Weil que se anulan sobre $A_K(D)$, pág 52

Ω_K Espacio de diferenciales de Weil, pág 52

$A_K(D)$ Espacio adele asociado a un divisor D, pág 43

$deg(D)$ Grado de un divisor, pág 38

$div(f)$ Divisor asociado a $f \in K$, pág 38

$div_0 f$ Divisor de ceros de $f \in K$, pág 38

$div_{\infty(f)}$ Divisor de polos de $f \in K$, pág 38

$I(X)$ Ideal de un conjunto de puntos, pág 4

$I_{\mathbb{P}}(Y)$ Ideal de un conjunto de puntos en el espacio proyectivo, pág 19

$k(V)$ Campo de funciones racionales de la variedad V, pág 12

$k[x_1, ..., x_n]$ Anillo de polinomios en n-variables sobre el campo k, pág 3

$L(D)$ Espacio vectorial asociado al divisor D, pág 40

$m_p(F)$ Multiplicidad de la curva F en p, pág 15

$ord_P(f)$ Evaluación del sitio P en f, pág 35

$Rad(I)$ Radical de un ideal I, pág 4

$supp(D)$ Soporte de un divisor, pág 38

$V(S)$ Conjunto de ceros, pág 3

$V_{\mathbb{P}}(S)$ Conjunto proyectivo de ceros de S, pág 18