UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

LA RACIONALIDAD Y ECUACIÓN FUNCIONAL DE LA FUNCIÓN Z EN GEOMETRÍA ARITMÉTICA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

ANTONIO DE JESÚS CAMPOS RODRÍGUEZ

DIRECTOR DE TESIS:
DR. ISRAEL MORENO MEJÍA
2012

Hoja de Datos del Jurado

1. Datos del alumno

Campos

Rodríguez

Antonio de Jesús

58 72 52 07

Universidad Nacional Autónoma de México

Facultad de Ciencias

Matemáticas

305012496

2. Datos del tutor

Dr

Israel

Moreno

Mejía

3. Datos del sinodal 1

Dr

Rolando

Jiménez

Benitez

4. Datos del sinodal 2

Dra

Adriana

Ortiz

Rodríguez

5. Datos del sinodal 3

Dr

Adrián

Cerda

Rodríguez

6. Datos del sinodal 4

Dr

Mustapha

Lahyane

7. Datos del trabajo escrito

LA RACIONALIDAD Y ECUACIÓN FUNCIONAL DE LA FUNCIÓN Z EN GEOMETRÍA ARITMÉTICA

146 p

2012

DEDICATORIA

A mi mamá Silvia Rodríguez Martínez.

AGRADECIMIENTOS

A mi familia. En particular a mis hermanos Jesús Campos Rodríguez y Silvia Campos Rodríguez que siempre me han apoyado en todo momento.

En especial a mi mamá Silvia Rodríguez Martínez quien ha sido mi fortaleza durante toda mi vida y a quien más quiero y quien siempre nos cuidó a mí y a mis hermanos. Este trabajo va dedicado para ti ma. Te quiero con toda mi alma.

A mi amiga Anita que nunca me ha dejado solo. Te amo.

A mis mascotas Oso, Micky, Tommy, Capulín, Duquesa, Tobi y mi gato Bedul, y también a mi gato Tino que ya no está conmigo pero que siempre dormía en las tardes sobre mis hojas mientras escribía este trabajo.

A mi asesor Israel Moreno Mejía que me brindó su apoyo cuando lo necesitaba. A mis sinodales que también me han apoyado.

Introducción

Sea $X_{\mathbb{F}_q}$ una variedad algebraica definida sobre un campo finito $\mathbb{F}_q$ con q elementos. Sea $X(\mathbb{F}_{q^r})$ el conjunto de puntos racionales de $X_{\mathbb{F}_q}$ en el campo $\mathbb{F}_{q^r}$, donde $\mathbb{F}_{q^r}$ es la única extensión de Galois de $\mathbb{F}_q$ de grado r. La función zeta de $X_{\mathbb{F}_q}$ se define como

$$\mathbf{Z}(X_{\mathbb{F}_q}, T) := \exp(\sum_{n=1}^{\infty} N_r T^r / r)$$

donde N_r es la cardinalidad de $X(\mathbb{F}_{q^r})$.

André Weil formuló una serie de conjeturas famosas acerca de la función $\mathbf{Z}$ de una variedad $X_{\mathbb{F}_q}$ en las que afirmaba, entre otras cosas, que la función $\mathbf{Z}$ debería ser una función racional y que debería satisfacer cierta ecuación funcional. La prueba de las conjeturas de Weil fue el trabajo de varios matemáticos, entre ellos Grothendieck y su cohomología l-ádica cuyas propiedades implicaban parte de las conjeturas de Weil (la racionalidad y la ecuación funcional), Dwork que probó la racionalidad (ver [5]) y Deligne quien probó el resto de las conjeturas (ver [4]).

El objetivo principal de la presente tesis será exponer una prueba de la racionalidad y la ecuación funcional de la función zeta cuando X_k es una curva completa no singular definida sobre un campo finito $k = \mathbb{F}_q$. Para nuestro propósito, consideraremos a X_k como una curva abstracta en lugar de considerar una curva geométrica, esto es, identificamos X_k con el conjunto de valoraciones suprayectivas $v : k(X)^* \to \mathbb{Z}$ (ver definición 2.2.2) que se anulan en k^*, donde $k(X)$ es el campo de funciones de X_k. Siempre que hablemos de campos de funciones se sobrentenderá que es un campo de grado de trascendencia 1 sobre el campo de definición de la curva (ver definición 2.3.2) ya que en este trabajo consideraremos solamente el caso de curvas (ver definición 2.3.3).

Con esta representación de X_k, el conjunto de puntos racionales de X_k en una extensión k'/k corresponde al conjunto $X(k')$ descrito a continuación:

Sea $\overline{k}/k$ la cerradura algebraica de k. Mediante un cambio de base (ver sección 2.4 del capítulo 2) se puede construir una curva $X_{\overline{k}}$ sobre $\overline{k}$ cuyo campo de funciones está generado por el de X_k y $\overline{k}$. Luego, hay una acción natural de $\mathrm{Gal}(\overline{k}/k)$ en $X_{\overline{k}}$ (ver sección 2.6 del capítulo 3). Sea $\overline{P} \in X_{\overline{k}}$ y sea $\mathrm{Stab}(\overline{P}) \leq \mathrm{Gal}(\overline{k}/k)$ el estabilizador de $\overline{P}$. Sea $\overline{k}^{\mathrm{Stab}(\overline{P})}$ el campo fijo de $\mathrm{Stab}(\overline{P})$. Entonces, dada una extensión k'/k contenida en $\overline{k}/k$, el conjunto de puntos k'-racionales de X es el conjunto $X(k') := \{P \in X_{\overline{k}} \mid \overline{k}^{\mathrm{Stab}(P)} \subseteq k'\}$.

Veremos a la función zeta de la curva completa no singular X_k/k como

$$Z(T) := \prod_{P \in X} (1 - T^{\deg(P)})^{-1}$$

donde $\deg(P)$ es el grado de la extensión $\mathcal{O}_P/\mathcal{M}_P$ sobre k (donde $\mathcal{O}_P$ es el anillo local correspondiente a la valoración del punto $P \in X_k$ y $\mathcal{M}_P$ es su ideal maximal).

En este trabajo se probará que la función $Z(T)$ de la curva completa no singular X/k de género g (con $k = \mathbb{F}_q$) es de la forma

$$Z(T) = \frac{f(T)}{(1-qT)(1-T)}$$

donde $f(T) \in \mathbb{Z}[T]$ es de grado igual a $2g$, y además, que cumple la siguiente ecuación funcional:

$$Z(1/qT) = (qT^2)^{1-g} Z(T)$$

Para probar estos dos resultados, nos basamos fundamentalmente en el libro *An Invitation To Arithmetic Geometry* de Dino Lorenzini. En la primer capítulo de la presente tesis se hace una compilación de los resultados más importantes de álgebra conmutativa y teoría algebraica de números que se usarán después pero sin demostrarlos. Por ejemplo, se menciona el siguiente resultado de álgebra conmutativa:

Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita y separable. Sea B la cerradura entera de A en L. Entonces B es dominio de Dedekind.

Para las demostraciones, remitimos al lector a las fuentes correspondientes en la bibliografía. Además, en este mismo capítulo se hace mención de varios resultados y definiciones que no se utilizarán después, pero que están relacionados con las demostraciones y enunciados de los resultados que sí se utilizarán más adelante, y es por esta razón que también se incluyen.

En el segundo capítulo, desarrollaremos con más detalles algunos resultados referentes a anillos con cocientes finitos, valoraciones, curvas completas no singulares, campos de funciones, morfismos entre curvas completas no singulares y grupos de clases de divisores, los cuales son indispensables durante el capítulo 3. En esta parte se demuestran los resultados que se vayan mencionando (utilizando algunas de las cosas vistas en el capítulo 1), y en algunos casos donde las demostraciones sean extensas o requieran herramientas fuera del objetivo principal de la tesis entonces se dará un esbozo lo más completo posible de la demostración en cuestión.

En el tercer capítulo se procede a probar la racionalidad y la ecuación funcional de la función zeta de nuestras curvas utilizando herramientas correspondientes a los capítulos 1 y 2 (principalmente del 2 y algunas pocas cosas del capítulo 1) así como del teorema de Riemann-Roch que se desarrolla en el capítulo 4.

En el cuarto capítulo se procede a probar el teorema de Riemann-Roch así como algunos lemas y corolarios que se utilizan en el capítulo 3 y que son la clave para las pruebas de la racionalidad y la ecuación funcional en el capítulo 3.

Finalmente, en el último capítulo se hace una breve colección de resultados (sin su demostración correspondiente en algunos casos) que resultan útiles durante todo el proceso del trabajo o que remarcan algunos detalles del mismo y que no se presentaron en los capítulo previos. Por ejemplo, se menciona en este

capítulo 5 sin probar el siguiente resultado que se utiliza en varias partes de la presente tesis:

Sea k un campo perfecto. Sea $L/k(x)$ una extensión finita y no separable (con $x \in L$), donde $k(x)$ es isomorfo como k-álgebra al campo de funciones racionales. Entonces existe $y \in L$ tal que $k(y)$ es isomorfo como k-álgebra al campo de funciones racionales, y además, tal que $L = k(x)(y)$ y $L/k(y)$ es extensión finita y separable.

Finalmente, se concluye el trabajo con la bibliografía utilizada.

Índice

1. Capítulo I - Preliminares

En este capítulo haremos un repaso de algunos resultados de álgebra conmutativa y teoría algebraica de números que usaremos a lo largo de los capítulos 2 y 3, así como en algunos fragmentos del capítulo 4. Se enunciarán los resultados sin demostrarlos, y se hacen algunas observaciones también. Las demostraciones se pueden encontrar en las referencias mencionadas. También se hace mención durante este capítulo de algunas otras definiciones y algunos resultados que no se vuelven a utilizar en los siguientes capítulos, pero que se usan en las pruebas de los resultados que sí se utilizan en capítulos posteriores.

1.1. Series de potencias

Las definiciones, resultados y sus demostraciones de esta sección se pueden encontrar en [11].

Sea F cualquier campo. Sea

$$F[[T]] := \{\sum_{n=0}^{\infty} a_n T^n \mid a_n \in F, \forall\, n \in \mathbb{N}\}$$

El anillo $F[[T]]$ es un dominio de ideales principales local con ideal maximal M generado por T (para verlo, notamos que cada serie de potencias de la forma $f(T) = a_0 + T(\sum_{n=1}^{\infty} a_n T^{n-1})$, con $a_0 \neq 0$, es invertible). Sea $\varphi : F[[T]] \to F[[T]]/M \cong F$ la función natural. Sea $U := \varphi^{-1}(F^*)$ el grupo de unidades en $F[[T]]$, y sea $U_1 := \varphi^{-1}(1)$ (llamado el subgrupo de las unidades principales). El campo de fracciones $F((T))$ de $F[[T]]$ es la campo de las series de Laurent

$$F((T)) := \{\sum_{n \geq n_0} a_n T^n \mid \forall\, n \in \mathbb{Z}, n \geq n_0\}$$

Como $F[T] \subseteq F[[T]]$, podemos considerar el campo de funciones racionales $F(T)$ como un subcampo de $F((T))$, es decir, la siguiente función es inyectiva

$$F(T) \to F((T))$$

$$f(T) \mapsto \text{la serie de Taylor asociada a } f(T) \text{ en } T = 0$$

Por ejemplo, $(1-T)^{-1} = 1 + T + T^2 + \ldots$.

Sea $\{f_i = \sum_{j=0}^{\infty} a_{ji} T^j\}_{i \in \mathbb{N}}$ una sucesión infinita de series de potencias. Decimos que esta sucesión admite sumas si, $\forall\, r \geq 0$, existe un entero $N = N(r)$ tal que $\forall\, n \geq N$, $a_{0n} = a_{1n} = \cdots = a_{rn} = 0$ (es decir, $\forall\, n \geq N$, $f_n = T^r g_n$ para algún $g_n \in F[[T]]$). Si $\{f_i\}_{i \in \mathbb{N}}$ admite sumas, decimos que $\sum f_i$ es una suma admisible, y podemos escribir $\sum_{i=1}^{\infty} f_i = \sum s_j T^j$, donde, $\forall\, j \geq 0$, $s_j = a_{j0} + a_{j1} + \cdots + a_{jN(j)}$.

Sea $\{g_i\}_{i \in \mathbb{N}}$ una sucesión de elementos en M. Si la sucesión $\{g_i\}_{i \in \mathbb{N}}$ admite sumas entonces decimos que la sucesión $\{1 + g_i\}_{i \in \mathbb{N}}$ admite multiplicaciones.

Si $\{1+g_i\}_{i\in\mathbb{N}}$ admite multiplicaciones entonces decimos que $\prod(1+g_i)$ es un producto admisible, y escribimos

$$\prod_{i=1}^{\infty}(1+g_i) = 1+\sum_{j=1}^{\infty}u_jT^j$$

donde u_j es el coeficiente de T^j en cualquier producto finito $\prod_{i=1}^{n}(1+g_i)$ con n suficientemente grande. Por ejemplo, dada una sucesión positiva de enteros $\{b_d\}_{d=1}^{\infty}$, el producto $\prod_{d\in\mathbb{N}}(1-T^d)^{-b_d}$ es un producto admisible.

Supongamos ahora que $\mathrm{char}(F)=0$, por lo que F contiene a un subcampo isomorfo a $\mathbb{Q}$. Denotamos por n al elemento $1+1+\cdots+1$ (n veces) de F, y denotamos por $1/n$ a su inverso. Se define la función logaritmo como

$$\log : U_1 \to M$$

$$\alpha \mapsto \log(\alpha) := \sum_{n=1}^{\infty}(-1)^{n+1}\frac{(\alpha-1)^n}{n}$$

y se define la función exponencial como

$$\exp : M \to U_1$$

$$\beta \mapsto \exp(\beta) := \sum_{n=0}^{\infty}\frac{\beta^n}{n!}$$

Se puede verificar que, $\forall\ \alpha\in U_1$, $\forall\ \beta\in M$,

- (i) $\exp(\log(\alpha)) = \alpha$
- (ii) $\log(\exp(\beta)) = \beta$

Se puede también verificar que, $\forall\ \alpha_1,\alpha_2\in U_1$, $\forall\ \beta_1,\beta_2\in M$,

- (iii) $\log(\alpha_1\alpha_2) = \log(\alpha_1)+\log(\alpha_2)$
- (iv) $\exp(\beta_1+\beta_2) = \exp(\beta_1)\exp(\beta_2)$

Más aún, si $\{1+\gamma_i\}_{i\in\mathbb{N}}$ es un producto admisible entonces se puede verificar que

$$\log(\prod_{i=1}^{\infty}(1+\gamma_i)) = \sum_{i=1}^{\infty}\log(1+\gamma_i)$$

1.2. Elementos enteros

Enunciamos a continuación algunos resultados con respecto a elementos enteros. Las demostraciones de los resultados y las observaciones de esta sección pueden encontrarse en [8] (capítulo 1, sección 2), en [9] (capítulo 1, sección 2) y en [1] (capítulo 5).

Tenemos el siguiente lema.

Lema 1.2.1. *Sea L/K una extensión de Galois con grupo de Galois L/K. Sea $R \subseteq L$ un subanillo tal que $\tau(R) = R$ para todo $\tau \in \mathrm{Gal}(L/K)$. Entonces el polinomio mínimo (sobre K) de cualquier elemento de R tiene coeficientes en $R \cap K$.*

Definimos ahora el concepto de elemento entero sobre un anillo.

Definición 1.2.2. *Sea A un subanillo del anillo L. Un elemento α de L es entero sobre A si es la raíz de un polinomio mónico $f(y) \in A[y]$. Cuando $A = \mathbb{Z}$, decimos que α es un entero algebraico en L.*

Definición 1.2.3. *Sea A un subanillo de un anillo C. El anillo C es entero sobre A, o una extensión entera de A, si cada elemento de C es entero sobre A.*

Observación 1.2.4. *Sea L/K una extensión de Galois con grupo de Galois $\mathrm{Gal}(L/k)$. Sea $R \subseteq L$ un subanillo tal que $\tau(R) = R$ para todo $\tau \in \mathrm{Gal}(L/K)$. Del lema 1.2.1 se obtiene que cada elemento $\alpha \in R$ es entero sobre $R \cap K$, o equivalentemente, que R es una extensión entera de $R \cap K$.*

Observación 1.2.5. *Sea K el campo de fracciones del anillo A. Sea L/K una extensión finita. Sea $\alpha \in L$. Notamos que si el polinomio mínimo $g(y)$ de α sobre K pertenece a $A[y]$ entonces α es entero sobre A. Supongamos ahora que α es entero sobre A. Sea $f(y) \in A[y]$ el polinomio mónico tal que $f(\alpha) = 0$. Se obtiene que el polinomio $g(y)$ divide a $f(y)$ en $K[y]$. Por el corolario 1.26.4 se tiene que cuando el anillo A es factorial, el polinomio $g(y)$ deben entonces pertenecer a $A[y]$. En particular, cuando A es factorial, α es entero sobre A si y sólo si su polinomio mínimo $g(y)$ pertenece a $A[y]$*

Ejemplo 1.2.6. *Sea K el campo de fracciones de un dominio A. Sea $\alpha \in K$. El polinomio mínimo de α sobre K es el polinomio lineal $y - \alpha$. Por la observación 1.2.5, si A es factorial entonces α es entero sobre A si y sólo si $y - \alpha \in A[y]$, es decir, si y sólo si $\alpha \in A$. En particular, los elementos de $\mathbb{Z}$ son los únicos enteros algebraicos en $\mathbb{Q}$.*

La siguiente proposición nos dice algunas equivalencias de que un elemento sea entero sobre un anillo.

Proposición 1.2.7. *Sea A un subanillo de un campo L. Sea $\alpha \in L$. Entonces son equivalentes:*

- *(i) El elemento α es entero sobre A.*
- *(ii) El subanillo $A[\alpha]$ de L, generado por A y α, es un A-módulo finitamente generado.*
- *(iii) Existe un A-submódulo finitamente generado M de L tal que $\alpha M \subseteq M$, con $\alpha M = \{\alpha m | m \in M\}$*

Se puede probar con la proposición 1.2.7 el siguente corolario:

Corolario 1.2.8. *Sea A un subanillo de un campo L. El conjunto B que consiste de todos los elementos de L que son enteros sobre A es un anillo.*

Del corolario anterior tenemos las siguientes definiciones:

Definición 1.2.9. *Sea A un subanillo de un campo L. La cerradura entera B de A en L es el anillo de elementos de L enteros sobre A. Cuando L es un campo de números (i.e., cuando $L/\mathbb{Q}$ es una extensión finita), la cerradura entera B de $\mathbb{Z}$ en L se le llama anillo de enteros de L, y se le denota por $\mathcal{O}_L$.*

Definición 1.2.10. *Un dominio A es enteramente cerrado si es igual a su cerradura entera en su campo de fracciones.*

Ejemplo 1.2.11. *Los anillos $\mathbb{Z}$ y $k[x]$ son enteramente cerrados. En general, cualquier dominio factorial es enteramente cerrado, lo cual se puede probar utilizando la observación 1.2.5 y el ejemplo 1.2.6 mencionado después.*

Enunciamos dos lemas a continuación.

Lema 1.2.12. *Un dominio factorial A es enteramente cerrado.*

Lema 1.2.13. *Sea A un dominio enteramente cerrado en su campo de fracciones K. Sea α un elemento algebraico sobre K, con polinomio mínimo $g(y) \in K[y]$. El elemento α es entero sobre A si y sólo si su polinomio mínimo tiene coeficientes en A.*

En la demostración de la siguiente proposición (ver [9], sección 2 del capítulo 1) se usa la proposición 1.2.7.

Proposición 1.2.14. *Sean A, B y C tres dominios tales que $A \subseteq B \subseteq C$. Entonces C es entero sobre A si y sólo si C es entero sobre B y B es entero sobre A.*

Usaremos con cierta frecuencia en este trabajo la siguiente proposición.

Proposición 1.2.15. *Sea A un dominio con K su campo de fracciones. Sea L/K una extensión finita, y B la cerradura entera de A en L.*

- *(i) Supongamos que $\alpha \in L$. Entonces existen $b \in B$ y $a \in A$ tal $\alpha = b/a$. En particular, L es el campo de fracciones de B.*
- *(ii) B es enteramente cerrado.*
- *(iii) Si A es enteramente cerrado entonces $B \cap K = A$.*
- *(iv) Si L/K es Galois con grupo de Galois G entonces $\tau(B) = B$ para todo $\tau \in G$. Más aún, si A es enteramente cerrado entonces $A = B^G := \{b \in B \mid \tau(b) = b,\ \forall\ \tau \in G\}$*

Corolario 1.2.16. *Sea A un dominio con K su campo de fracciones. Sea L/K una extensión finita de grado n y B la cerradura entera de A en L. Entonces B contiene a una base $\{e_1, \ldots, e_n\}$ del K-espacio vectorial L.*

Observación 1.2.17. *Dada una tripleta (A, K, L), donde A es un dominio con campo de fracciones K y L/K es una extensión finita, podemos asociarle de manera canónica un anillos B tal que:*

- *(1) L es el campo de fracciones de B.*

  Si A es enteramente cerrado entonces
- *(2) $B \cap K = A$*

  Si L/K es Galois entonces
- *(3) $\tau(B) = B$ para todo $\tau \in \mathrm{Gal}(L/K)$.*

1.3. Productos de ideales

Las demostraciones de los resultados de esta sección así como las observaciones se pueden encontrar en [9] (capítulo 1, sección 3).

Definición 1.3.1. *Sean I y J dos ideales de un anillo A. El producto de I y J, denotado por IJ, o I^2 si $I = J$, es el ideal de A generado por los elementos de la forma xy con $x \in I$ y $y \in J$. Definimos $I^0 := A$, y definimos de manera inductiva al ideal I^a como $I^{a-1} \cdot I$.*

Dado un elemento $\alpha \in IJ$, existe $n \in \mathbb{N}$ y $x_1, \ldots, x_n \in I$ y $y_1, \ldots, y_n \in J$, tales que $\alpha = x_1y_1 + \cdots + x_ny_n$. Notamos también que, en general, $IJ \subseteq I \cap J$.

Definición 1.3.2. *Sean I y J dos ideales de un anillo A. La suma de los ideales I y J, denotada por $I+J$, es el ideal de A generado por los elementos de I y J juntos.*

Notamos que si $a_1, \ldots, a_n \in A$, y si denotamos al ideal generado en A por estos elementos como $(a_1, \ldots, a_n)$ entonces $(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1}) + (a_n)$. Si I es cualquier ideal de A entonces el ideal generado por los elementos de I y $a_1, \ldots, a_n$ se denota por $(I, a_1, \ldots, a_n)$. Notamos que $(I, a_1, \ldots, a_n) = I + (a_1, \ldots, a_n)$

Definición 1.3.3. *Dos ideales son primos relativos si $I + J = A$.*

Notamos que si I, J son primos relativos entonces existen $x \in I$, $y \in J$ tales que $x + y = 1$.

Tenemos el siguiente lema:

Lema 1.3.4. *Si I, J son coprimos entonces $IJ = I \cap J$*

Y tenemos la siguiente observación.

Observación 1.3.5. *Sean P, Q dos ideales primos en un anillo A. Si P es maximal y $Q \subsetneq P$ entonces P y Q son primos relativos, pues el ideal $P + Q$ contiene estrictamente al ideal maximal P, por lo que $P + Q = A$.*

Consideramos ahora la siguiente definición:

Definición 1.3.6. *Un dominio entero R tiene la propiedad de factorización única de ideales si todo ideal no trivial $I \subseteq R$ puede ser escrito como $I = \mathcal{B}_1 \cdots \mathcal{B}_s$, donde $\mathcal{B}_i$, $i = 1, \ldots, s$ es un ideal primo de R, y si además $I = \mathcal{C}_1 \cdots \mathcal{C}_r$ entonces $r = s$ y $\mathcal{B}_i = \mathcal{C}_j$ para alguna permutación $i \mapsto j$ de $\{1, \ldots, r\}$*

Cualquier dominio de ideales principales tiene la propiedad única de factorización de ideales. Mencionamos por último un teorema para saber cuándo una cerradura entera de un anillo en una extensión de campos tiene la propiedad de factorización única de ideales.

Teorema 1.3.7. *Sea L/K una extensión separable. Sea $A \subseteq K$ un dominio de ideales principales. Entonces la cerradura entera B de A en L tiene la propiedad de factorización única de ideales.*

1.4. Anillos noetherianos

Las demostraciones de los resultados de esta sección así como las observaciones pueden encontrarse en [9] (capítulo 1, sección 4) y en [1] (capítulo 7).

Un ideal de un anillo A es finitamente generado si existe un número finito de elementos $c_1, \ldots, c_r$ en I tales que $I = \{a_1c_1 + \cdots + a_rc_r \mid a_i \in A, i = 1, \ldots, r\}$. Revisaremos más adelante el siguiente resultado: *Sea A un dominio de ideales principales y K su campo de fracciones. Sea L/K una extensión separable. Entonces cualquier ideal de la cerradura entera B de A en L es finitamente generado.*

Definición 1.4.1. *Si cualquier ideal I de un anillo A es finitamente generado entonces llamamos a A un anillo noetheriano.*

Ejemplo 1.4.2.

- *(i) Un campo es un anillo noetheriano.*
- *(ii) Cualquier dominio de ideales principales es noetheriano.*
- *(iii) Sea k un campo. El anillo $R = k[x]/(x^2)$ tiene un único ideal no trivial, generado por la clase de x. Por tanto, es noetheriano.*
- *(iv) Más en general, si A es noetheriano y $I \subseteq A$ es un ideal entonces A/I es noetheriano. Para verlo, tomamos la función natural $f : A \to A/I$. Sea $J \subseteq A/I$ cualquier ideal. Entonces el ideal $f^{-1}(J)$ es finitamente generado en A, por ser A noetheriano. Sean $c_1, \ldots, c_n$ un sistema de generadores para $f^{-1}(J)$. Entonces los elementos $f(c_1), \ldots, f(c_n)$ generan a J en A/I.*

Observación 1.4.3. *Si un anillo R es un grupo abeliano finitamente generado entonces R es noetheriano. Para verlo, sea $I \subseteq R$ cualquier ideal. Podemos considerar a I como un grupo abeliano. Notamos que entonces I es finitamente generado, ya que cualquier subgrupo de un grupo abeliano finitamente generado es también finitamente generado.*

Por ejemplo, si $f(y) \in \mathbb{Z}[y]$ es un polinomio mónico entonces el anillo $R := \mathbb{Z}[y]/(f(y))$ es noetheriano pues es un grupo abeliano libre cuya base consiste de las clases en R de los elementos $1, y, \ldots, y^{\deg(f)-1}$.

Proposición 1.4.4. *Sea A un anillo noetheriano. Entonces cualquier submódulo de un A-módulo finitamente generado también es finitamente generado.*

En particular, notamos que como cualquier grupo abeliano es un $\mathbb{Z}$-módulo y como $\mathbb{Z}$ es noetheriano (pues es dominio de ideales principales), se obtiene entonces que cualquier subgrupo de un grupo abeliano finitamente generado también es finitamente generado, lo cual ya se había mencionado al principio.

Corolario 1.4.5. *Sean $A \subseteq B$ dos anillos. Si A es noetheriano y B es un A-módulo finitamente generado entonces B es noetheriano.*

Tenemos el siguiente teorema.

Teorema 1.4.6. *Sea A un dominio noetheriano y además que sea enteramente cerrado en su campo de fracciones K. Sea L/K una extensión finita y separable. Entonces la cerradura entera B de A en L es un A-módulo finitamente generado. En particular, B es un anillo noetheriano.*

La hipótesis de que L/K sea separable se cumple cuando L sea un campo de números ($K = \mathbb{Q}$), ya que se sabe que cualquier extensión de un campo de característica 0 es separable.

Consideramos la siguiente proposición.

Proposición 1.4.7. *Sea A un dominio enteramente cerrado en su campo de fracciones K. Sea L/K una extensión separable de grado n, y B la cerradura entera de A en L. Tomamos $\{e_1, \ldots, e_n\} \subset B$ una base para L sobre K. Entonces existe un elemento no cero $d \in A$ tal que el A-módulo B está contenido en un A-módulo libre generado por los elementos $e_1/d, \ldots, e_n/d$, es decir, se tiene*

$$Ae_1 \oplus \cdots \oplus Ae_n \subseteq B \subseteq A\frac{e_1}{d} \oplus \cdots \oplus A\frac{e_n}{d} \subseteq L$$

Un elemento m en un A-módulo M es de torsión si existe $a \in A$, $a \neq 0$, tal que $am = 0$. Un A-módulo M es de torsión si todos los elementos de M son de torsión. Sea I un ideal no cero de A. Entonces el A-módulo A/I siempre es de torsión (en particular, $\mathbb{Z}/d\mathbb{Z}$ es un $\mathbb{Z}$-módulo de torsión). Si 0 es el único elemento de torsión en M entonces el módulo M es libre de torsión. Cuando A es dominio de ideales principales, cualquier A-módulo finitamente generado es isomorfo a la suma directa de un módulo de torsión finitamente generado y un A-módulo finitamente generado libre.

Corolario 1.4.8. *Sea K el campo de fracciones de un dominio A. Sea L una extensión finita y separable del campo de fracciones de A. Entonces la cerradura entera B de A en L es un A-módulo finitamente generado libre.*

En la demostración del corolario anterior (que se puede encontrar en la bibliografía mencionada en esta sección), se usa el siguiente lema.

Lema 1.4.9. *Sea K el campo de fracciones de un dominio A. Supongamos que L/K una extensión finita de grado n y B la cerradura entera de A en L. Si B es una A-módulo finitamente generado libre entonces el rango de B sobre A es igual a n.*

Tenemos la definición siguiente.

Definición 1.4.10. *Sea A un subanillo de un campo L y B la cerradura entera de A en L. Cuando B es un A-módulo finitamente generado libre, llamamos a la base $\{b_1, \ldots, b_n\}$ de B sobre A una base entera para B.*

De la demostración del lema 1.4.9 (que se puede consultar en las referencias mencionadas al principio de esta sección), se puede obtener que $\{b_1, \ldots, b_n\}$ es también una base para L sobre K.

Para definir un A-módulo noetheriano consideramos la definición siguiente.

Proposición 1.4.11. *Sea A cualquier anillo conmutativo y M cualquier A-módulo. Entonces son equivalentes:*

- *(i) Cualquier submódulo de M es un A-módulo finitamente generado.*
- *(ii) Cualquier sucesión creciente $M_1 \subseteq M_2 \cdots \subseteq M_n \subseteq \cdots$ de submódulos de M se estaciona en algún momento, es decir, existe n tal que $M_n = M_{n+1} = \ldots$.*
- *(iii) Cualquier subconjunto no vacío del conjunto de submódulos de M tiene un elemento maximal.*

Definición 1.4.12. *Un A-módulo M es llamado noetheriano si se cumple cualquiera de las tres equivalencias de la proposición 1.4.11.*

Un anillo A es noetheriano si y sólo si es un A-módulo noetheriano, pues los submódulos del A-módulo A son justamente los ideales de A.

Definición 1.4.13. *Un conjunto de A-módulos $\{M_i\}_{i\in\mathbb{Z}}$ y un conjunto de homomorfismos de A-módulos $\delta_i : M_i \to M_{i+1}$ es una sucesión si $\mathrm{Im}(\delta_{i-1}) \subset \mathrm{Ker}(\delta_i)$, $\forall\ i \in \mathbb{Z}$. Una sucesión*

$$\cdots \to M_{i-1} \overset{\delta_{i-1}}{\to} M_i \overset{\delta_i}{\to} M_{i+1} \to \ldots$$

de A-módulos y homomorfismos de A-módulos es exacta en M_i si $\mathrm{Im}(\delta_{i-1}) = \mathrm{Ker}(\delta_i)$. La sucesión es exacta si es exacta en cada M_i.

Definición 1.4.14. *Una sucesión exacta corta es una sucesión exacta de la forma*

$$0 \to M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0$$

Equivalentemente, una sucesión como arriba es exacta si f es inyectiva, g es suprayectiva, y $\mathrm{Im}(f)) = \mathrm{Ker}(g)$.

Ejemplo 1.4.15. *Sea M un A-módulo finitamente generado. Podemos representar a este módulo por medio de generadores y relaciones usando una sucesión exacta. Sean $m_1, \ldots, m_a$ un conjunto generador de M, y F el módulo libre $\oplus_{i=1}^{s} Ae_i$ con base $\{e_1, \ldots, e_s\}$. Consideramos la función $g : F \to M$, con $a := a_1e_1 + \cdots + a_se_s \mapsto g(a) := \sum_{i=1}^{s} m_i$. El módulo $N := \mathrm{Ker}(g)$ es el módulo de relaciones para el conjunto de generadores $\{m_1, \ldots, m_s\}$. La sucesión $0 \to N \to F \xrightarrow{g} M \to 0$ es exacta.*

Ejemplo 1.4.16. *Sea I un ideal no trivial de un anillo A. El cociente A/I es un anillo, y además es un A-módulo, con multiplicación escalar dada por $a \cdot m :=$ (clase de a)m en A/I, $\forall a \in A$, $m \in A/I$.*

El A-módulo A/I es finitamente generado, cuyo generador es la clase de $1 \in A$, ya que la función natural $A \to A/I$ que manda el 1 de A a la clase de 1 en A/I es suprayectiva. La siguiente sucesión de A-módulos es exacta:

$$0 \to I \to A \to A/I \to 0$$

Mencionamos un lema y una proposición con respecto a sucesiones exactas y módulos finitamente generados y noetherianos.

Lema 1.4.17. *Sea $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta de A-módulos. Entonces M es un A-módulo finitamente generado si M' y M'' son A-módulos finitamente generados. Más aún, si M es un A-módulo finitamente generado entonces M'' es A-módulo finitamente generado.*

Proposición 1.4.18. *Sea $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta de A-módulos. Entonces M es noetheriano si y sólo si M' y M'' son noetherianos.*

Tenemos el siguiente corolario de la proposición 1.4.18.

Corolario 1.4.19. *Sea $\{M_i\}_{i=1}^{n}$ un conjunto de A-módulos noetherianos. Entonces $M := \oplus_{i=1}^{n} M_i$ es noetheriano.*

1.5. Anillos de dimensión 1

Los resultados, demostraciones y observaciones de esta sección se pueden encontrar en [9] (capítulo 1, sección 5).

Definición 1.5.1. *Sea A un anillo. Una cadena de ideales primos de longitud n en A es un conjunto de $n+1$ ideales primos distintos $P_0, P_1, \ldots, P_n$ de A tales que $P_n \subset P_{n-1} \subset \cdots \subset P_1 \subset P_0$. La altura de un ideal primo P, $\mathrm{ht}(P)$, es el supremo de las longitudes de las cadenas de primos en A con $P_0 = P$. La dimensión de Krull de A se define como*

$$\dim(A) := \sup\{\mathrm{ht}(P) \mid P \text{ es ideal primo de } A\}$$

Ejemplo 1.5.2.

- *(i) Cualquier campo tiene dimensión 0, ya que en un campo el ideal trivial es el único ideal primo.*
- *(ii) Sea k cualquier campo. El anillo $R = k[x]/(x^2)$ no es dominio pues el cuadrado de la clase de x en R es igual a 0 en R. El anillo R tiene dimensión 0 ya que el ideal generado en R por la clase de x es el único ideal primo en R.*
- *(iii) Sea k un campo. El ideal $P := (x_1, \ldots, x_i)$ es un ideal primo en el anillo de polinomios $R = k[x_1, \ldots, x_n]$, ya que $\frac{k[x_1,\ldots,x_n]}{P} \cong k[x_{i+1}, \ldots, x_n]$ es dominio entero. Además, se tiene que $\mathrm{ht}(P) \geq i$ ya que*

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2 \ldots, x_i)$$

  es una cadena de primos de longitud i. El anillo de polinomios $k[x_1, \ldots, x_n]$ tiene dimensión al menos n pues contiene una cadena de longitud n.
- *(iv) El anillo $\mathbb{Z}[x]$ tiene dimensión al menos 2, ya que dado cualquier primo p,$(0) \subset (p) \subset (p, x)$ es una cadena de ideales primos de longitud 2.*

Un dominio entero R tiene dimensión 1 si y sólo si R contiene un ideal primo no cero y cualquier ideal primo no cero de R es maximal.

Tenemos el siguiente lema.

Lema 1.5.3. *Sea R un dominio entero, y sean $P_1 = (p_1)$ y $P_2 = (p_2)$ dos ideales primos principales no triviales distintos de R. Entonces $P_1 \subsetneq P_2$. En particular, un dominio de ideales principales tiene dimensión 1.*

Con el lema 1.5.3 se puede probar el siguiente lema.

Lema 1.5.4. *Sea R un dominio factorial y P un ideal primo no trivial de R. Entonces $\mathrm{ht}(P) = 1$ si y sólo si P es principal.*

Y el lema 1.5.4 se usa para probar la siguiente proposición (ver la bibliografía mencionada al principio de esta sección).

Proposición 1.5.5. *Un dominio factorial noetheriano R de dimensión 1 es un dominio de ideales principales. El recíproco también se cumple.*

Tenemos también la proposición siguiente.

Proposición 1.5.6. *Sea A un dominio de dimensión 1 y sea B un dominio que contiene a A y tal que cada elemento de B es entero sobre A. Entonces B tiene dimensión 1.*

Observación 1.5.7. *Sea A un dominio de dimensión 1 y B un dominio que contiene a A tal que cada elemento de B es entero sobre A. De la proposición 1.5.6 y su demostración (que se puede encontrar en la bibliografía mencionada al principio de esta sección) se puede obtener que, si $\mathcal{B} \subset B$ es un ideal maximal entonces $P := \mathcal{B} \cap A$ es un ideal maximal de A.*

Corolario 1.5.8. *Sea K el campo de fracciones de un dominio A de dimensión 1. Sea L/K una extensión finita. Entonces la cerradura entera B de A en L tiene dimensión 1.*

1.6. Dominios de Dedekind

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo I, sección 6), en [12] (capítulo 5) y en [1] (capítulo 9).

Definición 1.6.1. *Sea R un dominio entero. El anillo R es dominio de Dedekind si cumple las tres siguientes propiedades:*

- *(i) R es noetheriano.*
- *(ii) R tiene dimensión 1.*
- *(iii) R es enteramente cerrado (en su campo de fracciones).*

Del lema 1.2.12, y del lema 1.5.3 y la proposición 1.5.5 se obtiene que cualquier dominio de ideales principales es dominio de Dedekind. Además, aplicando el teorema 1.4.6 y la proposición 1.5.6 obtenemos el siguiente teorema:

Teorema 1.6.2. *Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita y separable. Entonces la cerradura entera B de A en L es un dominio de Dedekind.*

Enunciamos un último teorema para esta sección.

Teorema 1.6.3. *Sea R un dominio noetheriano de dimensión 1. El anillo R es dominio de Dedekind si y sólo si R tiene la propiedad de factorización única de ideales.*

1.7. Curvas planas

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 1 y también en el capítulo X).

Sea k cualquier campo. Sea $\overline{k}$ una cerradura algebraica de k. Sea $k \subseteq F \subset \overline{k}$ cualquier extensión de campos de k. Denotamos por $\mathbb{A}^n(F) := F^n$ al conjunto de puntos del n-espacio afín con coordenadas en F. Decimos que $\mathbb{A}^1 := F$ y $\mathbb{A}^2 := F \times F$ son el conjunto de puntos con coordenadas en F de la línea afín y del plano afín, respectivamente. Sea $f(x, y) \in k[x, y]$ un polinomio en dos variables con coeficientes en k. Escribiendo $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$, sea d el maximo valor en el conjunto $\{i + j \mid a_{ij} \neq 0\}$, y llamamos a d el grado de f. El grado de f en x, denotado por $\deg_x(f)$, es el grado del polinomio f visto como un polinomio en la variable x con coeficientes en $k[y]$. Similarmente, $\deg_y(f)$ es el grado de f visto como un elemento de $k[x][y]$. Consideraremos el conjunto

$$Z_f(F) := \{(a, b) \in F \times F \mid f(a, b) = 0\}$$

es decir, los ceros de f con coordenadas en F.

Definición 1.7.1. *El conjunto $Z_f(\overline{k})$ se le llama una curva plana afín. El conjunto $Z_f(F)$ es el conjunto de puntos con coordenadas en F de la curva plana afín de grado d definida por $f(x, y)$.*

Tenemos el siguiente lema.

Lema 1.7.2. *Sea $f(x, y) \in k[x, y]$ un polinomio de grado $d > 0$. Entonces $Z_f(\overline{k})$ es un conjunto infinito. En particular, $Z_f(\overline{k}) \neq \emptyset$.*

Ejemplo 1.7.3. *Sea p un número primo. Sea $\mathbb{F}_q$ el campo finito $\mathbb{Z}/p\mathbb{Z}$. Sean $r \in \mathbb{N}$ y $q := p^r$. Existe un único campo finito con q elementos (salvo isomorfismo), y lo denotamos por $\mathbb{F}_q$, el cual se obtiene adjuntando a $\mathbb{F}_p$ todas las raíces del polinomio $x^q - x$. Sea $f(x, y) \in \mathbb{F}_q[x, y]$. Decimos que $f(x, y)$ define una curva algebraica sobre un campo finito. Como $\mathbb{F}_q$ es un conjunto finito, se tiene que $Z_f(\mathbb{F}_q) \subset \mathbb{F}_q \times \mathbb{F}_q$ es también finito. Cuando $\mathbb{F}_{q^n}$ es la extensión de grado n sobre $\mathbb{F}_q$ (dicha extensión es única salvo isomorfismo), se usa la notación*

$$N_n := |Z_f(\mathbb{F}_{q^n})|$$

Se puede probar la siguiente afirmación importante, aunque es algo que no se tratará en la presente tesis: Sea $Z_f(\overline{\mathbb{F}_q})$ una curva no singular de género g. Entonces $N_n \leq (q^n + 1) + 2g\sqrt{q^n}$.

1.8. Anillos de funciones

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 2).

Sea k cualquier campo. Dotamos a $\overline{k}$ con la topología de Zariski, es decir, donde un subconjunto no vacío $C \subset \overline{k}$ es cerrado si y sólo si es una unión finita de puntos de $\overline{k}$, o $\overline{k}$. Consideramos las funciones

$$\mathbf{x} : Z_f(\overline{k}) \to \overline{k} \quad \text{y} \quad \mathbf{y} : Z_f(\overline{k}) \to \overline{k}$$

donde

$$(a, b) \mapsto a \quad \text{y} \quad (a, b) \mapsto b$$

Queremos dotar a $Z_f(\overline{k})$ con una topología tal que $\mathbf{x}$ y $\mathbf{y}$ sean continuas cuando $\mathbb{A}^1(\overline{k})$ tiene la topología de Zariski. Si ambas son continuas entonces un punto (a, b) de $Z_f(\overline{k})$ es cerrado, ya que $(a, b) = \mathbf{x}^{-1}(a) \cap \mathbf{y}^{-1}(b)$.

Sea $g(x, y) \in \overline{k}[x, y]$ cualquier polinomio. Definimos la función $\mathbf{g} : Z_f(\overline{k}) \to \overline{k}$ mediante $(a, b) \mapsto \mathbf{g}(a, b) := g(a, b)$. Entonces dotamos a la curva $Z_f(\overline{k})$ con la topología τ más chica sobre $Z_f(\overline{k})$ tal que todas las funciones $\mathbf{g}$, con $g \in \overline{k}[x, y]$, son continuas (donde $\overline{k}$ tiene la topología de Zariski mencionada), es decir, si τ' es una topología sobre $Z_f(\overline{k})$ tal que todas las funciones $\mathbf{g}$ son continuas entonces $\tau \subseteq \tau'$. Similarmente, podemos definir una topología sobre $\overline{k}^n$ como la topología más chica sobre $\overline{k}^n$ tal que todas las funciones $\mathbf{g}$, con $g \in \overline{k}[x_1, \ldots, x_n]$, son continuas. Notamos que la topología de Zariski sobre $\overline{k}^n$ es también la más chica tal que todos los conjuntos de la forma $Z_g(\overline{k})$ son cerrados. En particular, $Z_f(\overline{k})$ es cerrado en $\overline{k}^2$, y la topología de $Z_f(\overline{k})$ es la inducida por la topología de Zariski sobre $\overline{k}^2$. Podemos describir a la topología de Zariski sobre la curva $Z_f(\overline{k})$ de manera explícita como sigue:

Proposición 1.8.1. *Sea $f \in \overline{k}[x, y]$ irreducible. Un subconjunto no vacío $C \in Z_f(\overline{k})$ es cerrado si y sólo si es una unión finita de puntos de $Z_f(\overline{k})$, o $Z_f(\overline{k})$.*

Mencionamos un teorema importante.

Teorema 1.8.2. *Sea $f \in \overline{k}[x, y]$ un polinomio irreducible. Sea $g \in \overline{k}[x, y]$ un polinomio no divisible por $f(x, y)$. Entonces $Z_f(\overline{k}) \cap Z_g(\overline{k})$ es un conjunto finito.*

En la demostración del teorema 1.8.2 (que se puede consultar en la bibliografía mencionada en esta sección) se usan los siguientes resultados y definiciones.

Lema 1.8.3. *Sea A cualquier anillo. Sea $g(x)$ cualquier polinomio en $A[x]$. Sea $a \in A$. Entonces $x - a$ divide a $g(x)$ en $A[x]$ si y sólo si $g(a) = 0$.*

Definición 1.8.4. *Sea A cualquier anillo, y sea $f(y) := a_n y^n + \cdots + a_0$ y $g(y) := b_m y^m + \cdots + b_0$ dos polinomios en $A[y]$, con $a_n b_m \neq 0$. El resultante de f y g se define como el elemento*

$$\mathrm{Res}(f,g) := \det \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & \dots & b_0 & & \\ & \ddots & \ddots & & & \ddots & \\ & & b_m & b_{m-1} & \dots & \dots & b_0 \end{pmatrix}$$

donde el número de filas de la forma $(a_n \quad a_{n-1} \quad \dots \quad a_0)$ es igual a m, y el número de filas de la forma $(b_m \quad b_{m-1} \quad \dots \quad b_0)$ es igual a n. Si $f = 0$, hacemos $\mathrm{Res}(f,g) = 0$.

Lema 1.8.5. *Sea A un dominio factorial. Si $a_n b_m \neq 0$ entonces f y g tienen un factor no constante en común en $A[y]$ si y sólo si* $\mathrm{Res}(f,g) = 0$

Sea $f(x,y) := \sum_{i=1}^{n} a_i(x) y^i$, con $a_n(x) \neq 0$, y $g(x,y) := \sum_{j=0}^{m} b_j(x) y^j$, con $b_m(x) \neq 0$. Consideramos el polinomio

$$\mathrm{Res}(f(x,y), g(x,y)) \in \overline{k}[x]$$

Llamamos a este polinomio el resultante de f y g con respecto a la variable y, y se denota por $\mathrm{Res}_y(f,g)(x)$

Un corolario del teorema 1.8.2 es el siguiente:

Corolario 1.8.6. *Sean f y g dos polinomios primos relativos en $\overline{k}[x,y]$. Entonces $Z_f(\overline{k}) \cap Z_g(\overline{k})$ es un conjunto finito.*

Mencionamos una proposición más.

Proposición 1.8.7. *Sean f y g dos polinomios primos relativos en $\overline{k}[x,y]$. Supongamos que $f(x,y) = y^n + \sum_{i=0}^{n-1} a_i(x) y^i$ es mónico en y. Entonces $a \in \mathbf{x}(Z_f(\overline{k}) \cap Z_g(\overline{k}))$ si y sólo si* $\mathrm{Res}_y(f,g)(a) = 0$.

Observación 1.8.8. *Sean $f(x,y) = \prod_{i=1}^{n}(x - a_i)$ y $g(x,y) = \prod_{j=1}^{m}(y - b_j)$ dos polinomios primos relativos y libres de cuadrados. Entonces $Z_f(\overline{k}) \cap Z_g(\overline{k})$ contiene exactamente $mn = \deg(f)\deg(g)$ puntos distintos. El teorema de Bézout establece, en general, que cuando f y g son cualesquiera polinomios primos relativos entonces $|Z_f(\overline{k}) \cap Z_g(\overline{k})| \leq \deg(f)\deg(g)$.*

El siguiente es otro corolario del teorema 1.8.2.

Corolario 1.8.9. *Sea $f \in \overline{k}[x,y]$. Sean f y g dos polinomios tales que $\mathbf{g} = \mathbf{h}$ como funciones sobre $Z_f(\overline{k})$. Entonces f divide a $g-h$. En particular, g y h definen el mismo elemento en el anillo $C_f := \overline{k}[x,y]/(f)$.*

Dotamos a $Z_f(\overline{k})$ y $\overline{k}$ con la topología de Zariski, y consideramos el conjunto de funciones continuas de $Z_f(\overline{k})$ a $\overline{k}$, $C(Z_f(\overline{k}), \overline{k})$. Del corolario 1.8.9 se obtiene que la función $i_f : C_f \to C(Z_f(\overline{k}), \overline{k})$, con $g + (f) \mapsto \mathbf{g}$, es inyectivo. Llamamos a C_f el anillo de funciones algebraicas sobre $Z_f(\overline{k})$ (o anillo de funciones de $Z_f(\overline{k})$). Si C_f es dominio entonces f es irreducible.

Tenemos la siguiente definición y un lema después.

Definición 1.8.10. *Sea $f \in \overline{k}[x,y]$ un polinomio irreducible, tal que el anillo $C_f := \overline{k}[x,y]/(f)$ es un dominio entero. Denotamos por $\overline{k}(Z_f)$ el campo de fracciones del anillo C_f, y lo llamamos el campo de funciones racionales de la curva afín definida por f, y a sus elementos los llamamos funciones racionales de $Z_f(\overline{k})$.*

Lema 1.8.11. *Dada $\alpha \in \overline{k}(Z_f)^*$, existe un número finito de puntos $P_1, \ldots, P_s$ en $Z_f(\overline{k})$ tal que α define una función continua $\alpha : Z_f(\overline{k}) \setminus \{P_1, \ldots, P_s\} \to \overline{k}$.*

Sea $f(x,y) = a_n(x)y^n + \cdots + a_0(x)$ un polinomio irreducible en $\overline{k}[x,y]$. La función natural

$$\varphi : \overline{k}[x] \to C_f := \overline{k}[x,y]/(f)$$

es inyectiva si $f(x,y) \neq cx + d$, $\forall\ c, d \in \overline{k}$. Cuando la función φ es inyectiva, se puede extender a la función inyectiva dada por

$$\overline{k}(x) \to \overline{k}(Z_f)$$

$$g(x)/h(x) \mapsto \varphi(g(x))/\varphi(h(x))$$

del campo de fracciones $\overline{k}(x)$ de $\overline{k}[x]$ al campo de fracciones $\overline{k}(Z_f)$ de C_f. El campo $\overline{k}(Z_f)$ es isomorfo a $\overline{k}(x)[y]/(f)$ y, por tanto, la extensión $\overline{k}(Z_f)/\overline{k}(x)$ es de grado finito igual a $\deg_y(f)$. Tomamos la tripleta (A, K, L) con $A = \overline{k}[x]$, $K = \overline{k}(x)$, y $L = \overline{k}(Z_f)$. Cuando $a_n(x) = 1$, se tiene que cada elemento de C_f es entero sobre $\overline{k}[x]$, y entonces C_f es extensión entera de $\overline{k}[x]$.

Por la proposición 1.5.6 se obtiene que cuando $a_n(x) = 1$ entonces C_f tiene dimensión 1. Más aún, como C_f está generado sobre $\overline{k}[x]$ por las clases de los elementos $1, y, \ldots, y^{n-1}$ entonces se obtiene del corolario 1.4.5, que C_f es noetheriano. Por tanto, el dominio C_f es enteramente cerrado si y sólo si es un dominio de Dedekind.

1.9. Puntos e ideales maximales

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 3).

Queremos establecer una biyección entre los puntos de la curva $Z_f(\overline{k})$ y el conjunto de ideales maximales $\mathrm{Max}(C_f)$ del anillo $C_f := \overline{k}[x,y]/(f)$ (si A es conmutativo, se denota por $\mathrm{Max}(A)$ al conjunto de ideales maximales de A.)

Definición 1.9.1. *Sea $g \in C_f$. El valor de g en un punto $(a,b) \in Z_f(\overline{k})$ se define como el elemento $g(a,b) \in \overline{k}$, donde $g(x,y) \in \overline{k}[x,y]$ es cualquier polinomio cuya clase en C_f es g.*

Notamos que la definición anterior no depende del $g(x,y)$ elegido. Sea $(a,b) \in \overline{k}(Z_f)$ fijo. Tomamos el conjunto

$$M := \{g \in C_f \mid g(a,b) = 0\}$$

Veamos que el ideal M es igual al ideal N generado por las clases en C_f de $x-a$ y $y-b$. Tenemos que el ideal $(x-a, y-b) \subset \overline{k}[x,y]$ es maximal en $\overline{k}[x,y]$ pues el cociente $\overline{k}[x,y]/(x-a,y-b)$ es isomorfo al campo $\overline{k}$. Por tanto, si $f(x,y) \in (x-a,y-b)$ entonces N es maximal en C_f. Ahora, sea $g \in C_f$, y $g(x,y) \in \overline{k}[x,y]$ un representante de g en C_f. Escribimos

$$g(x,y) = g(a,b) + \frac{\partial g}{\partial x}(a,b)(x-a) + \frac{\partial g}{\partial y}(a,b)(y-b) + \text{ terminos de orden mayor}$$

la expansión de Taylor de $g(x,y)$ en (a,b). Notamos entonces que $g(a,b) = 0$ si y sólo si $g(x,y) \in (x-a,y-b) \subset \overline{k}[x,y]$. Por tanto, el ideal maximal $(x-a,y-b)$ de $\overline{k}[x,y]$ contiene a $f(x,y)$, y por lo tanto, define un ideal maximal de C_f, a saber, M.

Mencionamos dos lemas.

Lema 1.9.2. *Sea $f(x,y) \in k[x,y]$ cualquier polinomio no constante. Entonces el ideal de $k[x,y]$ generado por f no es maximal.*

Lema 1.9.3. *Sea A un dominio factorial con campo de fracciones K. Sea M un ideal maximal de $A[y]$ que no sea principal. Entonces $M \cap A \neq (0)$.*

Los lemas 1.9.2 y 1.9.3 se usan en la demostración de la siguiente proposición (la cual se puede encontrar en [9], capítulo 2, sección 3).

Proposición 1.9.4. *Sea M un ideal maximal de $\overline{k}[x,y]$. Entonces existe un punto $(a,b) \in \mathbb{A}^2(\overline{k})$ tal que M está generado por $(x-a)$ y $(y-b)$.*

Finalmente, mencionamos un corolario de la proposición 1.9.4.

Corolario 1.9.5. *Sea $f \in \overline{k}[x,y]$ un polinomio irreducible. Un ideal M del anillo $C_f := \overline{k}[x,y]/(f)$ es maximal si y sólo si puede ser generado por las clases en C_f de dos elementos de la forma $x-a$ y $y-b$ in $\overline{k}[x,y]$, con $f(a,b)=0$. Sea $I_f(a,b)$ el ideal de C_f generado por las clases en C_f de $x-a$ y $y-b$. La función $I_f : Z_f(\overline{k}) \to \mathrm{Max}(C_f)$ dada por $(a,b) \mapsto I_f(a,b)$ es una biyección.*

1.10. Morfismos de curvas

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 4).

Recordamos que si A es un anillo entonces una A-álgebra es un anillo B junto con un homomorfismo de anillos $\varphi : A \to B$ (decimos también que $\varphi : A \to B$ es una A-álgebra o que B es una A-algebra.). También, si $\varphi : A \to B$ y $\gamma : A \to C$ entonces un homomorfismo de A-álgebras es un homomorfismo de anillos $\phi : B \to C$ tal que $\gamma = \phi \circ \varphi$. Y por último, que B es una A-álgebra finitamente generada si existe, para algún $n \in \mathbb{N}$, un homomorfismo de A-álgebras suprayectivo $\varphi : A[x_1, \ldots, x_n] \to B$.

Sea $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ cualquier función entre dos curvas. Notamos entonces que φ determina de manera única dos funciones $\varphi_1, \varphi_2 : Z_f(\overline{k}) \to \overline{k}$ tales que $\varphi(a,b) := (\varphi_1(a,b), \varphi_2(a,b))$.

Definición 1.10.1. *Una función $Z_f(\overline{k}) \to Z_g(\overline{k})$ entre dos curvas planas es un morfismo de curvas planas afines si existen dos polinomios $\alpha(x,y)$ y $\beta(x,y)$ en $\overline{k}[x,y]$ tales que $\varphi_1(a,b) = \alpha(a,b)$ y $\varphi_2(a,b) = \beta(a,b)$, $\forall\ (a,b) \in Z_f(\overline{k})$.*

Tenemos entonces un lema.

Lema 1.10.2. *Sean $f, g \in \overline{k}[x,y]$ polinomios irreducibles. Dotamos a $Z_f(\overline{k})$ y $Z_g(\overline{k})$ con la topología de Zariski. Sea $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ un morfismo de curvas. Entonces φ es continua.*

Ejemplo 1.10.3. *Proyecciones sobre los ejes x y y. Sea $f(x,y)$ cualquier polinomio irreducible. Sea $g(x,y) = y$. La curva $Z_y(\overline{k})$ es el "eje x" en $\mathbb{A}^2(\overline{k})$. La función $p_x : Z_f(\overline{k}) \to Z_y(\overline{k})$, con $(a,b) \mapsto (a,0)$, es un morfismo de curvas. Definimos similarmente la proyección al "eje y", $p_y : Z_f(\overline{k}) \to Z_x(\overline{k})$, con $(a,b) \mapsto (0,b)$.*

Definición 1.10.4. *Un morfismo de curvas planas $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ es un isomorfismo si existe un morfismo de curvas planas $\psi : Z_g(\overline{k}) \to Z_f(\overline{k})$ tal que $\varphi \circ \psi = \mathrm{Id}_{Z_g(\overline{k})}$ y $\psi \circ \varphi = \mathrm{Id}_{Z_f(\overline{k})}$. Si $f = g$ entonces el isomorfismo φ es un automorfismo.*

Sean $Z_f(\overline{k})$ y $Z_g(\overline{k})$ dos curvas planas afines dadas por dos polinomios irreducibles f y g. Cualquier función continua $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ define una función

$$\varphi_c^* : C(Z_g(\overline{k}), \overline{k}) \to C(Z_f(\overline{k}), \overline{k})$$

$$h \mapsto h \circ \varphi$$

Se vio cómo los anillos $C_f := \overline{k}[x, y](f)$ y $C_g := \overline{k}[u, v]/(g)$ se puede pensar como el anillo de funciones continuas de las curvas $Z_f(\overline{k})$ y $Z_g(\overline{k})$ a $\overline{k}$. Consideramos el siguiente diagrama del cual se desprende un lema 1.10.5 siguiente:

$$\begin{array}{ccc} C_g & & C_f \\ \downarrow{\scriptstyle i_g} & & \downarrow{\scriptstyle i_f} \\ C(Z_g(\overline{k}), \overline{k}) & \xrightarrow{\varphi_c^*} & C(Z_f(\overline{k}), \overline{k}) \end{array}$$

Lema 1.10.5. *Sea $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ una función continua entre dos curvas algebraicas dotadas con la topología de Zariski. La función φ es un morfismo de curvas planas si y sólo si $(\varphi_c^* \circ i_g)(C_g) \subseteq i_f(C_f)$. Si φ es un morfismo de curvas entonces la función $\varphi_c^*|_{i_g(C_g)}$ define un homomorfismo de $\overline{k}$-álgebras entre C_g y C_f, denotado por φ^*, tal que el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} C_g & \xrightarrow{\varphi^*} & C_f \\ \downarrow{\scriptstyle i_g} & & \downarrow{\scriptstyle i_f} \\ C(Z_g(\overline{k}), \overline{k}) & \xrightarrow{\varphi_c^*} & C(Z_f(\overline{k}), \overline{k}) \end{array}$$

Explícitamente, se define como

$$\varphi^*(\text{clase de } u) := (i_f)^{-1}(\varphi_c^* \circ i_g)(\text{clase de } u)$$

$$\varphi^*(\text{clase de } v) := (i_f)^{-1}(\varphi_c^* \circ i_g)(\text{clase de } v)$$

Sea $\varphi^* : C_g \to C_f$ un homomorfismo de k-álgebras (i.e., φ^* es un homomorfismo de anillos tal que $\varphi^*|_{\overline{k}} = \mathrm{Id}$). El homomorfismo define de manera natural un morfismo de curvas $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$. Sea $\varphi_u(x, y) \in \overline{k}[x, y]$ un polinomio tal que su clase en C_f es igual a $\varphi^*(\text{clase de } u)$, y sea $\varphi_v(x, y) \in \overline{k}[x, y]$ tal que su clase en C_f es igual a $\varphi^*(\text{clase de } u)$. Definimos:

$$\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$$

$$(a, b) \mapsto (\varphi_u(a, b), \varphi_v(a, b))$$

Notamos que φ está bien definida y no depende de las elecciones de $\varphi_u(x, y)$ y $\varphi_v(x, y)$, pues como $g(\text{clase de } u, \text{clase de } v) = 0$ en C_g se obtiene en C_f que:

$$\varphi^*(g(\text{clase de } u, \text{clase de } v)) = 0 = g(\text{clase de } \varphi_u(x, y), \text{clase de } \varphi_v(x, y))$$

Por tanto, f divide a $g(\varphi_u(x,y),\varphi_v(x,y))$, y entonces para todo $(a,b) \in Z_f(\overline{k})$ se tiene $g(\varphi_u(a,b),\varphi_v(a,b)) = 0$, y por tanto $(\varphi_u(a,b),\varphi_v(a,b)) \in Z_g(\overline{k})$.

Lema 1.10.6. *Sea $\varphi^* : C_g \to C_f$ un homomorfismo de k-álgebras. Sea $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ el morfismo de curvas inducido como se describió antes. Sea*

$$\varphi_c^* : C(Z_g(\overline{k}),\overline{k}) \to C(Z_f(\overline{k}),\overline{k})$$

$$h \mapsto h \circ \varphi$$

Entonces el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} C_g & \xrightarrow{\varphi^*} & C_f \\ \downarrow{\scriptstyle i_g} & & \downarrow{\scriptstyle i_f} \\ C(Z_g(\overline{k}),\overline{k}) & \xrightarrow{\varphi_c^*} & C(Z_f(\overline{k}),\overline{k}) \end{array}$$

Ejemplo 1.10.7. *La función proyección al eje x, $p_x : Z_f(\overline{k}) \to Z_g(\overline{k})$, corresponde a un homomorfismo de anillos $p_x^* : \overline{k}[x,y]/(y) \to C_f$. Identificamos al anillo $\overline{k}[x,y]/(y)$ con $\overline{k}[x]$, y pensamos la función natural $k[x] \to C_f$ como una función sobre funciones a la proyección del eje x.*

Definición 1.10.8. *El conjunto de ideales primos de un anillo A es el espectro de A y se denota por* $\mathrm{Spec}(A)$. *Dado un homomorfismo de anillos $\psi : A \to B$, consideramos la función natural*

$$\mathrm{Spec}(\psi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

$$P \mapsto \psi^{-1}(P)$$

Sea $Z_f(\overline{k})$. Recordamos que la función $I_f : Z_f(\overline{k}) \to \mathrm{Max}(C_f)$, $(a,b) \mapsto (x-a, y-b)$, es biyectiva.

Concluimos con el siguiente lema.

Lema 1.10.9. *Sean C_f y C_g dos anillos de funciones de dos curvas planas afines dadas por dos polinomios irreducibles $f(x,y)$ y $g(u,v)$, respectivamente. Sea $\varphi^* : C_g \to C_f$ un homomorfismo de k-álgebras. Entonces la función* $\mathrm{Spec}(\varphi^*)$ *se restringe a una función $\varphi' : \mathrm{C_f} \to C_g$, $M \mapsto (\varphi^*)^{-1}(M)$. Más aún, el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} Z_f(\overline{k}) & \xrightarrow{I_f} & \mathrm{Max}(C_f) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} \\ Z_g(\overline{k}) & \xrightarrow{I_g} & \mathrm{Max}(C_g) \end{array}$$

1.11. Puntos singulares

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 5).

Definición 1.11.1. *Sea $f(x,y) \in k[x,y]$. Un punto (a,b) en $Z_f(\overline{k})$ es un punto singular si $(\frac{\partial f}{\partial x})(a,b) = (\frac{\partial f}{\partial y})(a,b)$. Si (a,b) es un punto singular entonces decimos que la curva $Z_f(\overline{k})$ es singular en (a,b). La curva afín $Z_f(\overline{k})$ definida por $f(x,y)$ es no singular si no contiene ningún punto singular.*

Sea $l(x,y) := (\frac{\partial f}{\partial x})(a,b)(x-a) + (\frac{\partial f}{\partial y})(a,b)(y-b)$. Cuando (a,b) es un punto no singular de $Z_f(\overline{k})$, la recta $Z_l(\overline{k})$ se le llama la recta tangente de $Z_f(\overline{k})$ en (a,b).

Definimos ahora el discriminante de un polinomio.

Definición 1.11.2. *Sea A cualquier anillo. Sea $g(x) \in A[x]$ cualquier polinomio. Sea $g'(x)$ la derivada de $g(x)$ en $A[x]$. El resultante de $g(x)$ y $g'(x)$ depende únicamente de los coeficientes de $g(x)$ y se le llama el discriminante de $g(x)$, y se denota por* $\mathrm{disc}(g)$.

Consideramos cualquier dominio factorial A, y sea $a \in A$. Supongamos que $(x-a)$ divide a $g(x)$. Entonces $(x-a)^2$ divide a $g(x)$ si y sólo si $(x-a)$ divide a $g'(x)$. En particular, del lema 1.8.5 se obtiene que $g(x)$ tiene una raíz doble si y sólo si $\mathrm{disc}(g) = 0$.

En general, si tuviéramos una factorización $h(x,y) = f(x,y)g(x,y)$ en $\overline{k}[x,y]$, con f y g primos relativos, entonces se puede verificar que $Z_h(\overline{k}) = Z_f(\overline{k}) \cup Z_g(\overline{k})$. Si tuviéramos $f \in \overline{k}[x,y]$ un polinomio irreducible entonces notamos que por la sección 1.10 se tiene que la proyección dada por

$$\mathbf{x} : Z_f(\overline{k}) \to \overline{k} = \mathbb{A}^1(\overline{k})$$

$$(a,b) \mapsto a$$

es un morfismo de curvas que corresponde al homomorfismo de anillos

$$\mathbf{x}^* : \overline{k}[x] \to C_f$$

$$x \mapsto \text{clase de } x$$

La función $\mathbf{x}^*$ es inyectiva si $f(x,y)$ no es de la forma $cx + d$, para algunos $c, d \in \overline{k}$ (para verlo, usamos que $\overline{k}$ es algebraicamente cerrado y que f es irreducible). Cuando $\mathbf{x}^*$ es inyectiva, podemos identificar $\overline{k}[x]$ con su imagen en C_f. Consideramos el caso en que $A = \overline{k}[x]$, $K = \overline{k}(x)$, y $L = \overline{k}(Z_f)$. Si el polinomio $f(x,y)$ es mónico en y (visto como polinomio en $\overline{k}[x][y]$) entonces la función $\mathbf{x}^*$ es inyectiva y el anillo C_f está contenido en la cerradura entera del anillo $\overline{k}[x]$

en el campo $\overline{k}(Z_f)$ (pues la clase de y en C_f es entero sobre $\overline{k}[x]$). El teorema siguiente nos dice cuándo C_f es la cerradura entera de $\overline{k}[x]$ en $\overline{k}(Z_f)$.

Teorema 1.11.3. *Sea $f \in \overline{k}[x,y]$ un polinomio irreducible. Entonces el anillo $C_f := \overline{k}[x,y]/(f)$ es enteramente cerrado si y sólo si la curva $Z_f(\overline{k})$ es no singular.*

1.12. Localización

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 6) o en [1] (capítulo 3).

Definición 1.12.1. *Sea A un anillo conmutativo. Un conjunto S en A es multiplicativo si $0 \notin S$, $1 \in S$, y si $a, b \in S$ entonces $ab \in S$.*

Ejemplo 1.12.2.

- *(i) Sea $n \in A$. Si n no es divisor de cero en A entonces el conjunto $S := \{1, n, n^2, \dots\}$ es multiplicativo.*
- *(ii) Sea $P \subseteq A$ un ideal primo. El conjunto $S := A \setminus P$ es multiplicativo.*

Sea A un anillo conmutativo, y sea S un subconjunto multiplicativo de A. Se define un nuevo anillo, denotado por $S^{-1}A$, el cual se puede interpretar como el anillo obtenido al ádjuntar a A los inversos de todos los elementos en el conjunto S', y se define como sigue:

Consideramos en $A \times S$ la relación

$$(a,s) \equiv (b,t) \text{ si y sólo si existe } \sigma \in S \text{ tal que } \sigma(at - bs) = 0$$

Notamos que cuando el anillo A es un dominio entero, la ecuación $\sigma(at - bs) = 0$ implica que $at - bs = 0$ pues $\sigma \in S$ y $0 \notin S$.

Lema 1.12.3. *La relación $\equiv$ sobre $A \times S$ es una relación de equivalencia.*

Sea a/s la clase de equivalencia de (a,s) en $A \times S$. Sea $S^{-1}A$ el conjunto de clases de equivalencia. Se le puede dar a $S^{-1}A$ una estructura de anillos como sigue:

$$(a/s) + (b/t) = (at + bs)/st$$

$$(a/s)(b/t) = (ab/st)$$

$$1/1 = \text{elemento identidad}$$

Se le llama a $S^{-1}A$ el anillo de fracciones de A con respecto a S. La función

$$j_S : A \to S^{-1}A$$

$$a \mapsto a/1$$

es un homomorfismo de anillos. La función j_A (también denotada por j) junto con $S^{-1}A$ cumplen las siguientes propiedades:

- (i) Sea $s \in S$. El elemento $j(s) = s/1$ en $S^{-1}A$ es invertible y su inverso es el elemento $1/s$.
- (ii) Si A es un dominio entero entonces j es inyectivo. Para verlo, notamos que si $j(a) = a/1 = 0/1$ entonces existe $\sigma \in S$ tal que $\sigma a = 0$, pero como A es dominio y $0 \notin S$, se obtiene $a = 0$.
- (iii) Cuando A es dominio, el anillo $S^{-1}A$ es también dominio. Para verlo, si tenemos $a/s, b/t \in S^{-1}A$ con $a/s \cdot b/t = 0$ entonces existe $\sigma \in S$ tal que $\sigma(ab - 0) = 0$. Como A es dominio y $\sigma \neq 0$, se obtiene que a o b tiene que ser cero.
- (iv) Cuando A es dominio, el campo de fracciones K de A es el anillo $S^{-1}A$ con $S = A \setminus \{0\}$.

Mencionamos ahora una propiedad importante.

Proposición 1.12.4. *(Propiedad universal de anillos de fracciones.) Sea A un anillo conmutativo y sea $S \subseteq A$ un subconjunto multiplicativo. Sea $g : A \to B$ un homomorfismo de anillos tal que para todo $s \in S$ se tiene que $g(s)$ es una unidad en B. Entonces existe un único homomorfismo de anillos $g' : S^{-1}A \to B$ tal que $g = g' \circ j$.*

De la proposición 1.12.4 tenemos el siguiente corolario.

Corolario 1.12.5. *Sea A un dominio con campo de fracciones K. Sea $S \subseteq A$ un subconjunto multiplicativo. El anillo $S^{-1}A$ puede ser identificado de manera única con el subanillo $A[1/s, s \in S]$ de K, generado por A y el conjunto $\{1/s \mid s \in S\}$.*

El lema 1.12.6 a continuación se usa para probar el lema 1.12.8, y a su vez el lema 1.12.8 y la observación 1.12.7 se usan para la proposición 1.12.9 (ver [9], sección 6 del capítulo 2 para las demostraciones).

Lema 1.12.6. *Sea A un anillo conmutativo. Sea $S \subseteq A$ un subconjunto multiplicativo. Sea I cualquier ideal de A. Sea $S^{-1}I$ el ideal de $S^{-1}A$ generado por la imagen $j_S(I)$. Entonces $S^{-1}I = \{x/s \mid x \in I, s \in S\}$. En particular, $S^{-1}I = S^{-1}A$ si y sólo si $I \cap S \neq \emptyset$.*

Observación 1.12.7. *Consideramos el homomorfismo de anillos $j : A \to S^{-1}A$. Sea J cualquier ideal de $S^{-1}A$, y sea $I := j^{-1}(J)$. Entonces el ideal $S^{-1}I$ es igual a J. Para verlo, si $x \in I$ entonces $x/s = j(x)s^{-1}$ pertenece a J. Y por otro lado, si $x/s \in J$ entonces $x/1 \in J$, y por tanto $x \in I$.*

Sea $f : A \to B$ un homomorfismo de anillos. Sea J cualquier ideal de B. Sea $I := f^{-1}(J)$. Notamos que el ideal $f(I)B$ de B generado por $f(I)$ está contenido en J. Cuando f es suprayectivo entonces $f(I)B = J$. Pero en general, la inclusión $f(I)B \subset J$ es estricta.

Lema 1.12.8. *Sea A un anillo conmutativo. Sea $S \subseteq A$ un subconjunto multiplicativo. Sea $P \subseteq A$ un ideal primo tal que $P \cap S = \emptyset$. Entonces $S^{-1}I$ es un ideal primo de $S^{-1}A$.*

Proposición 1.12.9. *Sea A un anillo conmutativo. Sea $S \subseteq A$ un subconjunto multiplicativo. La función $j : A \to S^{-1}A$ induce una biyección*

$$j^{-1} : \mathrm{Spec}(S^{-1}A) \to \{P \in \mathrm{Spec}(A) \mid P \subseteq A \setminus S\}$$

donde la función j^{-1} es tal que $P \mapsto S^{-1}P$. Además, j y su inverso preservan inclusiones.

Mencionamos ahora dos definiciones.

Definición 1.12.10. *Sea $P \subseteq A$ cualquier ideal primo. El conjunto $S = A \setminus P$ es multiplicativo, y el anillo $S^{-1}A$ es la localización de A en P, y se denota por A_P. El ideal $S^{-1}P$ se denota por PA_P.*

Definición 1.12.11. *Un anillo A es local si tiene un único ideal maximal.*

Ahora, mencionamos tres corolarios de la proposición 1.12.9.

Corolario 1.12.12. *Sea $P \in \mathrm{Spec}(A)$. Entonces $\mathrm{Spec}(A_P)$ está en biyección con el conjunto de ideales primos de A contenidos en P, y esta biyección es tal que preserva inclusiones. En particular, el anillo A_P es local con ideal maximal PA_P.*

Corolario 1.12.13. *Sea A cualquier anillo. Sea $P \in \mathrm{Spec}(A)$. Entonces $\mathrm{ht}(P) = \dim(A_P)$, y $\dim(A) = \sup\{\dim(A_P) \mid P \in \mathrm{Spec}(A)\}$.*

Corolario 1.12.14. *Sea A un dominio de dimensión 1. Sea S un conjunto multiplicativo tal que $A \setminus S$ contiene a un ideal maximal P de A. Entonces $S^{-1}A$ tiene dimensión 1. En particular, A_P tiene dimensión 1.*

Sea f un polinomio irreducible. Sea $C_f := \overline{k}[x, y]/(f)$. Consideramos $\overline{k}(Z_f)$ el campo de fracciones de C_f. Sea $(a, b) \in Z_f(\overline{k})$ cualquier punto. Tenemos la siguiente definición:

Definición 1.12.15. *Decimos que una función racional α en $\overline{k}(Z_f)$ está definida en (a,b) si existen $g(x,y)$ y $h(x,y)$ en $\overline{k}[x,y]$ tales que $\alpha = \frac{g(x,y)+(f)}{h(x,y)+(f)}$ en $\overline{k}(Z_f)$ (el cual denotamos solamente por $g(x,y)/h(x,y)$), y tal que $h(a,b) \neq 0$. Cuando α está definido en (a,b) entonces definimos el valor de α en (a,b) como $\alpha(a,b) := g(a,b)/h(a,b)$.*

Notamos que el valor de $\alpha(a,b)$ no depende de la elección de $g(x,y)$ y $h(x,y)$. Sea $I_f(a,b)$ el ideal maximal de C_f correspondiente a (a,b) (corolario 1.9.5). Recordamos que una función h de C_f pertenece a $I_f(a,b)$ si y sólo si $h(a,b) = 0$ (de la definición 1.9.1). Por tanto, una función racional α está definida en (a,b) si y sólo si existen $g, h \in C_f$ con $h \notin I_f(a,b)$ tal que $\alpha = g/h$. Se obtiene entonces que el anillo $(C_f)_{I_f(a,b)}$ puede ser identificado, como en el corolario 1.12.5, con el subanillo de $\overline{k}(Z_f)$ que consiste de todas las funciones racionales de $\overline{k}(Z_f)$ definidas en (a,b).

Definición 1.12.16. *Llamamos a un punto P sobre la curva $Z_f(\overline{k})$ un polo de α si una función α no está definida.*

Notamos que se obtiene del lema 1.8.11 que una función α tiene únicamente un número finito de polos $Z_f(\overline{k})$.

Mencionamos ahora dos proposiciones importantes.

Proposición 1.12.17. *Si A es un anillo noetheriano y S es un subconjunto multiplicativo entonces $S^{-1}A$ también es un anillo noetheriano.*

Proposición 1.12.18. *Sea A un dominio enteramente cerrado. Sea $S \subseteq A$ multiplicativo. Entonces $S^{-1}A$ también es dominio enteramente cerrado.*

El siguiente corolario es consecuencia de 1.2.18, y el corolario 1.12.20 es consecuencia de 1.2.17, 1.2.18 y de 1.2.14 (ver [9]. sección 6 del capítulo 2).

Corolario 1.12.19. *Sea B la cerradura entera de un dominio A en un campo L. Sea $S \subseteq A$ un subconjunto multiplicativo. Entonces el anillo $S^{-1}B$ es la cerradura entera de $S^{-1}A$ en L.*

Corolario 1.12.20. *Sea A un dominio de Dedekind. Sea $S \subseteq A$ un subconjunto multiplicativo tal que $A \setminus S$ contiene a un ideal primo no trivial de A. Entonces $S^{-1}A$ también es un dominio de Dedekind.*

1.13. Dimensión y curvas afines

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 7).

Consideramos la siguiente proposición.

Proposición 1.13.1. *Sea A un dominio de dimensión 1. Entonces el anillo $A[y]$ tiene dimensión 2 o 3. Si A es un dominio de ideales principales entonces $A[y]$ tiene dimensión 2.*

En general, se puede probar que si A es un anillo de dimensión n entonces $n+1 \leq \dim(A[y]) \leq 2n+1$, y que si A es noetheriano entonces $\dim(A[y]) = n+1$.

El siguiente es un corolario de la proposición 1.13.1.

Corolario 1.13.2. *Sea $f \in k[x,y]$ un polinomio irreducible. Entonces el anillo $k[x,y]/(f)$ tiene dimensión 1.*

Además, se puede probar el siguiente corolario usando el corolario 1.13.2 (ver [9]).

Corolario 1.13.3. *Sea $f \in \overline{k}[x,y]$ un polinomio irreducible. Entonces todo ideal primo distinto de cero de $C_f = \overline{k}[x,y]/(f)$ es un ideal maximal generado por las clases de $x-a$ y $y-b$ en C_f para algún $(a,b) \in \overline{k} \times \overline{k}$ tal que $f(a,b) = 0$.*

Sea $f \in \overline{k}[x,y]$ irreducible. La $\overline{k}$-álgebra C_f tiene dimensión 1. El conjunto $Z_f(\overline{k})$ está en biyección con $\mathrm{Max}(C_f)$. Cualquier morfismo de curvas $Z_f(\overline{k}) \to Z_g(\overline{k})$ viene dada por un homomorfismo de $\overline{k}$-álgebras $\varphi^* : C_g \to C_f$. Notamos que un conjunto de dos funciones sobre $Z_f(\overline{k})$ son fijados, a saber, $\{\text{clase de } x, \text{clase de } y\}$. Estas dos funciones generan a C_f como $\overline{k}$-álgebra. En particular, C_f es una $\overline{k}$-álgebra finitamente generada.

Definición 1.13.4. *Sea k cualquier campo. Una curva afín sobre k es un par $(\mathrm{Max}(A), A)$, donde A es una k-álgebra finitamente generada de dimensión 1. Cuando A es un dominio, la curva $(\mathrm{Max}(A), A)$ se le llama entera (o irreducible y reducida).*

Sea $(\mathrm{Max}(A), A)$ cualquier curva afín sobre $\overline{k}$. Notamos que podemos pensar a los elementos de A como funciones definidas sobre $\mathrm{Max}(A)$, así como se hizo en el caso de curvas planas, ya que se puede probar que si $M \in \mathrm{Max}(A)$ entonces A/M es isomorfo a $\overline{k}$, por lo que el valor que toma $h \in A$ en el elemento M se define entonces como $h(M) :=$ clase de h en el cociente $A/M \cong \overline{k}$.

Definición 1.13.5. *Una curva plana entera sobre $\overline{k}$ viene dada por una curva entera* $(\mathrm{Max}(A), A)$ *y un conjunto de dos funciones en A (fijas), digamos x y y, que generan a A visto como una $\overline{k}$-álgebra.*

Sea $(\mathrm{Max}(A), A)$ una curva plana entera sobre $\overline{k}$. Consideramos la función $\overline{k}[X, Y] \to A$, con $X \mapsto x$ y $Y \mapsto y$. Se obtiene de las hipótesis que esta función es suprayectiva. Como A es un dominio entonces el kernel de esta función es un ideal primo P de $\overline{k}[X, Y]$. Como A tiene dimensión 1, se obtiene que $P = (f(X, Y))$ para algún polinomio irreducible f. La función

$$\mathrm{Max}(A) \to \overline{k}^2$$

$$M \mapsto x(M), y(M)$$

es inyectivo, y su imagen es el conjunto $Z_f(\overline{k})$.

En general, dada cualquier curva entera $(\mathrm{Max}(A), A)$ y un conjunto de n funciones $x_1, \ldots, x_n$ que generan a A visto como una $\overline{k}$-álgebra, se puede probar que la función

$$\varphi : \mathrm{Max}(A) \to \overline{k}^n$$

$$M \mapsto (x_1(M), \ldots, x_n(M))$$

es también inyectiva. Más aún, su imagen puede describirse como sigue: consideramos la función $\overline{k}[X_1, \ldots . X_n] \to A$, con $X_i \mapsto x_i$, $\forall\ i = 1, \ldots, n$. El kernel de esta función es un ideal primo P. Como $\overline{k}[X_1, \ldots, X_n]$ es noetheriano, se obtiene del teorema 1.16.1 que $P = (f_1, \ldots, f_s)$ es finitamente generado. Se puede verificar entonces que la imagen de φ en $\overline{k}^n$ es el conjunto de ceros en común del sistema de ecuaciones $\{f_i = 0\}_{i=1}^s$.

Definición 1.13.6. *Un morfismo de curvas afines sobre k entre* $(\mathrm{Max}(A), A)$ *y* $(\mathrm{Max}(B), B)$ *es un par (φ, φ^*), donde $\varphi^* : B \to A$ es un homomorfismo de k-álgebras, y $\varphi : \mathrm{Max}(A) \to \mathrm{Max}(B)$ es tal que manda M a $(\varphi^*)^{-1}(M)$.*

El ideal $(\varphi^*)^{-1}(M)$ siempre es un ideal maximal, por lo que φ está bien definida. Notamos que la función φ es la restricción de la función $\mathrm{Spec}(\varphi^*) : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ a $\mathrm{Max}(A)$.

Definición 1.13.7. *Una curva afín* $(\mathrm{Max}(A), A)$ *sobre k se le llama una línea afín si A es isomorfo, como k-álgebra, al anillo de polinomios $k[x]$.*

La curva $(\mathrm{Max}(\overline{k}[x]), \overline{k}[x])$ puede pensarse como una línea afín con una función coordenada, a saber, x. La función $\mathrm{Max}(\overline{k}[x]) \to \overline{k}$, con $M \mapsto x(M)$, es una biyección.

Sea $(\mathrm{Max}(A), A)$ cualquier curva afín entera sobre $\overline{k}$. Identificamos a $\overline{k}$ con el subcampo de $\overline{k} \cdot 1$ de A. Un elemento de $\overline{k}$ de A se le llama una función constante. Cualquier función no constante α en A induce un morfismo de A a

una línea afín: la función $\varphi^* : \overline{k}[x] \to A$, con $x \mapsto \alpha$, es un homomorfismo de $\overline{k}$-álgebras. Por tanto, $(\varphi, \varphi^*) : (\mathrm{Max}(A), A) \to (\mathrm{Max}(\overline{k}[x]), \overline{k}[x])$ es un morfismo de curvas.

Definición 1.13.8. *Sea* $(\mathrm{Max}(A), A)$ *cualquier curva entera sobre* $\overline{k}$*. Un morfismo suprayectivo de curvas* $(\varphi, \varphi^*) : (\mathrm{Max}(\overline{k}[t]), \overline{k}[t]) \to (\mathrm{Max}(A), A)$ *se le llama una parametrización de* $(\mathrm{Max}(A), A)$*.*

Si $(\mathrm{Max}(C_f), C_f)$ es una curva plana entonces la parametrización (φ, φ^*) es tal que el homomorfismo $\varphi^* : C_f \to \overline{k}[t]$ está dado por dos polinomios $x(t), y(t) \in \overline{k}[t]$ tales que $f(x(t), y(t)) = 0$ en $\overline{k}[x]$. La función $\varphi : \mathrm{Max}(\overline{k}[t]) \to \mathrm{Max}(C_f)$ se puede identificar con la función $\overline{k} \to Z_f(\overline{k})$ que manda un elemento a a $(x(a), y(a))$.

1.14. Dominios de ideales principales locales

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 8).

Sea $f \in \overline{k}[x, y]$ un polinomio ireducible. Sea $C_f := \overline{k}[x, y]/(f)$. Sea $(a, b) \in Z_f(\overline{k})$, y sea M el correspondiente ideal maximal generado en C_f por las clases de $x - a$ y $y - b$. Como se vio antes, el anillo local $(C_f)_M$ puede interpretarse como el anillo de funciones racionales sobre $Z_f(\overline{k})$ que están definidas en (a, b). Tenemos que (a, b) es un punto no singular si y sólo si el anillo $(C_f)_M$ es un dominio de ideales principales.

Proposición 1.14.1. *El punto* (a, b) *es un punto no singular de* $Z_f(\overline{k})$ *si y sólo si el ideal maximal de* $(C_f)_M$ *está generado por un elemento.*

Sea $f \in \overline{k}[x, y]$ irreducible. Como C_f tiene dimensión 1, la localización $(C_f)_M$ es un dominio de dimensión 1 para todo $M \in \mathrm{Max}(C_f)$. En particular, $(C_f)_M$ tiene únicamente dos ideales primos: (0) y $M(C_f)_M$. Cuando M corrresponde a un punto no singular de la curva $Z_f(\overline{k})$, la proposición 1.14.1 nos dice que $M(C_f)_M$ es un ideal principal. La siguiente proposición nos dice que $(C_f)_M$ es un dominio de ideales principales.

Proposición 1.14.2. *Sea* A *cualquier anillo conmutativo. Entonces son equivalente:*

- *(1) Todo ideal de* A *es principal.*
- *(2) Todo ideal primo de* A *es principal.*

El siguiente es un corolario de la proposición 1.14.2.

Corolario 1.14.3. *Sea $f \in \overline{k}[x,y]$ cualquier polinomio irreducible. Entonces la curva $Z_f(\overline{k})$ es no singular si y sólo si el anillo C_f es tal que su localización en cualquier ideal maximal es un dominio de ideales principales local.*

Terminamos esta sección con tres lemas que serán de utilidad en los siguientes capítulos.

Lema 1.14.4. *Sea A un dominio de dimensión 1. Sea $M \subseteq A$ un ideal maximal generado por dos elementos x y y. Entonces son equivalentes:*

- *(i) A_M es un dominio de ideales principales.*
- *(ii) Existen dos elementos $u, v \in A$ tales que $ux + vy = 0$ y tal que al menos uno de los elementos u, v no pertenece a M.*
- *(iii) Uno de los dos elementos x, y genera a MA_M*

Lema 1.14.5. *Sea A un dominio de ideales principales local. Sea K su campo de fracciones y $x \in K$. Entonces $x \in A$ o $1/x \in A$.*

Lema 1.14.6. *Sea R un dominio de ideales principales local con campo de fracciones K. Sea S cualquier dominio local con $R \subseteq S \subseteq K$. Sean M_R y M_S los ideales maximales de R y S, respectivamente. Si $M_R \subseteq M_S$ entonces $R = S$.*

1.15. Localización de módulos

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 9) y en [1] (capítulo 3).

Sea A cualquier anillo. Sea M un A-módulo y $S \subseteq A$ un subconjunto multiplicativo. Consideramos la siguiente relación sobre $M \times S$:

$$(m,s) \equiv (m',s') \text{ si y sólo si } \exists\ \sigma \in S \text{ tal que } \sigma(s'm - sm') = 0.$$

La relación $\equiv$ es una relación de equivalencia. Denotamos por m/s a la clase de (m,s) bajo $\equiv$, y $S^{-1}M$ al conjunto de clases de equivalencia bajo $\equiv$. El conjunto $S^{-1}M$ tiene una estructura de $S^{-1}A$-módulo:

$$\forall\ m_1/s_1, m_2/s_2 \in S^{-1}M, \quad (m_1/s_1) + (m_2/s_2) = (s_2m_1 + s_1m_2)/s_1s_2$$

$$\forall\ a/s \in S^{-1}A, \forall\ m/t \in S^{-1}M, \quad (a/s)(m/t) = am/st$$

El $S^{-1}A$-módulo $S^{-1}M$ es el módulo de fracciones de M con respecto a S. Un homomorfismo de A-módulos $f : M \to N$ induce un homomorfismo de $S^{-1}A$-módulos

$$S^{-1}(f) : S^{-1}M \to S^{-1}N$$

$$m/s \mapsto f(m)/s$$

Si $g : N \to Q$ es cualquier homomorfismo de A-módulos entonces $S^{-1}(g \circ f) = S^{-1}(g) \circ S^{-1}(f)$.

Tenemos entonces

Proposición 1.15.1. *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión de A-módulos que sea exacta en M. Sea $S \subseteq A$ un subconjunto multiplicativo. Entonces la sucesión de $S^{-1}A$-módulos*

$$S^{-1}M' \overset{S^{-1}(f)}{\to} S^{-1}M \overset{S^{-1}(g)}{\to} S^{-1}M''$$

es exacta en $S^{-1}M$.

Tenemos dos corolarios de la proposición 1.15.1.

Corolario 1.15.2. *Sea $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta de A-módulos. Sea S un subconjunto multiplicativo. Entonces la sucesión*

$$0 \to S^{-1}M' \overset{S^{-1}(f)}{\to} S^{-1}M \overset{S^{-1}(g)}{\to} S^{-1}M'' \to 0$$

es una sucesión exacta de $S^{-1}A$-módulos

.

Corolario 1.15.3. *Sea $S \subseteq A$ un subconjunto multiplicativo. Sea $f : M \to N$ un homomorfismo de A-módulos. Entonces*

- *(i)* $S^{-1}(\mathrm{Im}(f)) = \mathrm{Im}(S^{-1}(f))$.
- *(ii)* $S^{-1}(\mathrm{Ker}(f)) = \mathrm{Ker}(S^{-1}(f))$.

Sea $P \subseteq A$ un ideal primo. Sea $S := A \setminus P$. Denotamos al $S^{-1}A$-módulo $S^{-1}M$ por M_P. Si $f : M \to N$ es un homomorfismo de A-módulos, denotamos a la función $S^{-1}(f)$ por f_P.

El siguiente lema sirve para probar la proposición 1.15.5.

Lema 1.15.4. *Sea M un A-módulo. Entonces son equivalentes:*

- *(i)* $M = (0)$.
- *(ii)* $M_P = (0)$ *para todo* $P \in \mathrm{Spec}(A)$.
- *(iii)* $M_P = (0)$ *para todo* $P \in \mathrm{Max}(A)$.

Proposición 1.15.5. *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión de A-módulos (es decir,* $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$*). Entonces son equivalentes:*

- *(i) La sucesión* $M' \xrightarrow{f} M \xrightarrow{g} M''$ *es exacta en* M.
- *(ii) La sucesión* $M'_P \xrightarrow{f_P} M_P \xrightarrow{g_P} M''_P$ *es exacta en* M_P *para todo* $P \in \mathrm{Spec}(A)$.
- *(iii) La sucesión* $M'_P \xrightarrow{f_P} M_P \xrightarrow{g_P} M''_P$ *es exacta en* M_P *para todo* $P \in \mathrm{Max}(A)$.

Una consecuencia de la proposición 1.15.5 es

Corolario 1.15.6. *Sea* $f : M \to N$ *un homomorfismo de* A*-módulos. Entonces* f *es inyectiva (respectivamente suprayectiva) si y sólo si la funciones* f_P *son inyectivas (respectivamente suprayectivas) para todo* $P \in \mathrm{Max}(A)$.

Tenemos la siguiente proposición.

Proposición 1.15.7. *Sea* A *un dominio conmutativo. Entonces*

$$A = \bigcap_{P \in \mathrm{Spec}(A)} A_P = \bigcap_{P \in \mathrm{Max}(A)} A_P$$

Una consecuencia de la proposición 1.15.7 es

Corolario 1.15.8. *Sea* A *un dominio conmutativo. Entonces son equivalentes:*

- *(i)* A *es enteramente cerrado.*
- *(ii)* A_P *es enteramente cerrado para todo* $P \in \mathrm{Spec}(A)$.
- *(iii)* A_P *es enteramente cerrado para todo* $P \in \mathrm{Max}(A)$.

El siguiente teorema nos dice sobre la relación entre una curva no singular y el concepto de enteramente cerrado.

Teorema 1.15.9. *Sea* $f(x, y) \in \overline{k}[x, y]$ *un polinomio irreducible. El anillo* $C_f := \overline{k}[x, y]/(f)$ *es enteramente cerrado en su campo de fracciones* $\overline{k}(Z_f)$ *si y sólo si* $Z_f(\overline{k})$ *es no singular.*

Terminamos esta sección con una consecuencia del teorema 1.15.9.

Corolario 1.15.10. *Sea* $f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x) \in \overline{k}[x, y]$ *un polinomio irreducible. Entonces* C_f *es igual a la cerradura entera de* $\overline{k}[x]$ *en* $\overline{k}(Z_f)$ *si y sólo si* $Z_f(\overline{k})$ *es una curva no singular.*

1.16. Teorema de la base de Hilbert

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo II, sección 10) y en [6] (capítulo 1, sección 1, subsección 1.4).

Mencionamos solamente dos teoremas en esta sección. El siguiente teorema es útil en algunos resultados de los siguientes capítulos.

Teorema 1.16.1. *Sea A un anillo noetheriano. Sea B un A-módulo finitamente generado. Entonces B es un anillo noetheriano.*

En la demostración de lo anterior (ver [9]) se utiliza, entre otras cosas, el teorema de la base de Hilbert.

Teorema 1.16.2. *Un anillo A es noetheriano si y sólo si el anillo de polinomios $A[y]$ es noetheriano.*

1.17. Factorización única de ideales

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo III, sección 2).

Empezamos con dos lemas que resultan útiles en los siguientes capítulos.

Lema 1.17.1. *Sean $J \subseteq I$ dos ideales en un anillo A. Entonces $J = I$ si y sólo si $J_M = I_M$ para todos los ideales maximales M de A que contienen a J.*

Lema 1.17.2. *Sea A cualquier anillo y sea $S \subset A$ un subconjunto multiplicativo. Sean I, J dos ideales de A. Entonces $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$ en el anillo $S^{-1}A$. Sea A un anillo de dimensión 1. Sea J un ideal de A que se puede factorizar como un producto de ideales maximales, digamos $J = P_1^{a_1} \cdots P_s^{a_s}$. Sea M cualquier ideal maximal de A. Entonces, $J_M = (MA_M)^{a_i}$ si $M = P_i$ para algún i, y $J_M = A_M$ si $M \neq P_i$ para todo $i = 1, \ldots, s$.*

Mencionamos ahora una proposición.

Proposición 1.17.3. *Sea I cualquier ideal no trivial en un anillo noetheriano A. Entonces existe un número finito de ideales primos $P_1, \ldots, P_s$ y enteros positivos $a_1, \ldots, a_s$ tales que $P_1^{a_1} \cdots P_s^{a_s} \subseteq I \subseteq P_1 \cap \cdots \cap P_s$.*

El siguiente corolario es consecuencia de la proposición 1.17.3. En la demostración de dicho corolario (ver [9]) se usan los lemas 1.17.5 y 1.17.6.

Corolario 1.17.4. *Sea A un dominio noetheriano de dimensión 1. Sea I cualquier ideal no trivial distinto de A. Entonces el conjunto de ideales maximales de A que contienen a I es finito. Si $\{M_1, \ldots, M_s\}$ es dicho conjunto entonces existen $a_1, \ldots a_s$ tal que $M_1^{a_1} \cdots M_s^{a_s} \subseteq I \subseteq M_1 \cdots M_s$.*

Lema 1.17.5. *Sea P un ideal primo. Sean I, J dos ideales tales que $IJ \subseteq P$. Entonces $I \subseteq P$ o $J \subseteq P$.*

Lema 1.17.6. *Sea A cualquier anillo conmutativo. Sean $I_1, \ldots, I_n$ n ideales de A tales que I_i, I_j son primos relativos si $i \neq j$. Entonces*

- *(i) $I_1 \cdots I_s$ es primo relativo a I_{s+1}, para $s = 1, \ldots, n-1$.*
- *(ii) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.*

Observación 1.17.7. *De la demostración del corolario 1.17.4 (ver [9], corolario 2.2, página 89) se obtiene que si I es un ideal de A que se factoriza en un producto $M_1^{a_1} \cdots M_s^{a_s}$ de ideales maximales (con $a_i > 0$, $\forall\, i = 1, \ldots, s$) entonces $\{M_1, \ldots M_s\}$ es el conjunto de todos los ideales maximales de A que contienen a I. En particular, todo ideal maximal de A que contenga a I aparece en la factorización de I.*

La demostración de la siguiente proposición usa, entre otras cosas, los lemas 1.17.1, 1.17.5 y 1.17.6 así como el corolario 1.17.4.

Proposición 1.17.8. *Sea A un dominio noetheriano de dimensión 1. Entonces son equivalentes:*

- *(i) A tiene la propiedad de factorización única de ideales.*
- *(ii) A_M tiene la propiedad de factorización única de ideales, para todo $M \in \mathrm{Max}(A)$.*

En la demostració de la siguiente proposición se usan, entre otras cosas, los resultados 1.2.7, 1.2.12, 1.14.2 y 1.17.4.

Proposición 1.17.9. *Sea A un dominio noetheriano local de dimensión 1, con ideal maximal M. Entonces son equivalentes:*

- *(i) A tiene la propiedad de factorización única de ideales.*
- *(ii) A es un dominio de ideales principales.*
- *(iii) A es enteramente cerrado.*

El teorema siguiente usa en su demostración el corolario 1.15.8 y las proposiciones 1.17.8 y 1.17.9.

Teorema 1.17.10. *Sea A un dominio noetheriano de dimensión 1. Entonces son equivalentes:*

- *(i) A es dominio de Dedekind.*
- *(ii) A tiene la propiedad de factorización única de ideales.*

En general, se puede probar que A es un dominio de Dedekind si y sólo si todo ideal de A es un producto de ideales primos (ver [9], página 93).

Definición 1.17.11. *Sea A un dominio de Dedekind. Si I es cualquier ideal no trivial de A y P es cualquier ideal maximal de A entonces decimos que P divide a I, y lo denotamos como $P \mid I$, si I puede ser factorizado en A como un producto de ideales de la forma $I = PJ$, para algún ideal J de A. Dados I y P, definimos el orden de I en P como el entero $\mathrm{ord}_P(I)$ obtenido como sigue: factorizamos $I = P_1^{a_1} \cdots P_s^{a_s}$. Entonces $\mathrm{ord}_P(I) := a_i$ si $P = P_i$, y $\mathrm{ord}_P(I) := 0$ si P no divide a I. Podemos escribir entonces*

$$I = \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(I)} = \prod_{P \mid I} P^{\mathrm{ord}_P(I)}$$

Se puede verificar que $\mathrm{ord}_P(I)$ es un invariante local de I, es decir, que depende únicamente de $IA_P \subseteq A_P$, lo cual se obtiene de $\mathrm{ord}_P(I) = \mathrm{ord}_{S^{-1}P}(S^{-1}I)$, $\forall\ S \subset A$ multiplicativo tal que $S \cap P = \emptyset$.

Notamos también que, dado un ideal primo de un anillo A, la función ord_P puede ser definida siempre y cuando A_P sea un dominio de Dedekind: si I es un ideal de A, ponemos $\mathrm{ord}_P(I) = \mathrm{ord}_{PA_P}(IA_P)$.

Mencionamos ahora otro teorema.

Teorema 1.17.12. *Sea A cualquier anillo conmutativo. Sean $I_1, \ldots, I_n$ n ideales de A. Supongamos que I_i, I_j son primos relativos si $i \neq j$. Sean $y_1, \ldots, y_n$ elementos de A. Entonces existe un elemento $y \in A$ tal que $y - y_j \in I_j$, para todo $j = 1, \ldots, n$.*

El siguiente corolario es consecuencia del teorema 1.17.12.

Corolario 1.17.13. *La función natural $f : A \to \prod_{i=1}^n A/I_i$ es suprayectivo, con kernel igual a $\prod_{i=1}^n I_i$. En particular, induce un isomorfismo de anillo $A/(I_1 \cdots I_n) \to \prod_{i=1}^n A/I_i$.*

Tenemos otra proposición.

Proposición 1.17.14. *Sea A un dominio de Dedekind. Entonces cualquier ideal de A puede ser generado por dos elementos.*

Finalmente, terminamos esta sección con una proposición importante que se usa en capítulos posteriores.

Proposición 1.17.15. *Sea A un dominio de dimensión 1 tal que tiene la propiedad de factorización única de ideales. Si $\mathrm{Max}(A)$ es un conjunto finito entonces A es un dominio de ideales principales.*

1.18. Índice de ramificación y grado residual

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo III, sección 3) y en [3](capítulo 9).

Sea A un dominio de Dedekind y sea K su campo de fracciones. Sea B la cerradura entera de A en una extensión finita L de K. Supondremos en esta sección que B es un A-módulo finitamente generado (y por tanto, que es un dominio de Dedekind. Por ejemplo, B es un A-módulo finitamente generado cuando la extensión L/K es separable (teorema 1.4.6). Sea P un ideal maximal de A. Se verá que el ideal PB generado por P en B nunca es igual al ideal trivial en B. Como B es un dominio de Dedekind, se obtiene que el ideal PB se factoriza en B como un producto $\prod_{i=1}^{s} M_i^{e_i}$ de ideales primos de B. También se revisará una fórmula que relaciona a los enteros e_i con el grado n de la extensión L/K.

Lema 1.18.1. *Sea A un dominio de Dedekind y K su campo de fracciones. Sea B la cerradura entera de A en una extensión finita L de K. Sea P un ideal maximal de A. Entonces $PB \neq B$.*

Entonces, por ser PB un ideal no trivial en el dominio de Dedekind B, podemos factorizar PB como un producto de ideales maximales

$$PB = M_1^{e_1} \cdots M_s^{e_s}, \text{ para algunos enteros positivos } e_1, \ldots, e_s$$

Llamamos al entero $e_{M_i/P} := e_i$ el índice de ramificación de M_i sobre P.

Notamos que $M_i \cap A = P$ para todo i (de la observación 1.17.7 se obtiene que M_i contiene en particular a P, por lo que $P \subseteq M_i \cap A$. Si se tuviera $M_i \cap A = A$ entonces $1 \in M_i$, implicando que $M_i = B$, lo cual es una contradicción. Por ser P maximal, se tiene $P = M_i \cap A$). Por tanto, la inclusión $A \subseteq B$ induce las inyecciones

$$A/P \to B/M_i, \text{ para } i = 1, \ldots, s.$$

Como B es un A-módulo finitamente generado, el campo B/M_i es una extensión finita del campo A/P. Entonces sea $f_{M_i/P} := [B/M_i : A/P]$ ($f_{M_i/P}$ también se denota por f_i) la dimensión de B/M_i visto como un espacio vectorial sobre A/P.

Definición 1.18.2. *El campo A/P es el campo residual de A en P. El entero $f_{M_i/P}$ es el grado residual de M_i sobre P.*

Definición 1.18.3. *Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita, y sea B la cerradura entera de A en L. Supongamos que B es una A-módulo finitamente generado. Sea M cualquier ideal maximal de B. El ideal primo $P := M \cap A$ es maximal (observación 1.5.7). Llamamos al entero* $\mathrm{ord}_M(PB)$ *el índice de ramificación de M sobre P, y lo denotamos por $e_{M/P}$.*

Enunciamos el siguiente teorema importante en cuya demostración (ver [9] y [3]) se utiliza el lema 1.18.5. Este último lema también se usa en capítulos posteriores.

Teorema 1.18.4. *Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita. Sea B la cerradura entera de A en L. Si B es un A-módulo finitamente generado entonces*

$$[L : K] = \sum_{M|PB} e_{M/P} f_{M/P}$$

Lema 1.18.5. *Sea A un anillo conmutativo, y sea $P \subseteq A$ un ideal maximal. Sea $S \subseteq A \setminus P$ un conjunto multiplicativo. Entonces los campos A/P y $S^{-1}A/S^{-1}P$ son isomorfos.*

1.19. Primos ramificados y no ramificados

En esta sección revisamos en su mayoría solamente definiciones y hacemos algunos comentarios (ver [9], capítulo III, sección 5).

Definición 1.19.1. *Sea A un dominio de Dedekind con campo de fracciones K y L/K una extensión finita, y sea B la cerradura entera de A en L. Supongamos que B es una A-módulo finitamente generado. Consideramos M un ideal maximal de B y $P := M \cap A$. El ideal M es ramificado sobre P (o sobre A) si $e_{M/P} > 1$ o si la extensión B/M es no separable sobre A/P. De lo contrario, decimos que el ideal M es no ramificado sobre P (o sobre A).*

Además, un ideal maximal P de A ramifica en B si PB está contenido en un ideal maximal M de B el cual es ramificado sobre A. Cuando ningún ideal maximal de B es ramificado sobre A, decimos que la extensión B/A es no ramificada.

Si tomamos B y A como en la definición anterior, se obtiene que un ideal maximal M de B es no ramificado sobre P si y sólo si $PB_M = MB_M$ y B/M es separable sobre A/P.

Se puede generalizar más la definición anterior.

Definición 1.19.2. *Sea $\varphi : A \to B$ un homomorfismo de anillos y $\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ la función asociada. Consideramos $M \in \mathrm{Spec}(B)$ y $P := \varphi^{-1}(M) = \mathrm{Spec}(\varphi)(M)$. Decimos que M es un punto de ramificación de la función $\mathrm{Spec}(\varphi)$, o que la función $\mathrm{Spec}(\varphi)$ es ramificada en M, si $\varphi(P)$ no genera a MB_M, o si B_M/MB_M no es extensión separable de A_P/PA_P. De lo contrario, decimos que $\mathrm{Spec}(\varphi)$ no es ramificado en M, y que M es un punto no ramificado. El conjunto de puntos en $\mathrm{Spec}(B)$ donde $\mathrm{Spec}(\varphi)$ es ramificado se le llama el ramification locus de $\mathrm{Spec}(\varphi)$. La imagen en $\mathrm{Spec}(A)$ del ramification locus se le llama el branch locus de $\mathrm{Spec}(\varphi)$. Si el branch locus es vacío entonces decimos que la función $\mathrm{Spec}(\varphi)$ es no ramificada.*

Sea $f, g \in \overline{k}[x, y]$ dos polinomios irreducibles y $\pi : Z_f(\overline{k}) \to Z_g(\overline{k})$ un morfismo de curvas. Recordamos que este morfismo viene inducido por un homomorfismo de $\overline{k}$-álgebras $\pi^* : C_g \to C_f$. Recordamos también que π puede ser identificado con la función $\mathrm{Spec}(\pi^*)|_{\mathrm{Max}(C_f)} : \mathrm{Max}(C_f) \to \mathrm{Max}(C_g)$, que manda M a $(\pi^*)^{-1}(M)$. Con esta notación, tenemos la siguiente definición:

Definición 1.19.3. *Decimos que π es no ramificado en (a, b) si la función $\mathrm{Spec}(\pi^*)$ es no ramificado en $(x - a, y - b)$.*

Como C_f es un dominio, $\mathrm{Ker}(\pi^*)$ es un ideal primo de C_g. Como C_g es un dominio de dimensión 1 entonces $\mathrm{Ker}(\pi^*)$ es maximal (en cuyo caso el morfismo π es constante), o $\mathrm{Ker}(\pi^*) = (0)$. Supongamos que π^* es inyectivo, y pensamos al anillo C_g como un subanillo de C_f (notamos que la extensión C_f/C_g no es necesariamente entera). Entonces se puede definir el índice de ramificación de un punto no singular (a, b) de $Z_f(\overline{k})$ sobre $\pi(a, b)$ como sigue:

Sea M el ideal maximal de C_f correspondiente a (a, b). Entonces $(C_f)_M$ es un dominio de ideales principales, y la función $\mathrm{ord}_{M(C_f)_M}$ está definida. Sea P es ideal maximal de C_g correspondiente a $\pi(a, b)$. Como π^* es inyectivo, se tiene que $P(C_f)_M \neq (0)$. Con toda esta notación, terminamos entonces esta sección con la siguiente definición.

Definición 1.19.4. *El índice de ramificación $e_{(a,b)/\pi(a,b)}$ de (a, b) sobre $\pi(a, b)$ es el entero $e_{M/P} := \mathrm{ord}_{M(C_f)_M}(P(C_f)_M)$. Si $e_{(a,b)/\pi(a,b)} > 1$ entonces (a, b) es un punto de ramificación de la función de la función π, y π es ramificado en (a, b).*

1.20. Extensiones de campos constantes

En esta sección mencionamos solamente una proposición que será de utilidad después. La demostración puede encontrarse en [9], proposición 7.15 de la página 115.

Sea k cualquier campo, $K/k(x)$ cualquier extensión finita y A un dominio de Dedekind con campos de fracciones K. Supongamos que k está contenido en A. Consideramos $\overline{K}$ una cerradura algebraica de K y $\overline{k} \subseteq \overline{K}$ el conjunto de elementos de $\overline{K}$ que son algebraicos sobre k. El conjunto $\overline{k}$ es un subcampo algebraicamente cerrado de $\overline{K}$, y en particular, es una cerradura algebraica de k. Si $E \subseteq \overline{K}$ es cualquier extensión de k entonces denotamos por EK al subcampo de $\overline{K}$ generado por E y K. En particular, si $E = k(\alpha_1, \ldots, \alpha_s)$ entonces $EK = K(\alpha_1, \ldots, \alpha_s)$. Si suponemos que E/k es una extensión finita, entonces EK/K es una extensión finita, y a la extensión EK/K se le llama una extensión de campos constante. Si tomamos B la cerradura entera de A en EK entonces tenemos la siguiente proposición que nos servirá después (ver por ejemplo la proposición 2.6.7).

Proposición 1.20.1. *Sea E/k una extensión finita separable. Entonces*

- *(i) Si $E = k(\alpha)$ entonces $B = EA = A[\alpha]$.*
- *(ii) La extensión B/A es no ramificada.*

1.21. Extensiones de Galois

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo III, sección 8).

Sea A un dominio de Dedekind con campo de fracciones K y L/K una extensión finita de Galois, con grupo de Galois $G = \mathrm{Gal}(L/K)$. Tomamos B la cerradura entera de A en L. De la proposición 1.2.15 se obtiene que $\sigma(B) = B$ para todo $\sigma \in G$. Consideramos la función natural $\pi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$, con $M \mapsto M \cap A$, asociado a la extensión B/A. Consideramos $P \in \mathrm{Spec}(A)$ y $\pi^{-1}(P) := \{M_1, \ldots, M_s\}$, y sea $M_i \in \pi^{-1}(P)$. Como $\sigma(P) = P$, se obtiene que $\sigma(M_i) \in \pi^{-1}(P)$, y con esta notación tenemos entonces la siguiente proposición que usaremos después (ver por ejemplo la proposición 2.6.4).

Proposición 1.21.1. *Sea $P \in \mathrm{Max}(A)$. Sean M_i y M_j dos ideales maximales en $\pi^{-1}(P)$. Entonces existe $\sigma \in G$ tal que $\sigma(M_i) = M_j$. Más aún, $e_{M_1/P} = \cdots = e_{M_s/P} = e$ y $f_{M_1/P} = \cdots = f_{M_s/P} = f$. En particular,*

$$PB = (M_1 \ldots M_s)^e, \text{ con } efs = [L : K].$$

Sea L/K una extensión de Galois. Sean A y B como antes y $G := \mathrm{Gal}(L/K)$. El grupo G actúa sobre $\mathrm{Max}(B)$ como sigue: $\sigma \cdot M := \sigma(M)$, $\forall\ \sigma \in G$, $M \in \mathrm{Max}(B)$. Tomamos $P = M \cap A$. Denotamos al estabilizador del elemento M bajo esta acción de G como el grupo $D_{M/P} := \{\sigma \in G \mid \sigma(M) = M\}$.

Al grupo $D_{M/P}$ se le llama el grupo de descomposición de M, y notamos entonces que la proposición 1.21.1 prueba que la acción de G sobre $\pi^{-1}(P)$ es transitivo. Por tanto, si $\pi^{-1}(P) = \{M_1, \ldots, M_s\}$ entonces

$$|G/D_{M/P}| = |\text{orbita de } M| = s$$

En particular, $|D_{M/P}| = e_{M/P} f_{M/P}$. Además, la transitividad de la acción de G sobre $\{M_1, \ldots, M_s\}$ también prueba que

$$\prod_{\sigma \in G} \sigma(M) = (M_1 \cdots M_s)^{|D_{M/P}|} = PB^{f_{M/P}}$$

(ver [9], capítulo 3, sección 8).

Cada automorfismo $\sigma : B \to B$ en $D_{M/P}$ induce una función natural

$$\overline{\sigma} : B/M \to B/\sigma(M) = B/M$$

Notamos que la función $\overline{\sigma}$ se restringe a la función identidad sobre A/P ($A/P \hookrightarrow B/M$), y consideramos $\mathcal{G}$ el grupo de Galois de la extensión B/M sobre A/P. La función $\sigma \mapsto \overline{\sigma}$, de $D_{M/P} \to \mathcal{G}$, es un homomorfismo de grupos que está bien definido. El kernel de esta función es el grupo

$$I_{M/P} := \{\sigma \in D_{M/P} \mid \forall\ b \in B, \sigma(b) \equiv b \pmod{M}\}$$

Al grupo $I_{M/P}$ se le llama el grupo de inercia en M, y notamos que como $I_{M/P}$ es el kernel entonces es un subgrupo normal de $D_{M/P}$y se obtiene que $|D_{M/P}/I_{M/P}| \leq |\mathcal{G}| \leq |B/M : A/P| = f_{M/P}$. Del lema a continuación, se obtiene además que cuando B/M es separable sobre A/P entonces

$$|D_{M/P}/I_{M/P}| = f_{M/P}$$

o, equivalentemente, que la función $D_{M/P} \to \mathcal{G}$ es suprayectiva. Esto implica que $|I_{M/P}| = e_{M/P}$ ya que

$$|I_{M/P}| \cdot |D_{M/P}/I_{M/P}| \cdot |G/D_{M/P}| = |G| = e_{M/P} \cdot f_{M/P} \cdot s.$$

Mencionamos entonces dicho lema para concluir esta sección.

Lema 1.21.2. *Supongamos que la extensión de campos residuales B/M sobre A/P es separable. Entonces es una extensión de Galois de grado $f_{M/P}$, y la función $D_{M/P} \to \mathcal{G}$ es suprayectiva. En particular, M es ramificado sobre A si y sólo si $I_{M/P} \neq \{\mathrm{Id}\}$.*

1.22. El discriminante como una norma

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo IV, sección 2).

Sea F un campo y R una F-algebra de dimensión n. Tomamos $r \in R$, y consideramos $\mu_r : R \to R$, con $x \mapsto \mu_r(x) := rx$, llamada la función 'multiplicación por r'. La función μ_r es un homomorfismo de F-espacios vectoriales. Llamamos a

$$\begin{aligned} \mathrm{Norm}_{R/F} : R &\to F \\ r &\mapsto \det(\mu_r) \end{aligned}$$

la función norma de R a F. Es multiplicativa:

$$\forall\, r, s \in R,\ \mathrm{Norm}_{R/F}(rs) = \mathrm{Norm}_{R/F}(r) \cdot \mathrm{Norm}_{R/F}(s)$$

Similarmente, llamamos a

$$\begin{aligned} \mathrm{Tr}_{R/F} : R &\to F \\ r &\mapsto \mathrm{Traza}(\mu_r) \end{aligned}$$

la función traza de R a F. Es aditiva:

$$\forall\, r, s \in R,\ \mathrm{Tr}_{R/F}(r+s) = \mathrm{Tr}_{R/F}(r) + \mathrm{Tr}_{R/F}(s)$$

Cuando R es un campo, denotamos a la función $\mathrm{Norm}_{R/F}$ por $N_{R/F}$. También, denotamos por $\mathrm{char}_r(y) \in F[y]$ al polinomio característico de μ_r

$$\mathrm{char}_r(y) = y^n - \mathrm{Tr}_{R/F}(r)y^{n-1} + \cdots + (-1)^n \mathrm{Norm}_{R/F}(r)$$

Tenemos el siguiente lema.

Lema 1.22.1. *Sea R una F-álgebra de dimensión s, y tomamos $\alpha \in R$. Consideramos $F[\alpha]$ la F-subálgebra más chica de R que contiene a α, y sea $f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in F[y]$ el polinomio mínimo de α sobre F (por lo que $F[\alpha] \cong F[y]/(f(y))$). Supongamos que el $F[\alpha]$-módulo R es libre de rango $[R : F[\alpha]]$. Entonces*

- *(i)* $\mathrm{Tr}_{R/F}(\alpha) = -[R : F[\alpha]]a_{n-1} = [R : F[\alpha]] \cdot \mathrm{Tr}_{F[\alpha]/F}(\alpha)$.
- *(ii)* $\mathrm{Norm}_{R/F}(\alpha) = ((-1)a_0)^{[R:F[\alpha]]} = (\mathrm{Norm}_{F[\alpha]/F}(\alpha))^{[R:F[\alpha]]}$.

Una consecuencia del lema 1.22.1 es el siguiente corolario.

Corolario 1.22.2. *Sea A un dominio enteramente cerrado en su campo de fracciones K. Sea L/K una extensión finita. Si $\alpha \in L$ es entero sobre A entonces* $\mathrm{Norm}_{L/K}(\alpha)$ *y* $\mathrm{Tr}_{L/K}(\alpha)$ *pertenecen a A.*

Mencionamos otro lema.

Lema 1.22.3. *Sea L/K una extensión separable y finita de grado s. Sean $\sigma_1, \ldots, \sigma_s$ los s distintos encajes de L en una cerradura algebraica de K. Entonces*

- *(i)* $\forall\ a \in L$, $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{s} \sigma_i(\alpha)$.
- *(ii)* $\forall\ a \in L$, $\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{s} \sigma_i(\alpha)$.

El siguiente teorema establece la transitividad de la norma y la traza.

Teorema 1.22.4. *Sean M/L y L/K dos extensiones finitas de campos. Entonces, $\forall\ \alpha \in M$,*

- *(i)* $N_{L/K}(N_{M/L}(\alpha)) = N_{M/K}(\alpha)$.
- *(ii)* $\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)) = \mathrm{Tr}_{M/K}(\alpha)$.

Mencionamos otra proposición.

Proposición 1.22.5. *Sea K cualquier campo y $f(y)$ un polinomio mónico en $K[y]$. Sea L la K-álgebra $K[y]/(f(y))$ y α la clase de y en L. Tomamos $g(y) \in K[y]$ cualquier polinomio. Entonces*

$$\mathrm{Res}(f(y), g(y)) = \mathrm{Norm}_{L/K}(g(\alpha)).$$

En particular, $\mathrm{disc}(f) = \mathrm{Norm}_{L/K}(f'(\alpha))$.

El siguiente lema nos da algunas propiedades del resultante.

Lema 1.22.6. *Sea A cualquier dominio conmutativo y $a \in A \setminus \{0\}$. Sean $f(y)$ y $g(y)$ dos polinomios en $A[y]$. Entonces*

- *(i)* $\mathrm{Res}(af, g) = a^{\deg(g)}\mathrm{Res}(f, g)$.
- *(ii)* $\mathrm{Res}(f, g) = (-1)^{\deg(f)\deg(g)}\mathrm{Res}(g, f)$.
- *(iii)* $\mathrm{Res}(f, y - a) = a^{\deg(f)} f(a)$.

Un corolario de 1.22.5 es el siguiente.

Corolario 1.22.7. *Sea K cualquier campo. Sean $f(y), g(y), h(y)$ tres polinomios en $K[y]$. Entonces* $\mathrm{Res}(f, gh) = \mathrm{Res}(f, g)\mathrm{Res}(f, h)$.

Utilizando el lema 1.22.6 y el corolario 1.22.7 obtenemos otro corolario.

Corolario 1.22.8. *Sea $\overline{K}$ una cerradura algebraica de K. Sean $f, g \in \overline{K}[y]$ dos polinomios de grado positivo con factorizaciones $f(y) := a_n \prod_{i=1}^{n}(y - \alpha_i)$ y $g(y) := b_m \prod_{j=1}^{m}(y - \beta_j)$. Entonces* $\mathrm{Res}(f, g) = (a_n)^m (b_m)^n \prod_{i,j}(\alpha_i - \beta_j)$.

Observación 1.22.9. *Sea A un dominio con campo de fracciones A. Sabemos que si A es factorial entonces* $\mathrm{Res}(f,g) = 0$ *si y sólo si $f(y)$ y $g(y)$ tienen un factor en común. El corolario 1.22.8 nos dice que, aún cuando A no es factorial,* $\mathrm{Res}(f,g) = 0$ *si y sólo si $f(y)$ y $g(y)$ tienen una raíz en común.*

Concluimos con un último corolario.

Corolario 1.22.10. *Sea $f(y)$ un polinomio mónico irreducible de grado $n > 0$ en $K[y]$. Factorizamos a $f(y)$ en $\overline{K}[y]$ como $f(y) = \prod_{i=1}^{n}(y - \alpha_i)$. Entonces* $\mathrm{disc}(f) = \prod_{i \neq j}(\alpha_i - \alpha_j)$.

1.23. El discriminante de una base

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo IV, sección 3).

Sea R una F-álgebra de dimensión finita, y consideramos la función

$$\mathrm{Tr} : R \times R \to F$$

$$(x, y) \mapsto \mathrm{Tr}_{R/F}(xy)$$

La función Tr es una forma F-bilineal. Tomamos $e_1, \ldots, e_n$ una base para R sobre F y denotamos por

$$T_{\{e_1,\ldots,e_n\}} := (\mathrm{Tr}_{R/F}(e_i e_j))_{1 \leq i,j \leq n}$$

a la matriz que representa a la función Tr con respecto a la base $\{e_1, \ldots, e_n\}$. Si $\{f_i\}_{i=1}^{n}$ es otra base para R sobre F entonces tomamos la matriz C que expresa a la base $\{f_i\}$ en términos de la base $\{e_i\}$. Sea C^t la traspuesta de C. Entonces

$$T_{\{f_1,\ldots,f_n\}} = C^t T_{\{e_1,\ldots,e_n\}} C$$

En particular, $\det(T_{\{e_1,\ldots,e_n\}})$ y $\det(T_{\{f_1,\ldots,f_n\}})$ difieren únicamente por un cuadrado en F, a saber, $\det(C)^2 \neq 0$. Se obtiene entonces que $\det(T_{\{e_1,\ldots,e_n\}}) = 0$ si y sólo si $\det(T_{\{f_1,\ldots,f_n\}}) = 0$.

Denotamos por $(F^*)^2$ al subgrupo de F^* que consiste de los cuadrados en F^* (notamos que los cuadrados en F^* no son un subgrupo del grupo aditivo F a menos que $\mathrm{char}(F) = 2$). Damos entonces la siguiente definición.

Definición 1.23.1. *El discriminante de la función* Tr *es igual a cero si*

$$\det(T_{\{e_1,\ldots,e_n\}}) = 0$$

De lo contrario, el discriminante de Tr *es igual a la clase del determinante de $T_{\{e_1,\ldots,e_n\}}$ en $F^*/(F^*)^2$.*

Tenemos la siguiente proposición.

Proposición 1.23.2. *Sea L/K una extensión separable y finita de grado n y sean $\sigma_1, \ldots, \sigma_n$ los n distintos encajes de L en una cerradura algebraica $\overline{K}$ de K. Entonces*

- *(i) Si tomamos $\alpha_1, \ldots, \alpha_n$ una base para L/K y consideramos $M := (\sigma_i(\alpha_j))_{1 \leq i,j \leq n}$ entonces*

$$T_{\{\alpha_1,\ldots,\alpha_n\}} := (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{1 \leq i,j \leq n} = M^t M$$

- *(ii) Si $L = K(\alpha)$ para algún $\alpha \in L$ con polinomio mínimo $f(y) \in K[y]$ de grado n, entonces*

$$\mathrm{disc}(f) = N_{L/K}(f'(\alpha)) = (-1)^{n(n-1)/2}\det(T_{\{1,\alpha,\ldots,\alpha^{n-1}\}})$$

Utilizando la proposición 1.23.2 puede probarse la siguiente proposición (ver la bibliografía mencionada al principio de esta sección).

Proposición 1.23.3. *Sea L/K una extensión finita de campos. Entonces L/K es separable si y sólo si el discriminante de la función $\mathrm{Tr} : L \times L \to K$ no es igual a cero.*

Tenemos la siguiente definición.

Definición 1.23.4. *Sea A un dominio enteramente cerrado en su campo de fracciones K y L/K una extensión finita de grado n. Tomamos B la cerradura entera de A en L. Sean $\alpha_1, \ldots, \alpha_n \in L$. El discriminante del conjunto $\{\alpha_1, \ldots, \alpha_n\}$ se define como*

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) := \det(T_{\{\alpha_1,\ldots,\alpha_n\}})$$

Si $\alpha_1, \ldots, \alpha_n \in B$ entonces $\alpha_i\alpha_j \in B$, $\forall i, j$, y $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \in A$. En particular, si $\{\alpha_1, \ldots, \alpha_n\}$ es una base para L/K contenida en B entonces se obtiene que $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in A$, y su clase en $K^*/(K^*)^2$ es igual al discriminante de la función $\mathrm{Tr} : L \times L \to K$.

Cuando $L = K(\alpha)$ con $\alpha \in B$, y $f(y)$ es el polinomio mínimo de α, de las proposiciones 1.23.2 y 1.23.3 se obtiene que

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2}\mathrm{disc}(f)$$

Esta descripción del discriminante de un polinomio se puede usar para dar una condición suficiente para que $A[\alpha]$ sea igual a B. Dicha condición se da en el siguiente lema (ver [9], capítulo 4, sección 3) con el que terminamos esta sección.

Lema 1.23.5. *Sea A un dominio de ideales principales con campo de fracciones K, L/K una extensión separable y finita de grado n y B la cerradura entera de A en L. Sea $b_1, \ldots, b_n \in B$ una base para L/K. Si* $\operatorname{disc}(b_1, \ldots, b_n)$ *es un elemento libre de cuadrados de A entonces $\{b_1, \ldots, b_n\}$ es una base para B sobre A. En particular, supongamos que $L = K(\alpha)$ para algún $\alpha \in B$, y sea $f(y)$ el polinomio mínimo de α sobre K. Si* $\operatorname{disc}(f)$ *es un elemento libre de cuadrados de A entonces $A[\alpha] = B$.*

1.24. El ideal discriminante

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo IV, sección 5).

Empezamos con la siguiente definición.

Definición 1.24.1. *Sea A un dominio de Dedekind con campo de fracciones K y L/K una extensión finita, y sea B la cerradura entera de A en L. Sea $d_{B/A}$ el ideal de B generado por los elementos de la forma $f'(\alpha)$, donde α es tal que $\alpha \in B$ y $L = K(\alpha)$, y $f(y)$ es el polinomio mínimo de α sobre A. Si L/K no es una extensión simple entonces definimos $d_{B/A} := (0)$. Al ideal $d_{B/A}$ se le llama el ideal diferencial de B/A. Sea $\delta_{B/A}$ el ideal de A generado por los elementos de la forma* $\operatorname{disc}(f)$*, donde f es el polinomio mínimo sobre A de un elemento $\alpha \in B$ tal que $L = K(\alpha)$. Si L/K no es una extensión simple entonces definimos $\delta_{B/A} := (0)$.*

Notamos que $d_{B/A}$ y $\delta_{B/A}$ no dependen del elemento primitivo elegido para describir a la extensión L/K. Ambos ideales son nulos si la extensión L/K no es separable.

Tenemos la siguiente proposición.

Proposición 1.24.2. *Sea A un dominio de Dedekind con campo de fracciones K y L/K una extensión separable y finita. Tomamos B la cerradura entera de A en L. Entonces*

- *(i) Si $M \in \operatorname{Max}(B)$ y es ramificado sobre A entonces $d_{B/A} \subseteq M$.*
- *(ii) Si $P \in \operatorname{Max}(A)$ y ramifica en B entonces $\delta_{B/A} \subseteq P$.*

En particular, hay únicamente un número finito de ideales maximales de A que ramifican en B.

Veamos ahora la siguiente definición.

Definición 1.24.3. *Sea A un dominio enteramente cerrado en su campo de fracciones K y L/K un extensión finita de grado n. Tomamos B la cerradura entera de A en L. El ideal discriminante $\Delta_{B/A}$ es el ideal de A generado por*

los elementos de la forma $\mathrm{disc}(b_1, \ldots, b_n)$*, donde los conjuntos* $\{b_1, \ldots, b_n\}$ *se toman sobre todas las bases de* L *sobre* K *que están contenidas en* B*.*

Recordamos que $\delta_{B/A}$ es el ideal de A generado por los elementos de la forma $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$, donde α se toma sobre todos los elementos de B tales que $L = K(\alpha)$. Notamos que $\delta_{B/A} \subseteq \Delta_{B/A}$. Cuando $B = A[\alpha]$ para algún $\alpha \in B$, y $f(y)$ es el polinomio mínimo de α sobre A entonces

$$\delta_{B/A} = \Delta_{B/A} = \mathrm{disc}(f)A$$

Más en general, $\Delta_{B/A} = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)A$ si $\{\alpha_1, \ldots, \alpha_n\}$ es una base para B sobre A.

Tenemos el siguiente teorema.

Teorema 1.24.4. *Sea* A *un dominio de Dedekind con campo de fracciones* K *y* L/K *una extensión finita. Consideramos* B *la cerradura entera de* A *en* L*. Supongamos que* B *es un* A*-módulo finitamente generado. Entonces* $P \in \mathrm{Max}(A)$ *ramifica en* B *si y sólo si* $\Delta_{B/A} \subseteq P$*.*

En la demostración del teorema 1.24.4 se usan, entre otras cosas, los siguientes tres lemas:

Lema 1.24.5. *Sea* R *una* F*-álgebra conmutativa de dimensión* n*. Supongamos que* R *contiene a un elemento nilpotente distinto de cero* r*. Entonces el discriminante de la función* $\mathrm{Tr} : R \times R \to F$ *es igual a cero.*

Lema 1.24.6. *Sea* S *cualquier subconjunto multiplicativo de* A*. Entonces*

$$\Delta_{S^{-1}B/S^{-1}A} = S^{-1}\Delta_{B/A}$$

Lema 1.24.7. *Sea* $P \in \mathrm{Max}(A)$*. Sea* $S = A \setminus P$*. Entonces* P *ramifica en* B *si y sólo si* $PA_P \subset A_P$ *ramifica en* $S^{-1}B$*.*

Terminamos con una observación.

Observación 1.24.8. *Si* L/K *es no separable entonces de la proposición 1.23.3 se obtiene que el discriminante de la función* $\mathrm{Tr} : L \times L \to K$ *es igual a cero. En este caso,* $\Delta_{B/A} = (0)$*. Del teorema 1.24.4, se obtiene que todo ideal de* A *ramifica en* B*.*

1.25. La función norma sobre ideales

Las observaciones y los resultados de esta sección junto con sus correspondientes demostraciones se pueden encontrar en [9] (capítulo IV, sección 6).

Sea A un dominio de Dedekind con campo de fracciones K y L/K una extensión finita, y sea B la cerradura entera de A en L. Denotamos a estos cuatro elementos por (A, K, B, L). Consideramos a la función norma $N_{L/K} : L \to K$. Queremos definir una función

$$N_{B/A} : I_B := \{\text{ideales de } B\} \to I_A := \{\text{ideales de } A\}$$

tal que, cuando L/K es separable, cumpla que, $\forall\, \alpha \in B$, $N_{B/A}(\alpha B) := N_{L/K}(\alpha)A$.

Para motivar la definición de $N_{B/A}$, supongamos que la extensión L/K es Galois, con grupo de Galois $G = \{\sigma_1, \ldots, \sigma_n\}$. Del lema 1.22.3 se tiene que $N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$. Esto sugiere definir, para un ideal I de B, a la función $N_{B/A}$ como sigue:

$$N_{B/A}(I) := (\prod_{i=1}^{n} \sigma_i(I)) \cap A$$

Tenemos la siguiente proposición.

Proposición 1.25.1. *Sea L/K una extensión de Galois. Sea $\alpha \in B$. Entonces $N_{B/A}(\alpha B) := N_{L/K}(\alpha)A$.*

Tenemos el siguiente lema y una observación con respecto a dicho lema.

Lema 1.25.2. *Sea (A,K,B,L) como antes. Sea $J \subseteq A$ un ideal. Entonces $J = JB \cap A$. Más aún, la función $i_{B/A} : I_A \to I_B$, con $J \mapsto JB$, es inyectiva.*

Observación 1.25.3. *Sea $a \in A \setminus \{0\}$. Si se tiene un ideal de la forma $I = (aA)$, se puede verificar que $(IB) \cap A = I$ sin usar el lema anterior. Para verlo, notamos que $(aA) \subseteq (aB) \cap A$. Recíprocamente, si $c = ab \in (aB) \cap A$ entonces $b = c/a \in K$. Como A es enteramente cerrado, se tiene $K \cap B = A$, por lo que $b \in A$. Por tanto, $c \in aA$. Utilizando localizaciones de $J \subseteq JB \cap A$ y el argumento anterior, se puede probar el lema anterior.*

Mencionamos otro lema.

Lema 1.25.4. *Sea (A, K, B, L) como antes, y tal que L/K es Galois de grado n. Sea $\mathcal{B}$ un ideal maximal de B y $P := \mathcal{B} \cap A$. Entonces $N_{B/A}(\mathcal{B}) = P^{f_{\mathcal{B}/P}}$.*

Consideramos otra proposición.

Proposición 1.25.5. *Sea (A, K, B, L) como antes, y tal que L/K es Galois. Sea $I = \mathcal{B}_1^{a_1} \dots \mathcal{B}_1^{a_1}$ un producto de ideales maximales de B. Entonces*

$$N_{B/A}(I) = \prod_{i=1}^{r} N_{B/A}(\mathcal{B}_i)^{a_i}$$

En particular, $\forall\ I, J \in I_B$, $N_{B/A}(IJ) = N_{B/A}(I) \cdot N_{B/A}(J)$.

Sea (A, K, B, L) como antes. Si L/K no es Galois, la proposición 1.25.5 sugiere definir la función norma de ideales $N_{B/A} : I_B \to I_A$ como sigue:

- (i) Si $\mathcal{B} \in \mathrm{Max}(B)$ entonces $N_{B/A}(\mathcal{B}) := (\mathcal{B} \cap_A)^{f_{\mathcal{B}/\mathcal{B}\cap A}}$.
- (ii) $N_{B/A}(\mathcal{B}_1^{a_1} \cdots \mathcal{B}_r^{a_r}) := \prod_{i=1}^{r} N_{B/A}(\mathcal{B}_i)^{a_i}$.
- (iii) $N_{B/A}(B) := A$ y $N_{B/A}((0)) := (0)$.

Notamos entonces que la función $N_{B/A} : I_B \to I_A$ (también llamada función norma) es multiplicativa.

Con la definición de la función norma de ideales, tenemos los siguientes dos lemas.

Lema 1.25.6. *Sea (A, K, B, L) como antes, y sea n el grado de la extensión L/K. Entonces la composición $N_{B/A} \circ i_{B/A} : I_A \to I_A$ es la función que manda a un ideal de I_A a su n-ésima potencia.*

Lema 1.25.7. *Sean M/L y L/K dos extensiones finitas de campos. Supongamos que tenemos un dominio de Dedekind A cuyo campo de fracciones sea K. Tomamos B (respectivamente, C) la cerradura entera de A en L (respectivamente, en M). Supongamos que B y C son A-módulos finitamente generados. Entonces $N_{C/A} = N_{B/A} \circ N_{C/B}$.*

Finalmente, terminamos esta sección con una proposición y un teorema.

Proposición 1.25.8. *Sea (A, K, B, L) como antes. Entonces $\forall\ \alpha \in B$ se cumple*

$$N_{L/K}(\alpha)A = N_{B/A}(\alpha B)$$

Teorema 1.25.9. *Sea (A, K, B, L) como antes. Supongamos que la extensión L/K es separable. Sea $M \in \mathrm{Max}(B)$, y sea $P := M \cap A$. Supongamos que la extensión de campos residuales B/M es separable sobre A/P. Entonces*

$$\mathrm{ord}_M(d_{B/A}) \geq e_{M/P} - 1$$

y se alcanza la igualdad si y sólo si la característica de A/P y el valor $e_{M/P}$ son primos relativos.

1.26. Lema de Gauss

Definición 1.26.1. *Sea A un dominio. Un elemento $a \neq 0$ es irreducible si no es unidad y si siempre que se pueda escribir $a = bc$, con $b, c \in A$, se tenga que b es unidad o c es unidad. Un elemento $a \neq 0$ tiene factorización única en elementos irreducibles si existe una unidad u y elementos irreducibles $p_1, \ldots, p_r$, tal que $a = up_1 \ldots p_r$, y si dadas dos factorizaciones $a = u\prod_{i=1}^{r} p_i = v\prod_{j=1}^{s} q_j$ en elementos irreducibles, debe ocurrir que $r = s$ y que después de alguna permutación de los índices se tenga $(p_i) = (q_i)$. Un anillo A es factorial si es dominio y si todo elemento no cero de A tiene una factorización única en elementos irreducibles.*

Sea A cualquier dominio factorial con campo de fracciones K. El contenido de un elemento $f \in K[x]$ es un elemento $\mathrm{cont}(f) \in K$, definido salvo multiplicación por una unidad $u \in A$, tal que $f(x) = \mathrm{cont}(f)f_1(x)$, donde $f_1(x) \in A[x]$ es tal que el maximo común divisor de sus coeficientes es 1. El polinomio $f_1(x)$ es único salvo multiplicación por una unidad en A, y se le llama un polinomio primitivo asociado a f.

Lema 1.26.2. *Sean f y g polinomios mónicos en $\mathbb{Q}[x]$. Si los coeficientes de f y g coeficientes no son todos enteros entonces los coeficientes del producto fg tampoco son todos enteros.*

Lema 1.26.3. *Sea A un dominio factorial con campo de fracciones K. Sean $f, g \in K[x]$. Entonces el contenido de fg es el producto del contenido de f por el contenido de g.*

Corolario 1.26.4. *Supongamos que $f(x) \in A[x]$ se factoriza en $K[x]$ como $f(x) = g(x)h(x)$, con $g, h \in K[x]$. Escribimos $g(x) = \mathrm{cont}(g)g_1(x)$ y $h(x) = \mathrm{cont}(h)h_1(x)$, con $g_1(x), h_1(x) \in A[x]$. Entonces $f(x) = \mathrm{cont}(f)g_1(x)h_1(x)$ es una factorización de $f(x)$ en $A[x]$.*

1.27. Extensiones infinitas de Galois

Sea E/k una extensión contenida en $\overline{k}$, y sea G su grupo de Galois. Sea F/k cualquier extensión de k contenida en E. Sea $\mathrm{Hom}_k(F, E)$ el conjunto de encajes de k-álgebras $F \to E$. Sea i_0 la inclusión de F en E. Entonces el grupo G actúa naturalmente sobre el conjunto $\mathrm{Hom}_k(F, E)$ como sigue: $\forall\ \sigma \in G$, $\forall\ i \in \mathrm{Hom}(F, E)$, sea $\sigma \cdot i = \sigma \circ i$. Se obtiene que el subgrupo $\mathrm{Gal}(E/F)$ es el estabilizador del elemento i_0 bajo esta acción de G.

Proposición 1.27.1. *Sea E/k una extensión normal. Sea $\mu : F \to E$ un homomorfismo de k-álgebras. Entonces existe un automorfismo de k-álgebras $\overline{\mu} : E \to E$ tal que $\overline{\mu}|_F = \mu$.*

Corolario 1.27.2. *Sea F/k una extensión finita de Galois contenida en E, y sea G_F el grupo* $\mathrm{Gal}(F/k)$. *Entonces la restricción natural $G \to G_F$ es suprayectiva.*

Corolario 1.27.3. *La acción de G sobre* $\mathrm{Hom}_k(F, E)$ *es transitiva.*

Se obtiene que el conjunto cociente $G/\mathrm{Gal}(E/F)$ está en biyección con $\mathrm{Hom}_k(F, E)$. Una extensión separable F/k es finita si y sólo si $\mathrm{Hom}_k(F/E)$ es un conjunto finito. Cuando F/k es separable entonces $\mathrm{Hom}_k(F, E)$ es un conjunto finito de orden $[F : k]$.

Lema 1.27.4. *Sea E/k cualquier extensión finita de Galois de k en $\overline{k}$. Sea F/k cualquier extensión finita contenida en E. Sea $H = \mathrm{Gal}(E/F)$. Entonces $F = E^H$.*

Por el teorema fundamental de teoría de Galois, existe un biyección entre los subcampos de una extensión finita de Galois E/k y los subgrupos del grupo de Galois G de dicha extensión. Pero aún cuando la extensión de Galois E/k no sea finita, es posible asociarle a un subgrupo H de G el subcampo E^H y asociarle a un subcampo F el subgrupo $\mathrm{Gal}(E/F)$. Pero a diferencia del teorema fundamental de teoría de Galois, cuando E/k es extensión infinita de Galois, la asignación $H \mapsto \overline{k}^H \mapsto \mathrm{Gal}(E/E^H)$ puede no ser inyectivo sobre el conjunto de subgrupos de G. Sin embargo, podemos dotar a G con una topología y probar que existe una biyección entre los subcampos de E y los subgrupos cerrados de G. En particular, se puede tomar el caso en que k es perfecto y $E = \overline{k}$.

Para definir la topología mencionada, tomamos cualquier extensión de Galois E/k de k contenida en $\overline{k}$ con grupo de Galois G. Sea I el conjunto de todas las extensiones finitas de Galois de k contenidas en E. Sean $M, M' \in I$ tal que $M \subseteq M'$, y sean G_M y $G_{M'}$ sus grupos de Galois respectivamente. Consideramos la restricción natural $G_{M'} \to G_M$ y la denotamos por $\mathrm{res}_{M',M}$, y consideramos el homomorfismo de grupos

$$\psi : G \longrightarrow \prod_{M \in I} G_M$$

$$\sigma \longmapsto \{\sigma_M\}_{M \in I} \quad \text{con} \quad \sigma_M := \mathrm{res}_{E,M}(\sigma)$$

Entonces ψ es inyectiva, ya que por ser E/k algebraico, un elemento α de E está contenido en una extensión finita de Galois F/k contenido en E, y si tenemos $\psi(\sigma) = \mathrm{Id}$ entonces en particular $\sigma_F = \mathrm{Id}_F$, es decir, $\sigma|_F = \mathrm{Id}_F$ y por tanto $\sigma(\alpha) = \alpha$, y se obtiene que $\sigma = \mathrm{Id}_G$.

Por otro lado, sea S el conjunto de todos los elementos $\{\sigma_M\}_{M\in I}$ en $\prod_{M\in I} G_M$ tales que $\forall\, M, N \in I$, se cumple que $\mathrm{res}_{M,M\cap N}(\sigma_M) = \mathrm{res}_{N,M\cap N}(\sigma_N)$. Entonces S es un subgrupo de $\prod_{M\in I} G_M$ y se cumple la siguiente proposición.

Proposición 1.27.5. *La imagen de ψ es igual a S.*

Identificando a G con $\psi(G)$, podemos darle a G una estructura topológica. Dotando a cada factor G_M con la topología discreta, y a $\prod_{M\in I} G_M$ con la topología producto entonces la topología de $\psi(G)$ es la inducida por $\prod_{M\in I} G_M$. Llamamos a esta topología sobre G la topología de Krull. Tenemos entonces el teorema fundamental de teoría de Galois para extensiones infinitas:

Teorema 1.27.6. *Sea E/k una extensión de Galois con grupo de Galois G. Dotamos a G con la topología de Krull. Entonces existe una biyección entre los subcampos de E y los subgrupos cerrados de G. Más precisamente, a un subgrupo cerrado H de G se le asocia el subcampo $F := E^H$ contenido en E, y a un subcampo F de E se le asocia el subgrupo (cerrado) $H := \mathrm{Gal}(E/F)$. Entonces, $H = \mathrm{Gal}(E/E^H)$, y $F = E^{\mathrm{Gal}(E/F)}$. El subgrupo cerrado H es normal en G si y sólo si F/k es una extensión de Galois.*

De este teorema se obtienen algunas consecuencias:

Primero, si H y H' dos subgrupos cerrados de G entonces $E^{H\cap H'} = E^H E^{H'} \subseteq E$. Para verlo, notamos que del teorema anterior se tiene que $E^H E^{H'}$ es de la forma $E^{H''}$ para algún subgrupo cerrado H'' de G. Como H y H' son cerrados en G, se obtiene de las inclusiones $E^H, E^{H'} \subseteq E^{H''}$ que $H'' \subseteq H \cap H'$. Además, $H \cap H'$ es cerrado, y se puede verificar que $E^{H\cap H'} \supseteq E^H E^{H'}$. Luego, como $H \cap H'$ es cerrado se obtiene que $H'' \supseteq H \cap H'$ y entonces $H'' = H \cap H'$.

Segundo, supongamos que E/k es una extensión de Galois con grupo de Galois G y que $H \subseteq G$ es un subgrupo de índice finito. Se puede probar que entonces H es cerrado. Asumiendo este hecho y utilizando el teorema anterior, se obtiene que $H = \mathrm{Gal}(E/E^H)$. Como G/H es un conjunto finito en biyección con $\mathrm{Hom}_k(E^H, E)$, se concluye que E^H/k es finito de grado $|G/H|$.

Por último, si G' cualquier subgrupo entonces un homomorfismo de grupos $\rho : G' \to G$ puede recuperarse de un conjunto de homomorfismos de grupos compatibles $\{\rho_M : G' \to G_M\}_{M\in I}$ utilizando también sistemas proyectivos.

1.28. Límites proyectivos

Definición 1.28.1. *Sea I un conjunto con orden parcial $\leq$. Llamamos a I un conjunto dirigido si dados $i, j \in I$, existe $l \in I$ tal que $i \leq l$ y $j \leq l$.*

El conjunto I de todas las extensiones finitas de Galois de E/k es un ejemplo de conjunto dirigido, donde $M \leq N$ si y sólo si $M \subseteq N$, y si $M, N \in I$ entonces $M \cdot N \in I$ y $M, N \leq M \cdot N$.

Definición 1.28.2. *Sea I cualquier conjunto dirigido. Sea $\{G_i\}_{i\in I}$ un conjunto de grupos. Para todo $i \leq j$, sea $g_{ji} : G_j \to G_i$ un homomorfismo de grupos. Al conjunto $\{G_i\}_{i\in I}$ junto con los homomorfismos $\{g_{ji}\}_{i\leq j}$ se le llama un sistema proyectivo si, $\forall\ l \leq i \leq j$, se tiene $g_{jl} = g_{il} \circ g_{ji}$ y $g_{ii} = \mathrm{Id}$.*

Se puede verificar que el sistema de grupos de Galois $\{G_M\}_{M\in I}$ con las funciones restricción usuales es un sistema proyectivo.

Definición 1.28.3. *Sea $\{G_i\}_{i\in I}$ un sistema proyectivo de grupos. El límite proyectivo de este sistema es el subgrupo Γ del producto $\prod_{i\in I} G_i$ definido como sigue: un elemento $\lambda = (\lambda_i)_{i\in I}$ pertenece a Γ si y sólo si, $\forall\ i \leq j$, se cumple $g_{ji}(\lambda_j) = \lambda_i$.*

Se puede verificar que Γ es un grupo. Denotamos a Γ como $\varprojlim(G_i)$.

Se puede probar que el grupo de Galois $\mathrm{Gal}(E/k)$ es isomorfo al límite proyectivo del sistema de grupos de Galois $\{\mathrm{Gal}(M/k)\}_{M\in I}$ (donde $k \subseteq M \subseteq E$). Cualquier grupo que sea el límite proyectivo de un sistema de grupos finitos se le llama un grupo profinito.

Notamos que el límite proyectivo Γ induce ua función natural $g_i : \Gamma \to G_i$, $\forall\ i \in I$, donde g_i es la restricción a Γ de la proyeción natural $\prod_{i\in I} G_i \to G_i$.

Ahora, sea $\{G_i\}_{i\in I}$ un sistema proyectivo de grupos. Si denotamos por $\mathrm{Hom}(H, H')$ al conjunto de homomorfismos entre dos grupos arbitrarios H, H', consideramos la siguiente función natural:

$$\begin{aligned} \mathrm{Hom}(H, \Gamma) &\longrightarrow \prod_{i\in I} \mathrm{Hom}(H, G_i) \\ \mu &\longmapsto g_i \circ \mu \end{aligned}$$

Se puede verificar que esta asignación es inyectiva, y no solamente eso sino también que $\{\mathrm{Hom}(H, G_i)\}_{i\in I}$ es un sistema proyectivo con las funciones $h_{ji} : \mathrm{Hom}(H, G_j) \to \mathrm{Hom}(H, G_i)$, donde $h_{ji}(\alpha) := g_{ji} \circ \alpha$, $\forall\ i \leq j$.

Proposición 1.28.4. *La imagen del grupo $\mathrm{Hom}(H, \Gamma)$ en $\prod_{i\in I} \mathrm{Hom}(H, G_i)$ es igual al límite proyectivo del sistema proyectivo de $\{\mathrm{Hom}(H, G_i)\}_{i\in I}$. Es decir, $\mathrm{Hom}(H, \varprojlim(G_i)) \cong \varprojlim(\mathrm{Hom}(H, G_i))$.*

Sean $\{H_i\}_{i\in I}$ y $\{G_i\}_{i\in I}$ dos sistemas proyectivos de grupos sobre el mismo conjunto dirigido y sean h_{ji} y g_{ji} sus homomorfismos de grupos asociados, respectivamente. Un morfismo entre los sistemas proyectivos $\{H_i\}_{i\in I}$ y $\{G_i\}_{i\in I}$ es un conjunto $\{f_i\}_{i\in I}$ de homomorfismos de grupos $f_i : H_i \to G_i$ tal que $\forall\ i \leq j$ se tiene $g_{ji} \circ f_j = f_i \circ h_{ji}$

Proposición 1.28.5. *Sea $\{f_i\}_{i\in I}$ un morfismo de sistemas proyectivos.*

1. *El morfismo $\{f_i\}_{i\in I}$ define un homomorfismo de grupos $f : \varprojlim(H_i) \to \varprojlim(G_i)$*
2. *Si cada f_i es inyectivo (resp. biyectivo) entonces f es inyectivo (resp. biyectivo).*

Observación 1.28.6. *Sea J un subconjunto de un conjunto dirigido I tal que el orden parcial $\leq$ de I induce una estructura de conjunto dirigido sobre J. Dado un sistema proyectivo $\{G_i\}_{i\in I}$, podemos considerar el sistema proyectivo $\{G_j\}_{j\in J}$, y sean Γ_I y Γ_J sus límites proyectivos respectivos. Entonces la proyección natural $\prod_{i\in I} G_i \to \prod_{j\in J} H_j$ induce un homomorfismo de grupos $\Gamma_I \to \Gamma_J$.*

Si además J cumple que, $\forall\, i \in I$, existe $j \in J$ tal que $i \leq j$ entonces decimos que J es cofinal en I. Por ejemplo, si $i_0 \in I$ entonces $J := \{j \in I | j \geq i_0\}$ es cofinal en I. Cuando J es cofinal en I entonces la proyección natural $\Gamma_I \to \Gamma_J$ es un isomorfismo de grupos.

Proposición 1.28.7. *Sea E/k una extensión de Galois con grupo de Galois G, y sea $H \subset G$ un subgrupo de índice finito. Entonces $H = \mathrm{Gal}(E/E^H)$. En particular, la extensión E^H/k es finita y $|G/H| = [E^H : k]$.*

2. Capítulo II - Propiedades de curvas completas no singulares

En este capítulo 2 se utilizarán varios de los resultados que revisamos en el capítulo 1. El objetivo en este capítulo es definir una curva completa no singular sobre un campo y su función zeta asociada cuando el campo es finito y después desarrollar los resultados necesarios para probar la racionalidad y la ecuación funcional de dicha función en el capítulo 3. Algunos de los resultados en este capítulo serán útiles en el capítulo 4, donde se prueba el teorema de Riemann-Roch y algunas de sus consecuencias que, como se verá en el capítulo 3, implican la racionalidad y la ecuación funcional.

2.1. Anillos con cocientes finitos

Definición 2.1.1. *Decimos que un dominio de Dedekind A tiene cocientes finitos si, para cualquier ideal maximal $P \in \mathrm{Max}(A)$, el campo residual A/P es un campo finito.*

Definición 2.1.2. *Sea A un dominio de Dedekind con cocientes finitos. Definimos la norma de un ideal I distinto de cero como la cardinalidad del cociente A/I, y denotamos a este valor como $||I||_A$.*

Notamos que $||I||_A = 1$ si y sólo si $I = A$, y además, que $||I||_A$ puede ser infinito, Sin embargo, se verá más adelante que este valor es finito cuando $I \neq (0)$.

Ejemplo 2.1.3. *Tenemos que el anillo $A = \mathbb{Z}$ tiene cocientes finitos. Entonces, sea $I = (a)$ cualquier ideal distinto de cero. Tenemos que*

$$||I||_A := |\mathbb{Z}/a\mathbb{Z}| = |a|$$

En particular, dado un número real γ, existe únicamente un número finito de ideales I en $\mathbb{Z}$ con $||I||_{\mathbb{Z}} \leq \gamma$. El anillo $A = k[x]$, con k campo finito de $q = p^r$ elementos, tambien tiene coeficientes finitos. Sea $I = (g(x))$ un ideal distinto de cero. Entonces

$$||I||_A := |k[x]/(g(x))| = q^{\deg(g(x))}.$$

pues $k[x]/(g(x))$ es un espacio vectorial sobre k de dimensión igual al grado de $g(x)$. En particular, dado un número real γ, existe únicamente un número finito de ideales I de $k[x]$ con $||I||_{k[x]} \leq \gamma$ pues existen a lo más $q^{\frac{\log(\gamma)}{\log(q)}+1}$ polinomios en $k[x]$ de grado menor o igual a $\log(\gamma)/\log(q)$.

Lema 2.1.4. *Sea A un dominio de Dedekind. Sea $P \in \mathrm{Max}(A)$ ideal maximal de A. Entonces, $\forall\, n \in \mathbb{N}$, el A-módulo P^{n-1}/P^n es isomorfo al A-módulo A/P. En particular, si el conjunto A/P es finito entonces el conjunto A/P^r es también finito, y $|A/P^r| = |A/P|^r$.*

Demostración. Como A es dominio de Dedekind, podemos elegir un elemento $x \in P^{n-1} \setminus P^n$ (por ser A dominio de Dedekind, tiene la propiedad de factorización única en ideales maximales, y por tanto $P^{n+1} \neq P^n\ \forall\, n \geq 1$). Consideramos el siguiente diagrama

$$\begin{array}{ccccccccc}
(0) & \longrightarrow & P & \longrightarrow & A & \longrightarrow & A/P & \longrightarrow & (0) \\
 & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \overline{\varphi}} & & \\
(0) & \longrightarrow & P^n & \longrightarrow & P^{n-1} & \longrightarrow & P^{n-1}/P^n & \longrightarrow & (0)
\end{array}$$

donde $\varphi : A \to P^{n-1}$, con $a \mapsto ax$, está bien definida ya que x pertenece a P^{n-1} que es un ideal, y además donde φ' y $\overline{\varphi}$ son las funciones naturales inducidas por φ (si $p \in P$ entonces $\varphi'(p) := px$, y si $a + P \in A/P$ entonces $\overline{\varphi}(a+P) := ax + P^n$ está bien definida pues $x \in P^{n-1}$ y P^{n-1} es un ideal). Notamos que las dos sucesiones horizontales son exactas, y que como A es dominio entonces φ es inyectivo pero no suprayectivo, a menos que $P^{n-1} = (x)$. Queremos ver que $\overline{\varphi}$ es un isomorfismo. Si ocurre que $\overline{\varphi}(a + P) = 0$ en P^{n-1}/P^n entonces $ax \in P^n$, por lo que $\mathrm{ord}_P(a) + \mathrm{ord}_P(x) \geq n$ (de la observación 5.2.19 se obtiene que $\mathrm{ord}_P(ax) \geq n$, y por otro lado, factorizando a los ideales (a) y (x) y multiplicando ambos, obtenemos que $(ax) = (a)(x) = (\prod_i P_i^{n_i})(\prod_j P_j^{n_j})$, y por la unicidad de la factorización del ideal (ax), se obtiene que $\mathrm{ord}_P(a) + \mathrm{ord}_P(x) = n_i + n_j$ (para los índices i, j tales que $P_i = P = P_j$), y que $n_i + n_j = \mathrm{ord}_P(ax) \geq n$), lo que implica que $\mathrm{ord}_P(a) \geq 1$ (ya que tenemos $x \notin P^n$ y $x \in P^{n-1}$, y entonces por la observación 5.2.19 se tiene $\mathrm{ord}_P(x) = n - 1$, es decir, $\mathrm{ord}_P(a) \geq 1$), y por tanto, de la observación 1.17.7 se obtiene que $x \in P$. Así, $\overline{\varphi}$ es inyectiva. Para ver que es suprayectiva, de la proposición 1.15.5 basta probar que, $\forall\, Q \in \mathrm{Max}(A)$, la función $\overline{\varphi}_Q : (A/P)_Q \to (P^{n-1}/P^n)_Q$ es suprayectivo. Consideramos el diagrama localizado

$$\begin{array}{ccccccccc}
(0) & \longrightarrow & P_Q & \longrightarrow & A_Q & \longrightarrow & (A/P)_Q & \longrightarrow & (0) \\
 & & \downarrow{\scriptstyle \varphi'_Q} & & \downarrow{\scriptstyle \varphi_Q} & & \downarrow{\scriptstyle \overline{\varphi}_Q} & & \\
(0) & \longrightarrow & (P^n)_Q & \longrightarrow & (P^{n-1})_Q & \longrightarrow & (P^{n-1}/P^n)_Q & \longrightarrow & (0)
\end{array}$$

Por la proposición 1.15.1 y por tener que las sucesiones horizontales del primer diagrama son exactas, se tiene que las dos sucesiones horizontales de este diagrama siguen siendo exactas. Si $Q \neq P$ entonces $(P^n)_Q = (P^{n-1})_Q = A_Q$ (lo cual se obtiene del lema 1.17.2). Por tanto, $\overline{\varphi}_Q$ es trivialmente suprayectiva (y además, notamos que φ_Q no es suprayectiva cuando $x \in Q$ (si fuera suprayectiva entonces dado $\frac{a'}{s'} \in (P^{n-1})_Q$ tal que $a' \in A \setminus Q$, existiría $\frac{a}{s} \in A_Q$ tal

que $\frac{ax}{s} = \frac{a'}{s'}$, es decir, $axs' = a's$, y si $x \in Q$ entonces el primer lado de la igualdad pertenecería a Q, por ser Q ideal, pero el lado derecho de la igualdad no pertenece a Q, por ser Q maximal y en particular primo, y esto sería una contradicción). Si $Q = P$ entonces $(P^{n-1})_Q = (xA_Q)$. Por tanto, la función φ_Q, y por consiguiente $\overline{\varphi}_Q$, son suprayectivas.

Supongamos ahora que A/P es campo finito. Para ver que A/P^r es un grupo finito, consideramos la siguiente sucesión exacta de grupos abelianos y procedemos por inducción sobre r:

$$(0) \to P^{r-1}/P^r \to A/P^r \to A/P^{r-1} \to (0)$$

Como el lema se cumple para $r = 1$, supongamos que se cumple para $r - 1 \geq 1$. Entonces, por hipótesis de inducción se tiene $|A/P^{r-1}| = |A/P|^{r-1}$, y como P^{r-1}/P^r es isomorfo a A/P entonces $|P^{r-1}/P^r| = |A/P|$ y se obtiene que

$$|A/P^r| = |A/P^{r-1}||P^{r-1}/P^r| = |A/P|^{r-1}|A/P| = |A/P|^r$$

(donde la segunda igualdad se obtiene de la hipótesis de inducción y de la igualdad $|P^{r-1}/P^r| = |A/P|$). Se obtiene entonces el resultado. □

Lema 2.1.5. *Sea A un dominio de Dedekind con cocientes finitos. Entonces la norma de cualquier ideal no cero de A es finita, y la función $||\quad||_A : \mathcal{M}(A) \to \mathbb{N}$ es multiplicativa, donde $\mathcal{M}(A)$ es el conjunto de ideales de A.*

Demostración. Sea $P \in \mathrm{Max}(A)$. Por el lema 2.1.4 obtenemos que $|A/P^r| = |A/P|^r$, que es un número finito, por lo que si tomamos cualquier ideal distinto de cero I entonces es de la forma $I = P_1^{a_1} \cdots P_r^{a_r}$, y por el corolario 1.17.13 tenemos $A/I \cong A/P_1^{a_1} \times \cdots \times A/P_r^{a_r}$, y por tanto $||I||_A = \prod_{i=1}^r ||P_i||_A^{a_i}$ (*). Se obtiene de lo anterior que $||I||_A$ es finito. Si I, J son cualesquiera dos ideales de A entonces I, J y IJ se factorizan en un producto único de potencias de ideales maximales, por lo que la factorización de I por la factorización de J es igual a la factorización de IJ, y se obtiene que si IJ es de la forma $IJ = \prod_{i=1}^r P_i^{a_i}$ entonces se puede obtener, sin pérdida de generalidad, que $I = \prod_{i=1}^j P_i^{a_i}$ y $J = \prod_{i=j+1}^r P_i^{a_i}$ para algún $1 \leq j \leq r$, y aplicando (*) se tiene $||IJ||_A = ||I||_A||J||_A$. □

Proposición 2.1.6. *Sea A dominio de Dedekind con cocientes finitos y K su campo de fracciones. Sea L/K una extensión finita. Supongamos que la cerradura entera B de A en L es un A-módulo finitamente generado. Entonces B es un dominio de Dedekind con cocientes finitos. Más aún, si $I \subset B$ es un ideal no cero entonces $||I||_B = ||N_{B/A}(I)||_A$.*

Demostración. Se obtiene del teorema 5.2.11 que B es dominio de Dedekind. Sea $M \in \text{Max}(B)$. Sea $P := M \cap A$. Entonces B/M es un espacio vectorial sobre A/P (por ser B un A-módulo finitamente generado) de dimensión $f_{M/P}$. Por tanto, B/M es un campo finito (A/P es finito por ser A de cocientes finitos), y se cumple que

$$||M||_B = |B/M| = |A/P|^{f_{M/P}} = ||P^{f_{M/P}}||_A = ||N_{B/A}(M)||_A$$

donde la penúltima igualdad se obtiene del lema 2.1.5, y la última igualdad es la definición de $N_{B/A}$ cuando L/K no es Galois.Como $N_{B/A}$ es multiplicativa (lo cual se obtiene de la definición de $N_{B/A}$), obtenemos que para cualquier ideal I de B, $||I||_B = ||N_{B/A}(I)||_A$. □

Denotamos ahora por A ya sea a $\mathbb{Z}$ o a $k[x]$, donde k es un campo finito, por L a una extensión finita de grado n del campo de fracciones K de A, y por B a la cerradura entera de A en L. Supongamos que B es un A-módulo finitamente generado. Entonces de la proposición 2.1.6 se obtiene que B tiene cocientes finitos. Tenemos el siguiente lema:

Lema 2.1.7. *Sea $\lambda \in \mathbb{R}$ fijo. Entonces existe únicamente un número finito de ideales B con $||I||_B \leq \lambda$.*

Demostración. Como un ideal $I \in \mathcal{M}(B)$ tiene norma $||I||_B = 1$ si y sólo si $I = B$, y como $||\ \ ||_B$ es multiplicativa y positiva por el lema 2.1.5, basta probar que B contiene únicamente un número finito de ideales maximales M con $||M||_B \leq \lambda$. Como un ideal maximal de A está contenido únicamente en un número finito de ideales maximales de B (ya que un ideal maximal P de A está contenido en un ideal maximal M de B si y sólo si el ideal generado por P en B está contenido en M, lo cual se obtiene de la observación 1.5.7), y como

$$||M||_B = ||M \cap A||_A^{f_{M/M\cap A}} \geq ||M \cap A||_A$$

(donde la igualdad se obtiene de la proposición 2.1.6 y de la definición de $N_{B/A}$) es suficiente probar que, dado $\lambda \in \mathbb{R}$, existe únicamente un número finito de ideales maximales P de A con $||P||_A \leq \lambda$ (pues de lo anterior, se tiene que la norma de un maximal M de B es igual a la norma del maximal $M \cap A$ de A elevado a una cierta potencia, por lo que basta fijarse solamente en la norma del maximal $M \cap A$ de A), lo cual se cumple para los casos $A = \mathbb{Z}$ o $A = \mathbb{F}_q[x]$, por el ejemplo 2.1.3 mencionado antes. □

2.2. Valoraciones y dominios de ideales principales

Definición 2.2.1. *Sea $\mathbb{R}_{\geq 0}$ el conjunto de números reales no negativos . Sea L cualquier campo. Una función $|\ |: L \to \mathbb{R}_{\geq 0}$ se le llama un valor absoluto de L si satisface:*

- *(i) $|x| = 0$ si y sólo si $x = 0$.*
- *(ii) $|xy| = |x||y|$ para todo $x, y \in L$.*
- *(iii) $|x + y| \leq |x| + |y|$ para todo $x, y \in L$.*

Definición 2.2.2. *Sea L cualquier campo. Una valoración de L es una función $v : L^* \to \mathbb{Z}$ tal que se se satisfacen las siguientes propiedades:*

- *(i) $v(xy) = v(x)+v(y)$ $\forall x, y \in L^*$ (i.e., v es un homomorfismo de grupos).*
- *(ii) $v(x + y) \geq \min\{v(x), v(y)\}$ $\forall x, y \in L^*$*

Extendemos v a L poniendo $v(0) := +\infty$

Sea $\mathcal{O}_v = \{\alpha \in L^* | v(\alpha) \geq 0\}$ y $\mathcal{M}_v := \{\alpha \in L^* | v(\alpha) > 0\}$. Se puede verificar que $\mathcal{O}_v$ es un anillo y que $\mathcal{M}_v$ es un ideal propio. Notamos que si $\alpha \in \mathcal{O}_v$ es invertible en $\mathcal{O}_v$ entonces $0 = v(1) = v(\alpha\alpha^{-1}) = v(\alpha) + v(\alpha^{-1}) \Rightarrow v(\alpha) = 0$ y $v(\alpha^{-1}) = 0$, y recíprocamente si α es tal que $v(\alpha) = 0$ entonces tomando $\alpha^{-1} \in L^*$ se tiene $0 = v(1) = v(\alpha\alpha^{-1}) = v(\alpha) + v(\alpha^{-1}) \Rightarrow v(\alpha^{-1}) = 0 \Rightarrow \alpha^{-1} \in \mathcal{O}_v$ y por tanto α es invertible en $\mathcal{O}_v$. Aplicando el siguiente lema se obtiene que $\mathcal{O}_v$ es un anillo local cuyo ideal maximal es $\mathcal{M}_v$. Denotamos por k_v al campo residual $\mathcal{O}_v/\mathcal{M}_v$.

Lema 2.2.3. *Un anillo A es local si y sólo si el complemento en A del conjunto de unidades A^* es un ideal de A.*

Demostración. Si A es local con ideal maximal M entonces sabemos que $A \setminus M$ consta de los elementos invertibles en A y su complemento es M, el cual es un ideal.

Recíprocamente, si el complemento del conjunto de unidades, digamos J, es un ideal de A entonces J es un ideal maximal, ya que de lo contrario si hubiera I ideal de A con $J \subseteq I$ $(I \neq J)$ entonces $\exists x \in I \setminus J$ y por tanto x es invertible, por lo que $1 \in J \Rightarrow J = A$. Por otro lado, si hubiera M maximal distinto de J entonces debe contener a algún elemento invertible, por lo que $1 \in M \Rightarrow M = A$, lo cual es contradicción.

Por tanto, A es local con ideal maximal J. □

Valoraciones P-ádicas. Sea A un dominio de Dedekind (conmutativo), y K su campo de fracciones. Sea $P \subset A$ un ideal maximal. Asociamos a P una

valoración suprayectiva $v_P : K^* \to \mathbb{Z}$ como sigue: si $x \in A$ entonces escribimos el ideal (x) generado por x en A como

$$(x) = \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(x)}$$

donde $\mathrm{Max}(A)$ es el conjunto de ideales maximales de A y $\mathrm{ord}_P(x) \in \mathbb{N} \bigcup \{0\}$ es el número de veces que aparece P en la factorización (única) del ideal (x). Notamos que $\mathrm{ord}_P(x) = 0$ para todos excepto para un número finito de elementos $P \in A$, y notamos también que, para cada P fija, el número $\mathrm{ord}_P(x)$ varía dependiendo de cada x. Definimos entonces $v_P(x) := \mathrm{ord}_P(x)$. Si $x = a/b \in K$ con $a, b \in A$ entonces definimos

$$v_P(x) := v_P(a) - v_P(b)$$

Notamos que $v_P : K^* \to \mathbb{Z}$ es efectivamente una valoración, ya que si $x, y \in A$ se tiene $x = a/b$ y $y = c/d$ con $a, b, c, d \in A$ y entonces

$$v_P(x \cdot y) = v_P(\frac{a}{b} \cdot \frac{c}{d}) = v_P(\frac{ac}{bd}) = v_P(ac) - v_P(bd) = \mathrm{ord}_P(ac) - \mathrm{ord}_P(bd)$$

Pero por ser A conmutativo, se tiene que $(ac) = (a)(c)$ y por tanto

$$\prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(ac)} = (ac) = (a)(c) = \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(a)} \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(c)}$$

y por la unicidad de la factorización se obtiene

$$\prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(ac)} = \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(a) + \mathrm{ord}_P(c)}$$
$$\Rightarrow \mathrm{ord}_P(ac) = \mathrm{ord}_P(a) + \mathrm{ord}_P(c)$$

Análogamente se obtiene $\mathrm{ord}_P(bd) = \mathrm{ord}_P(b) + \mathrm{ord}_P(d)$ y entonces

$$\begin{aligned} v_P(x \cdot y) &= v_P(\tfrac{a}{b} \cdot \tfrac{c}{d}) = v_P(\tfrac{ac}{bd}) = v_P(ac) - v_P(bd) \\ &= \mathrm{ord}_P(ac) - \mathrm{ord}_P(bd) \\ &= (\mathrm{ord}_P(a) + \mathrm{ord}_P(c)) - (\mathrm{ord}_P(b) + \mathrm{ord}_P(d)) \\ &= (\mathrm{ord}_P(a) - \mathrm{ord}_P(b)) + (\mathrm{ord}_P(c) - \mathrm{ord}_P(d)) = v_P(\tfrac{a}{b}) + v_P(\tfrac{c}{d}) \\ &= v_P(x) + v_P(y) \end{aligned}$$

Por otro lado, notamos también que la valoración v_P es suprayectiva. Como $P \setminus P^2$ es un conjunto no vacío (por la factorizacón única de ideales maximales), se obtiene que v_P es suprayectiva, ya que tomando $x \in P \setminus P^2$ y dado cualquier $n \in \mathbb{N}$, tomamos el ideal $(x)^n = (x^n)$ y notamos que está contenido en P^n pero no en P^{n+1}, y aplicando la observación 5.2.19 se obtiene que $v_P(x^n) = n$ (notamos que $x^n \in A$), y de aquí se obtiene la suprayectividad (otra forma de verlo es notar que, dado $P \in \mathrm{Max}(A)$ fijo, la localización A_P es dominio de

Dedekind local con un solo ideal maximal PA_P, por lo que es un dominio de ideales principales. Tomando cualquier $n \in \mathbb{N}$ fijo, se obtiene entonces que existe $x/s \in PA_P$, con $x \in P$, $s \in S$ tal que $(x/s) = (PA_P)^n$. Factorizando el ideal $(x) = \prod_{Q \in \mathrm{Max}(A)} Q^{e_Q}$, notamos que $x \in P$ implica que el ideal P (elevado a un valor positivo e_P) aparece en la factorización de (x). Por tanto, se obtiene que $(x/1) = (PA_P)^{e_P}$, y como $(x/1) = (x/s)$ y A_P es dominio de Dedekind entonces $e_Q = n$. Por tanto, $v_P(x) = n$, y se obtiene entonces que v_P es suprayectiva).

Notamos además que $v_P(x) \geq 0$ si $x \in A$ y que $v_P(x) = 0$ si y sólo si $x \notin P$ (observación 1.17.7).

Sea A un dominio de Dedekind con campo de fracciones K. Sea $P \in \mathrm{Max}(A)$. Supongamos que A tiene cocientes finitos. Definimos el valor absoluto estandarizado $|\ |_P$ asociado a v_P como:

$$|\ |_P : K \to \mathbb{R}_{\geq 0}$$

$$x \mapsto |x|_P := |A/P|^{-v_P(x)}, \text{ si } x \neq 0$$

y $|0|_P = 0$. La cardinalidad de A/P es una valor finito, pues A tiene cocientes finitos.

Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita. Sea B la cerradura de A en L. Supongamos que B es un A-módulo finitamente generado. Entonces B también es un dominio de Dedekind. Cada ideal $\mathcal{B} \in \mathrm{Max}(B)$ tiene asociado una valoración $v_{\mathcal{B}} : L^* \to Z$. Cuando A tiene cocientes finitos entonces también B tiene cocientes finitos. Podemos asociar de manera similar a lo anterior un valor absoluto $||\ ||_{\mathcal{B}}$ a cada valoración $v_{\mathcal{B}}$

$$||\ ||_{\mathcal{B}} : L \to \mathbb{R}_{\geq 0}$$

$$x \mapsto ||\ ||_{\mathcal{B}} := |B/\mathcal{B}|^{-v_{\mathcal{B}}(x)}, \text{ si } x \neq 0$$

y $|0|_{\mathcal{B}} = 0$, es decir, el valor absoluto $||\ ||_{\mathcal{B}}$ es el valor absoluto estandarizado de L asociado a $\mathcal{B}$. Sin embargo, también podemos definir el siguiente valor absoluto: Sea $P := \mathcal{B} \cap A$ y $PB = \prod_{\mathcal{B}|PB} \mathcal{B}^{e_{\mathcal{B}/P}}$. Definimos

$$|\ |_{\mathcal{B}} : L \to \mathbb{R} \geq 0$$

$$x \mapsto |\ |_{\mathcal{B}} := |A/P|^{-v_{\mathcal{B}}(x)/e_{\mathcal{B}/P}}, \text{ si } x \neq 0$$

$$0 \mapsto 0$$

Observación 2.2.4. *El valor absoluto $|\ |_{\mathcal{B}}$ de L extiende al valor absoluto $|\ |_P$ de K, es decir, para todo $x \in K$ se cumple $|x|_{\mathcal{B}} = |x|_P$. Para verlo, notamos que si $x \in L$ entonces $v_{\mathcal{B}}(x) = e_{\mathcal{B}/P} v_P(x)$ (5.2.16). Por tanto, de las definiciones se obtiene la observación. Notamos también que*

$$||\ ||_{\mathcal{B}} = (|\ |_{\mathcal{B}})^{e_{\mathcal{B}/P} f_{\mathcal{B}/P}}$$

(de la demostración de la proposición 2.1.6 se obtiene que $|B/\mathcal{B}| = |A/P|^{f_{\mathcal{B}/P}}$).

Denotamos por $n_{\mathcal{B}/P}$ al producto $e_{\mathcal{B}/P} \cdot f_{\mathcal{B}/P}$. Tenemos entonces:

Lema 2.2.5. *Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita de grado n. Sea B la cerradura entera de A en L. Supongamos que B es un A-módulo finitamente generado. Entonces*

- *(i) $\sum_{\mathcal{B}|PB} n_{\mathcal{B}/P} = n = [L : K]$.*
- *(ii) Sea $x \in B$. Entonces $v_P(N_{L/K}(x)) = \sum_{\mathcal{B}|PB} f_{\mathcal{B}/P} v_{\mathcal{B}}(x)$.*
- *(iii) Supongamos que A tiene cocientes finitos. Sea $|\ |_P$ el valor absoluto estandarizado asociado a $P \in \mathrm{Max}(A)$. Entonces $|N_{L/K}(x)|_P = \prod_{\mathcal{B}|PB}(|x|_{\mathcal{B}}^{n_{\mathcal{B}/P}})$*

Demostración. La primera parte es en realidad el teorema 1.18.4.

Para la parte (ii), notamos que podemos escribir

$$(xB) = \prod_{P \in \mathrm{Max}(A)} \left(\prod_{\mathcal{B}|PB} \mathcal{B}^{v_{\mathcal{B}}(x)} \right)$$

Por definición, $N_{B/A}(xB) = \prod_{P \in \mathrm{Max}(A)} P^{\sum_{\mathcal{B}|PB} f_{\mathcal{B}/P} v_{\mathcal{B}}(x)}$. Como $N_{B/A}(xB) = N_{L/K}(x)A$ (proposición 1.25.8), se obtiene la parte (ii). Para la parte (iii), notamos que por ser los valores absolutos y la función norma ambos funciones multiplicativas, basta ver el caso en que $x \in B$. Usando la factorización de (xB), la proposición 1.25.8 y la parte (ii) ya probada, se obtiene que

$$\prod_{\mathcal{B}|PB} |x|_{\mathcal{B}}^{n_{\mathcal{B}/P}} = |A/P|^{-\sum_{\mathcal{B}|PB} f_{\mathcal{B}/P} v_{\mathcal{B}}(x)} = |A/P|^{-v_P(N_{L/K}(x))} = |N_{L/K}(x)|_P$$

obteniéndose lo que se buscaba. □

La función grado $\deg : k[x] \setminus \{0\} \to \mathbb{N}$, con $f(x) \mapsto \deg(f(x))$, puede extenderse a una función sobre $k(x) \setminus \{0\}$ como sigue:

Si $r(x) = p(x)/q(x)$, $p(x), q(x) \in k[x]$ entonces $\deg(r(x)) := \deg(p(x)) - \deg(q(x))$. Notamos que

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

$$\deg(f + g) \leq \max(\deg(f), \deg(g))$$

Se puede definir entonces una nueva valoración

$$v_\infty : k(x) \to \mathbb{Z} \setminus \{0\}$$

$$f \mapsto -\deg(f)$$

Observación 2.2.6. *Las valoraciones suprayectivas v_P, $P \in \mathrm{Max}(k[x])$, y v_∞, son todas distintas. Para verlo, sea $f(x) \in k[x]$ un polinomio irreducible que genera al ideal maximal P. Se obtiene entonces que*

$$v_P(f) = 1$$

$$v_\infty(f) = -\deg(f) < 0$$

$$v_Q(f) = 0 \text{ si } Q \in \mathrm{Max}(k[x]) \text{ y } Q \neq P$$

Cuando k es un campo finito con q elementos, asociamos a la valoración v_∞ de $k(x)$ el valor absoluto definido como

$$|f(x)|_\infty := q^{-v_\infty(f)} = q^{\deg(f)}$$

Lema 2.2.7. *Sea k cualquier campo. La valoración v_∞ de $k(x)$ es igual a la valoración v_P de $k(x)$ asociada al ideal maximal $P := (1/x)k[1/x]$ de $k[1/x]$.*

Demostración. Consideramos la inclusión $k[1/x] \subset k(1/x) = k(x)$. El anillo $k[1/x]$ es un dominio de ideales principales con campo de fracciones $k(x)$. Sea $f(x) = \sum_{i=0}^{\deg(f)} a_i x^i$, con $a_{\deg(f)} \neq 0$, cualquier elemento de $k[x]$. Como $k(x)$ es el campo de fracciones de $k[1/x]$, podemos escribir $f(x)$ como un cociente de la forma $g(1/x)/h(1/x)$, con $g(1/x), h(1/x) \in k[1/x]$, como sigue. Escribimos

$$f(x) = (\frac{1}{x})^{-\deg(f)}(\sum_{i=0}^{\deg(f)} a_i \frac{1}{x^{\deg(f)-i}}) =$$

$$\frac{a_{\deg(f)} + a_{\deg(f)-1}(\frac{1}{x}) + \cdots + a_0(\frac{1}{x})^{\deg(f)}}{(\frac{1}{x})^{\deg(f)}}$$

Notamos que el elemento $a_{\deg(f)} + a_{\deg(f)-1}(\frac{1}{x}) + \cdots + a_0(\frac{1}{x})^{\deg(f)}$ no es divisible por $1/x$ en el dominio de ideales principales $k[1/x]$. Por tanto, se obtiene de la definición de la valoración P-ádica v_P asociada a $P := (1/x)$ que

$$v_P(f(x)) := \mathrm{ord}_P(f(x)) = 0 - \mathrm{ord}_P((1/x)^{\deg(f)}) = -\deg(f).$$

Por tanto, $v_P = v_\infty$. Para mostrar que $|\ |_\infty = |\ |_P$, notamos que $k[1/x]/P \cong k$. Se obtiene entonces que si $|k| = q$, $|f|_P := q^{-v_P(f)} = |f|_\infty$. □

Teorema 2.2.8. *Sea K cualquier campo. Sea $v : K^* \to \mathbb{Z}$ una valoración no trivial. Entonces $\mathcal{O}_v$ es un dominio de ideales principales local, la función v está determinada de manera única por el valor $v(\pi)$, donde π es un generador de $\mathcal{M}_v$, y la función $v \mapsto \mathcal{O}_v$, del conjunto de valoraciones suprayectivas de K al conjunto de dominios de ideales principales locales contenidos en K y con campo de fracciones K, es una biyección.*

Demostración. Sea π un elemento de $\mathcal{M}_v$ tal que $v(\pi)$ es igual al mínimo valor positivo que toma v. Sea $\alpha \in \mathcal{O}_v$. Si α no es unidad (por tanto $v(\alpha) > 0$) entonces $v(\alpha)$ es múltiplo de $v(\pi)$, ya que de lo contrario se tendría $v(\alpha) = mv(\pi) + r$, con $0 < r < v(\pi) \Rightarrow v(\alpha\pi^{-m}) = r < v(\pi)$, por lo que $\alpha\pi^{-m} \in \mathcal{M}_v$, contradiciendo que $v(\pi)$ es el mínimo valor posible. Luego, tenemos $v(\alpha) = mv(\pi) \Rightarrow v(\alpha\pi^{-m}) = 0$, por lo que $\alpha\pi^{-m}$ es unidad en $\mathcal{O}_v$. Se obtiene entonces que cada elemento de $\mathcal{O}_v$ se puede escribir como el producto de una unidad en $\mathcal{O}_v$ y una potencia de π, y por tanto π genera a $\mathcal{M}_v$. Notamos que si $\alpha \in \mathcal{O}_v$ con $\alpha = u\pi^m = u'\pi^n$, con u, u' unidades en $\mathcal{O}_v$ entonces se obtiene que $v(u) + mv(\pi) = v(u') + nv(\pi)$, y como $v(u) = v(u') = 0$ entonces se obtiene $m = n$, luego $u\pi^m = u'\pi^m \Rightarrow u = u'$, por tanto α se escribe de manera única como el producto de una unidad y una potencia de π.

De manera similar se puede ver que cualquier otro ideal $I \subseteq \mathcal{O}_v$ está generado por un elemento de $\mathcal{O}_v$. Para esto, notamos que si $\alpha \in I$ entonces $v(\alpha) \geq 0$, por lo que $v(\alpha) > 0$ (si ocurriera $v(\alpha) = 0$ entonces α sería invertible en $\mathcal{O}_v$, por lo que $I = \mathcal{O}_v$), y entonces es de la forma $\alpha = u\pi^n$, para algún $n \in \mathbb{N}$, $u \in \mathcal{O}_v$ invertible en $\mathcal{O}_v$. Tomando n_0 el mínimo de los enteros positivos n, se obtiene que π^{n_0} genera a I. Entonces $\mathcal{O}_v$ es de ideales principales.

Además, cada elemento de K es el producto de una unidad y una potencia de π, posiblemente negativa (pues si $x \in K$ entonces es un cociente $\frac{a}{b}$ con $a, b \in \mathcal{O}_v$, y además a y b son ambos el producto único de una unidad y una potencia del generador de $\mathcal{M}_v$). De esto, y del hecho que la valoración de una unidad es igual a cero, se obtiene que la valoración v está determinada de manera única por el valor $v(\pi)$.

Veamos ahora que la función $v \mapsto \mathcal{O}_v$ es inyectiva. Sean v_1 y v_2 dos valoraciones suprayectivas de K. Si $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$ entonces $\mathcal{M}_{v_1} = \mathcal{M}_{v_2}$ es un ideal principal. Sea π un generador. Como v_1 y v_2 son suprayectivas, se obtiene $v_1(\pi) = v_2(\pi) = 1$, y como los valores $v_1(\pi)$ y $v_2(\pi)$ determinan de manera única las valoraciones v_1 y v_2, se concluye que $v_1 = v_2$.

Ahora veamos que $v \mapsto \mathcal{O}_v$ es suprayectiva. Sea $\mathcal{O}$ un dominio de ideales principales local con campo de fracciones K. Sea $\mathcal{M}$ su ideal maximal. Sea π un generador de $\mathcal{M}$. Cada elemento $x \in K^*$ puede ser escrito de manera única como un producto $x = u\pi^s$, con $u \in \mathcal{O}^*$, $s \in \mathbb{Z}$ (si tenemos $x = u\pi^s = v\pi^t$ entonces, por ser u, v unidades, se obtiene $\pi^s = \pi^t$, y entonces $s = t$. Se obtiene que $u = v$.). Tomando la valoración $\mathcal{M}$-ádica $v_{\mathcal{M}} : K^* \to \mathbb{Z}$ se tiene $x \in \mathcal{O}_{v_{\mathcal{M}}} \Leftrightarrow v_{\mathcal{M}}(x) \geq 0 \Leftrightarrow v_{\mathcal{M}}(u) + sv_{\mathcal{M}}(\pi) \geq 0 \Leftrightarrow s \geq 0$ (lo último pues $v_{\mathcal{M}}(u) = 0$ y $v_{\mathcal{M}}(\pi) = 1$, ya que $v_{\mathcal{M}}$ es sobre), y luego $x = u\pi^s, s \geq 0 \Leftrightarrow x \in \mathcal{O}$ (pues si $x = u\pi^s$, $s \geq 0$ entonces por ser π generador de $\mathcal{M}$ y $u \in \mathcal{O}$, se obtiene que $x \in \mathcal{O}$. Recíprocamente, si $x = u\pi^s \in \mathcal{O}$, notamos que π no es invertible en $\mathcal{O}$, ya que genera a $\mathcal{M}$, y entonces si se tuviera $s < 0$, obtendríamos $u = x\pi^{-s} \in \mathcal{M}$, pero u es invertible en $\mathcal{O}$, y se tendría entonces $\mathcal{M} = \mathcal{O}$, una contradicción. Entonces, $s \geq 0$). Entonces $\mathcal{O}_{v_{\mathcal{M}}} = \mathcal{O}$, y por tanto la función es suprayectiva. □

Observación 2.2.9. *Sea $v : K^* \to \mathbb{Z}$ cualquier valoración. Sea $n \in \mathbb{N}$. Sea $nv : K^* \to \mathbb{Z}$ tal que $(nv)(x) = nv(x)$. Entonces $\mathcal{O}_v = \mathcal{O}_{nv}$ y $\mathcal{M}_v = \mathcal{M}_{nv}$.*

Ahora, sea $v : K^* \to \mathbb{Z}$ cualquier valoración no trivial. Entonces existe un único entero positivo e_v tal que la función $v/e_v : K^* \to \mathbb{Z}$, con $x \mapsto v(x)/e_v$, es una valoración suprayectiva. Basta tomar $e_v := \min\{v(x)|x \in \mathcal{M}_v\}$. Entonces $v(K^*) = e_v\mathbb{Z}$.

Teorema 2.2.10. *Sea A un cualquier dominio de dimensión 1 con campo de fracciones K. Entonces la función $v \mapsto \mathcal{M}_v \cap A$ entre el conjunto de valoraciones suprayectivas de K con $v(A) \geq 0$ y $\mathrm{Max}(A)$ está bien definida. Si A es un dominio de Dedekind entonces esta función es biyectiva, es decir, cada ideal maximal $M \subseteq A$ define una valoración suprayectiva v_M de K (la valoración M-ádica) tal que $v_M(A) \geq 0$, y $M \mapsto v_M$ es el inverso de la función $v \mapsto \mathcal{M}_v \cap A$. Además, $\cap_{\{v|v(A)\geq 0\}}\mathcal{O}_v = A$. Más aún, $k_{v_M} := \mathcal{O}_{v_M}/\mathcal{M}_{v_M} \cong A/M$.*

Demostración. Como $v(A) \geq 0$, se tiene $A \subseteq \mathcal{O}_v$. Sea $M := A \cap \mathcal{M}_v$. Cada elemento de $A \setminus M$ es invertible en $\mathcal{O}_v$, pues si $x \in A \setminus M \Rightarrow x \in A \subseteq \mathcal{O}_v$, $x \notin \mathcal{M}_v \cap A \Rightarrow v(x) = 0$, y entonces x es invertible en $\mathcal{O}_v$. Tomando la inclusión $\mathrm{i} : A \setminus M \to \mathcal{O}_v$ y por ser $j : A \to A_M, a \mapsto \frac{a}{1}$ inyectivo (ya que A es dominio) entonces la propiedad universal de anillos de fracciones nos dice que existe una única $g' : A_M \to \mathcal{O}_v$ con $\mathrm{i} = g' \circ j$, por lo que g' es inyectiva y $A_M \subseteq \mathcal{O}_v$. Como A tiene dimensión 1 entonces $M = (0)$ o M es un ideal maximal de A. Si $M = (0)$ entonces $A_M = K \Rightarrow \mathcal{O}_v = K$, lo cual no es posible pues v es una valoración suprayectiva. Entonces $M \in \mathrm{Max}(A)$.

Supongamos que A es un dominio de Dedekind. Tomamos la valoración v_M. La función $M \mapsto v_M$ es inyectiva, pues en general si P y Q son dos ideales maximales distintos de A, tomamos $x \in P \setminus P \cap Q$, y entonces $x \in P$ y $x \notin Q$, por lo que $x \in P \Leftrightarrow v_P(x) := \mathrm{ord}_P(x) > 0$ (observación 1.17.7), y $x \notin Q \Leftrightarrow v_Q(x) = \mathrm{ord}_Q(x) = 0$ (observación 1.17.7) entonces se obtiene que $v_P \neq v_Q$.

Para ver la suprayectividad de la función $M \mapsto v_M$, basta probar que, dado v con $v(A) \geq 0$, existe un ideal primo M de A tal que $A_M = \mathcal{O}_v$, ya que el teorema 2.2.8 implica entonces que $v = v_M$ (aplicamos el lema 5.2.14 para obtener $A_M = \mathcal{O}_{v_M}$, por lo que $\mathcal{O}_v = \mathcal{O}_{v_M}$, y del teorema 2.2.8 se obtiene $v = v_M$). Sea v una valoración de K tal que $v(A) \geq 0$. Tenemos $A \subseteq \mathcal{O}_v$. Sea $M = \mathcal{M}_v \cap A$. Análogamente a lo que se hizo antes, encontramos que $M \in \mathrm{Max}(A)$, y que $A_M \subseteq \mathcal{O}_v$. Como A_M es un dominio de ideales principales local (pues A dominio de Dedekind implica que A_M también es de Dedekind, y como tiene un número finito de ideales maximales (pues A_M es local) entonces aplicamos la proposición 1.17.15) entonces del lema 1.14.6 se tiene $A_M = \mathcal{O}_v$ (notamos que se cumple $MA_M \subseteq M_v$, ya que $M = M_v \cap A$ y j es inyectivo, por lo que efectivamente podemos aplicar el lema). Por tanto, la función $M \mapsto v_M$ es biyección.

Por la proposición 1.15.7 se prueba que $A = \cap_{M\in\mathrm{Max}(A)}A_M$, y por la biyección $M \mapsto v_M$ y por todo lo anterior, se obtiene que $\cap_{M\in\mathrm{Max}(A)}A_M = \cap_{\{v|v(A)\geq 0\}}\mathcal{O}_v$. Del lema 1.18.5 se tiene que $k_v \cong A/M$ si $v = v_M$, donde además se tiene $A/M \cong A_M/MA_M$. □

2.3. Curvas completas no singulares

Definición 2.3.1. *Sea L/k una extensión finita. Denotamos por $\mathcal{V}(L/k)$ al conjunto de valoraciones suprayectivas de L triviales en k, es decir, al conjunto de funciones suprayectivas $v : L^* \to \mathbb{Z}$ con $v(k^*) = 0$.*

Definición 2.3.2. *Un campo de funciones L/k es una extensión L/k que tiene grado de trascendencia 1 sobre k (es decir, $\exists x \in L$ tal que $L/k(x)$ es una extensión finita (con $k(x)$ el menor subcampo de L que contiene a k y a x) y $k(x)$ es isomorfo como k-álgebra al campo de funciones racionales en una variable sobre k), y tal que k es algebraicamente cerrado en L (es decir, el conjunto de elementos en L algebraicos sobre k es igual a k precisamente).*

Definición 2.3.3. *Sea k cualquier campo. Una curva completa no singular X/k sobre k es una pareja $(X, k(X)/k)$ que consiste de un campo de funciones $k(X)/k$, y un conjunto X que está en correspondencia biyectiva con $\mathcal{V}(k(X)/k)$.*

Notamos que a cada punto $P \in X$ le corresponde una valoración v_P, y por tanto un anillo de ideales principales local $\mathcal{O}_P := \mathcal{O}_{v_P}$ con ideal maximal $\mathcal{M}_P$. Llamamos al campo $k(X)$ el campo de funciones racionales sobre X. Al anillo $\mathcal{O}_P$ se le llama el anillo de funciones racionales definidas en P, y a un elemento de él se le llama una función sobre X definida en P. Un elemento $\alpha \in \mathcal{O}_P$ tiene un cero en P si $\alpha \in \mathcal{M}_P$, y $v_P(\alpha)$ es el orden de dicho cero. Si $\alpha \in \mathcal{O}_P \setminus \mathcal{M}_P$ entonces α tiene un polo en P, y su orden se define como $|v_P(\alpha)|$. El dominio de $\alpha \in k(X)$ es el conjunto de puntos P en X tales que $\alpha \in \mathcal{O}_P$. Si $U \subseteq X$ entonces consideraremos el anillo $\mathcal{O}_X(U) := \bigcap_{P \in U} \mathcal{O}_P$, y lo llamamos el anillo de funciones sobre X definidas en todos lados sobre U.

Podemos dotar a X con la topología de Zariski, donde un subconjunto C es cerrado si y sólo si C es vacío, o igual a X, o un conjunto finito de puntos.

Definición 2.3.4. *Un abierto U de X se llama afín si el anillo $\mathcal{O}_X(U)$ es una k-álgebra finitamente generada y un dominio de Dedekind, y si la función $U \to \mathrm{Max}(\mathcal{O}_X(U))$ con $P \mapsto \mathcal{M}_P \cap \mathcal{O}_X(U)$ está bien definida y es biyectiva.*

Notamos que cualquier extensión L/k de grado de trascendencia 1 sobre k define una curva completa no singular, donde tomamos $X = \mathcal{V}(L/k)$, y donde cada punto P de X es una valoración v_P (la valoración P-ádica).

Definición 2.3.5. *Una línea proyectiva sobre k es una curva completa no singular $\mathbb{P}^1/k$ tal que el campo de funciones $k(\mathbb{P}^1)/k$ es isomorfo como k-álgebra al campo de funciones racionales en una variable.*

Sea $\mathbb{P}^1/k$ la línea proyectiva asociada al campo de funciones $k(x)/k$. Denotamos por ∞ al punto de $\mathbb{P}^1/k$ correspondiente a la valoración v_∞.

Proposición 2.3.6. *Sea k cualquier campo. Sea $\mathbb{P}^1/k$ la línea proyectiva asociada al campo de funciones $k(x)/k$. Entonces*

$$\mathbb{P}^1 = \{v_{g(x)} \mid g(x) \in k[x], \text{ irreducible y monico}\} \sqcup \{v_\infty\}$$

Demostración. Sea $v \in \mathcal{V}(k(x)/k)$. Supongamos que $x \in \mathcal{O}_v$. Entonces $k[x] \subseteq \mathcal{O}_v$, por lo que $v(k[x]) \geq 0$. Aplicando el lema 5.2.13 debe existir un maximal M en $k[x]$ tal que $k[x]_M = \mathcal{O}_v$. Como $k[x]$ es de ideales principales cuyos generadores son polinomios irreducibles entonces M está generado por algún polinomio irreducible $g(x)$, y se obtiene que $v_{(g(x))} = v$, es decir, $v_{g(x)} = v$. Supongamos que $x \notin \mathcal{O}_v$. Entonces $v(x) < 0$, por lo que $v(1/x) > 0$ y se tiene $1/x \in \mathcal{M}_v$ (en particular, $k[1/x] \subseteq \mathcal{O}_v$). Notamos entonces que $1/x$ pertenece a $M_v \cap k[1/x]$, el cual es un ideal principal en $k[1/x]$, el cual está generado por algún polinomio irreducible (no constante) $f'(1/x)$. Por tanto, $1/x = f'(1/x)r(1/x)$, para algún $r(1/x) \in k[1/x]$. Se obtiene entonces que $f'(1/x) = s \cdot 1/x$, con $s \in k^*$, y $r(1/x) \in k^*$. Por tanto, $M_v \cap k[1/x] = P := (1/x)k[1/x]$. Aplicando el lema 5.2.13 (donde tomamos A igual al dominio de Dedekind $k[1/x]$), se obtiene que $v = v_P$, y aplicando el lema 2.2.7 se obtiene que $v_P = v_\infty$, y se obtiene el resultado. □

Lema 2.3.7. *Sea X/k una curva completa no singular asociada a una extensión $k(X)/k$ de grado de trascendencia 1. Sea $x \in k(X)$. Sea U el dominio de x (i.e., el conjunto de puntos P en X tales que $x \in \mathcal{O}_P$) y U' el dominio de $1/x$. Entonces $X = U \cup U'$.*

Demostración. Sea $P \in X$. Por el lema 1.14.5 se tiene que el dominio de ideales principales local $\mathcal{O}_P$ contiene a x o a $1/x$. Se obtiene entonces que $P \in U \cup U'$. □

Observación 2.3.8. *Sea $\mathbb{P}^1/k$ como en la proposición 2.3.6. Entonces el dominio U de x es igual a $\mathbb{P}^1 \setminus \{\infty\}$, y $\mathcal{O}_{\mathbb{P}^1}(U) = k[x]$. Para lo primero, basta notar que cada punto en $\mathbb{P}^1 \setminus \{\infty\}$ tiene asociado una valoración P-ádica, donde $P := (g(x))$ es un ideal maximal en $k[x]$ generado por un polinomio irreducible $g(x) \in k[x]$, y además que el ideal maximal (x) está contenido en $k[x]$, por lo que en su factorización aparecerá cada ideal maximal P elevado a algún entero $a_P \geq 0$, donde $a_P = 0$ para todos excepto para un número finito de ideales maximales P, y de la definición de v_P, se obtiene que $v_P(x) \geq 0$. Para lo segundo, basta aplicar el teorema 2.3.9.*

Teorema 2.3.9. *Sea X/k una curva completa no singular asociada a una extensión $k(X)/k$ de grado de trascendencia 1. Sea $x \in k(X)$ tal que $k(X)/k(x)$ es una extensión finita. Sea U el dominio de x . Entonces U es un abierto afín de X, y $\mathcal{O}_X(U)$ es la cerradura entera de $k[x]$ en $k(X)$ (con $k[x]$ el menor subanillo contenido en $k(X)$ que contiene a k y a x) . El complemento de U en X es el conjunto de puntos P tal que $\mathcal{O}_P \supset k[1/x]_{(1/x)}$.*

Demostración. Sea $P \in U$. Entonces $x \in \mathcal{O}_P$. Como $k \subseteq \mathcal{O}_P$ entonces $k[x] \subseteq \mathcal{O}_P$. Tenemos que $k(X)/k(x)$ es finita y por tanto es extensión algebraica. Como $k(X)$ contiene a un elemento que no es algebraico sobre k (por ser de grado de trascendencia 1, existe un elemento $y \in k(X)$ tal que $k(X)/k(y)$ es extensión finita y $k(y)$ es isomorfo como k-álgebras al campo de funciones racionales en una variable), se obtiene que x no es algebraico sobre k (si se tuviera x algebraico sobre k entonces $k(x)/k$ es extensión finita y por tanto $k(X)/k$ sería extensión finita, lo cual implica que $k(y)/k$ es finita y por tanto que y es algebraica sobre k, una contradicción). Como x no es algebraico sobre k entonces $k[x] \subset k(X)$ es un anillo de polinomios. Sea B la cerradura entera de $k[x]$ en $k(X)$. Como tenemos una biyección entre las valoraciones suprayectivas v de $k(X)$ y los dominios de ideales principales locales $\mathcal{O}_v$ cuyo campo de fracciones es $k(X)$ mediante $v \mapsto \mathcal{O}_v$ (teorema 2.2.8) entonces $\mathcal{O}_P$ (que es dominio de ideales principales) tiene a $k(X)$ como campo de fracciones, y como $\mathcal{O}_P$ es dominio de ideales principales entonces es dominio de Dedekind, y por tanto es enteramente cerrado en $k(X)$. Luego, como la cerradura entera respeta contenciones entonces $k[x] \subseteq \mathcal{O}_P \Rightarrow B \subseteq \mathcal{O}_P$. Aplicando la proposición 5.1.4 obtenemos que B es un $k[x]$-módulo finitamente generado, y por tanto, también es un dominio de Dedekind (teorema 5.2.11). En particular, B es una k-álgebra finitamente generada. Además, por ser B un dominio de Dedekind, del teorema 2.2.8, se tiene una biyección entre U y $\mathrm{Max}(B)$ y además $\mathcal{O}_X(U) = B$.

Así, sólo resta mostrar que U es abierto en X. Como B es dominio de Dedekind entonces U no es vacío ($B = \cap_{P \in U} \mathcal{O}_P$). Sea $P_0 \in X \setminus U$. Entonces $x \notin \mathcal{O}_{P_0} \Rightarrow v_{P_0}(x) < 0 \Rightarrow v_{P_0}(1/x) > 0$. Veamos que esto implica que $\mathcal{O}_{P_0} \supseteq k[1/x]_{(1/x)}$. Tenemos que $v_{P_0}(1/x) > 0 \Leftrightarrow \frac{1}{x} \in \mathcal{O}_{P_0} \Rightarrow k[1/x] \subseteq \mathcal{O}_{P_0}$ (pues $k^* \subseteq \mathcal{O}_{P_0}$), con $k[1/x]$ un anillo de polinomios ($1/x$ no es algebraico sobre k ya que x no lo es). Tomando la inclusión $\mathrm{i} : k[1/x] \to \mathcal{O}_{P_0}$, y como $k[1/x]$ es anillo de polinomios entonces es dominio de ideales principales (en particular, es dominio), por lo que se tiene que $j : k[1/x] \to k[1/x]_{(1/x)}$, $m \mapsto \frac{m}{1}$ es inyectivo, y como $k[1/x] \setminus (1/x) = k$ es invertible en $\mathcal{O}_{P_0}$ ($v_{P_0}(k^*) = 0$) entonces por la propiedad universal de anillos de fracciones (proposición 1.12.4) se tiene que $\exists g' : k[1/x]_{(1/x)} \to \mathcal{O}_{P_0}$ tal que $\mathrm{i} = g' \circ j \Rightarrow g'$ es inyectiva, por lo que $k[1/x]_{(1/x)} \hookrightarrow \mathcal{O}_{P_0}$, y por tanto $k[1/x]_{(1/x)} \subseteq \mathcal{O}_{P_0}$. Recíprocamente, si $P_0 \in X$ es tal que $k[1/x]_{(1/x)} \subseteq \mathcal{O}_{P_0}$, la inclusión $k[1/x] \hookrightarrow k[1/x]_{(1/x)}$ implica que $v_{P_0}(1/x) \geq 0$. Si ocurriera la igualdad entonces se tendría $v_{P_0}(x) = 0$, por lo que $x, 1/x \in \mathcal{O}_{P_0}$, y por tanto, se tendría que $(1/x) = \mathcal{O}_{P_0}$, lo cual es una contradicción pues $(1/x) \subset k[1/x]$. Por tanto, $v_{P_0}(1/x) > 0$ y se obtiene que $x \notin \mathcal{O}_{P_0}$, y $P_0 \in X \setminus U$.

Ahora, sea C la cerradura entera de $k[1/x]_{(1/x)}$ en $k(X)$. De nuevo por la proposición 5.1.4 se tiene que C es un dominio de Dedekind, con $k(X)$ campo de fracciones de C (para ver esto, notamos primero que por ser $k[1/x]$ dominio de Dedekind entonces su localización también es dominio de Dedekind. Además, como $k[1/x] \subseteq k[1/x]_{(1/x)} \subseteq k(x)$ entonces el campo de fracciones de $k[1/x]_{(1/x)}$ es $k(x)$, y la extensión $k(X)/k(x)$ es finita, por hipótesis. Aplicando la proposición 1.2.15 se obtiene que el resultado), y luego por el teorema 2.2.10 tenemos una correspondencia biyectiva entre los elementos de $\mathrm{Max}(C)$ y las valoraciones suprayectivas v_P de $k(X)$ con $v_P(C) \geq 0$. Además, $k[1/x]_{(1/x)} \subseteq \mathcal{O}_{P_0}$ y al ser $\mathcal{O}_{P_0}$ dominio de ideales principales, y por ende dominio de Dedekind entonces es enteramente cerrado, y como la cerradura entera respeta contenciones, se obtiene $C \subseteq \mathcal{O}_{P_0}$, y por tanto $v_{P_0}(C) \geq 0$. Así, v_{P_0} (que corresponde a P_0) tiene asociado un ideal maximal de C. Por tanto, cada punto P_0 perteneciente a $X \setminus U$ tiene asociado un ideal maximal de C. Por otro lado, como $k[1/x]_{(1/x)}$ es anillo local entonces C tiene un número finito de ideales maximales (de lo contrario, habría un número infinito de ideales $M \in \mathrm{Max}(C)$, y por la observación 1.5.7 se obtiene que $M \cap A = P := (\frac{1}{x})k[1/x]_{(1/x)}$, lo cual implica que $PC \subseteq M$, y esto para un número infinito de maximales $M \in \mathrm{Max}(C)$, pero por otro lado por ser C dominio de Dedekind, se tiene la factorización única de PC es un producto finito de ideales maximales $PC = M_1^{e_1} \cdots M_s^{e_s}$, y de la observación 1.17.7 se tendría una contradicción). Así, como C tiene un número finito de ideales maximales entonces $X \setminus U$ es igual a un número finito de puntos (y en particular, si $\mathcal{B}_1, \ldots, \mathcal{B}_s$ son los ideales maximales de C entonces $X \setminus U$ es igual al conjunto de puntos asociados a las valoraciones $\mathcal{B}_i$-ádicas $\{v_{\mathcal{B}_1}, \ldots, v_{\mathcal{B}_s}\}$). □

Corolario 2.3.10. *Una curva completa no singular X/k es la unión de dos subconjuntos abiertos afines.*

Demostración. Sea x como en el teorema 2.3.9. Entonces los dominios de x y $1/x$ son abiertos afines, donde notamos que $k(x) = k(1/x)$ y por tanto $k(X)/k(x)$ es extensión finita, y del teorema se obtiene que el dominio U' de $1/x$ también es abierto afín. Por el lema 2.3.7 se obtiene que los abiertos afines U y U' de x y $1/x$, respectivamente, cubren a X. □

Corolario 2.3.11. *Sea k cualquier campo. Sea $L/k(x)$ una extensión finita. Sean B y B' las cerraduras enteras de $k[x]$ y $k[1/x]$ en L, respectivamente. Sea $(1/x)B' = \prod_{i=1}^{s} \mathcal{B}_i^{e_i}$. Entonces*

$$\mathcal{V}(L/k) = \{v_{\mathcal{B}} \mid \mathcal{B} \in \mathrm{Max}(B)\} \sqcup \{v_{\mathcal{B}_1}, \ldots, v_{\mathcal{B}_s}\}$$

Demostración. Sean U y U' los dominios en X de x y $1/x$. Tenemos $X = U \cup U'$. Del teorema 2.3.9 se obtiene que $B = \mathcal{O}_X(U)$ y que hay una biyección entre

los puntos de U y los maximales de B (es decir, entre los puntos de U y las valoraciones $\mathcal{B}$-ádicas de L). Además, del mismo teorema 2.3.9 se obtiene que el complemento de U son todos los puntos P tales que $\mathcal{O}_P \supseteq k[1/x]_{(1/x)}$ (en particular, $\mathcal{O}_P \supseteq (1/x)$), y además notamos que todos estos puntos estn contenidos en U', y por el teorema 2.3.9 se obtiene que cada uno corresponde a un ideal maximal de B' (pues los puntos de U' están en biyección con los ideales maximales de $B' = \mathcal{O}_X(U')$). Sea $\mathcal{B}_i$ el ideal maximal de B' correspondiente a un punto perteneciente a $X \setminus U$. Entonces $\mathcal{O}_{v_{\mathcal{B}_i}} \supseteq k[1/x]_{(1/x)}$. Queremos ver entonces que $\mathcal{B}_i \supseteq \frac{1}{x}B'$ (notamos que de la conmutatividad se obtiene que $(1/x)B' = \frac{1}{x}B'$), pues implicaría que $\mathcal{B}_i$ aparece en la factorización de $(1/x)B'$ en ideales maximales de B'. Como $k[1/x] \hookrightarrow k[1/x]_{(1/x)}$ entonces $v_{\mathcal{B}_i}(1/x) \geq 0$. No podría ocurrir la igualdad, pues eso implicaría que $v_{\mathcal{B}_i}(x) = 0$, por lo que $x, 1/x \in \mathcal{O}_{v_{\mathcal{B}_i}}$, y entonces $(1/x) = \mathcal{O}_{v_{\mathcal{B}_i}}$, lo cual no es posible pues $(1/x) \subset k[1/x]$. Por tanto, $v_{\mathcal{B}_i}(1/x) > 0$ y $1/x \in \mathcal{M}_{v_{\mathcal{B}_i}}$. Del teorema 2.3.9 y su demostración se obtiene que $\mathcal{M}_{v_{\mathcal{B}_i}} \cap B' = \mathcal{B}_i$, y como $1/x \in k[1/x] \subseteq B'$ y $\mathcal{B}_i$ es un ideal maximal en B' entonces se obtiene $\frac{1}{x}B' \subseteq \mathcal{B}_i$. Recíprocamente, si un ideal maximal $\mathcal{B}_i$ de B' aparece en la factorización de $(1/x)B'$ entonces en particular contiene al elemento $1/x$. Como $v_{\mathcal{B}_i}$ es la valoración $\mathcal{B}_i$-ádica entonces $v_{\mathcal{B}_i}(\mathcal{B}') \geq 0$, por lo que $v_{\mathcal{B}_i}(1/x) \geq 0$, y obtenemos como antes que $v_{\mathcal{B}_i}(1/x) > 0$. Así, $v_{\mathcal{B}_i}(x) < 0$, y por tanto $v_{\mathcal{B}_i}$ corresponde a un punto en $X \setminus U$. Se obtiene así el resultado. □

Corolario 2.3.12. *Sea k cualquier campo. Sea $L/k(x)$ una extensión finita. Sea $v \in \mathcal{V}(L/k)$. Entonces el grado $[k_v : k]$ es finito.*

Demostración. Notamos que el corolario se cumple en el caso $L = k(x)$ (se obtiene $k_v := \mathcal{O}_v/\mathcal{M}_v = k$). Sean B y B' las cerraduras enteras de $k[x]$ y $k[1/x]$ en L, respectivamente. Por el corolario 2.3.11 basta probar el caso en que v es la valoración $\mathcal{B}$-ádica asociada a algún maximal $\mathcal{B} \in \mathrm{Max}(B)$ (y análogamente, para el caso $\mathcal{B}_i \in \mathrm{Max}(B')$, $i = 1, \ldots, s$, del corolario 2.3.11). Sea $P := \mathcal{B} \cap k[x]$. Notamos que la dimensión de $k[x]/P$ es finita sobre k (igual al grado del polinomio mónico e irreducible que genera al ideal maximal P). Por tanto, resta ver que $f_{\mathcal{B}/P}$ es finita ya que por ser L el campo de fracciones de B y del teorema 2.2.10 se tendría entonces

$$[k_v : k] = [\mathcal{O}_v/\mathcal{M}_v : k] = [B/\mathcal{B} : k] = [B/\mathcal{B} : k[x]/P][k[x]/P : k]$$

El entero $f_{\mathcal{B}/P}$ es finito cuando B es un $k[x]$-módulo finitamente generado. Cuando $L/k(x)$ es separable entonces del teorema 1.4.6, se obtiene que B es un $k[x]$-módulo finitamente generado. Sin embargo, la proposición 5.1.4 asegura que B siempre es un $k[x]$-módulo finitamente generado. □

Observación 2.3.13. *Sea $X/\overline{k}$ una curva completa no singular. Sea $P \in X$. Del corolario 2.3.12 se obtiene que la composición $\overline{k} \subset \mathcal{O}_P \to \mathcal{O}_P/\mathcal{M}_P$ es un*

isomorfismo. Identificamos el cociente $\mathcal{O}_P/\mathcal{M}_P$ *con el campo* $\overline{k}$ *utilizando el inverso de este isomorfismo. Dado* $\alpha \in \overline{k}(X)$ *definido en* P*, llamamos el valor de la función* α *en* P*, denotado por* $\alpha(P)$*, al elemento de* $\overline{k}$ *correspondiente a la clase de* α *módulo* $\mathcal{M}_P$*.*

2.4. Campos de funciones 1

Sea $f \in k[x,y]$ un polinomio irreducible. Tomando $C_f := k[x,y]/(f)$, denotamos por $k(Z_f)$ al campo de fracciones de C_f.

Definición 2.4.1. *Sea L/k una extensión de campos. Decimos que k es algebraicamente cerrado en L si los únicos elementos de L algebraicos sobre k son los elementos de k mismo.*

Notamos que si k es un campo algebraicamente cerrado entonces k es algebraicamente cerrado en L para cualquier extensión L/k.

Sea $k(x)$ el campo de funciones racionales sobre k. Entonces k es algebraicamente cerrado en $k(x)$, ya que si $f, g \in k[x]$ son tales que f/g es algebraico sobre k entonces se cumple $a_n(f/g)^n + a_{n-1}(f/g)^n + \ldots + a_1(f/g) + a_0 = 0$ para algunos $a_i \in k$. Sin pérdida de generalidad, podemos asumir que f, g no tienen factores en común, y entonces $a_n f^n + \ldots + a_1 f g^{n-1} + a_0 g^n = 0$ y se obtiene que $f \mid g$ y $g \mid f$, y por tanto $f/g \in k$.

Lema 2.4.2. *Sea $f \in k[x,y]$.*

- *i) Supongamos que $f = gh$ en $\bar{k}[x,y]$, con $g \in k[x,y]$. Entonces $h \in k[x,y]$.*
- *ii) Supongamos que f es divisible por un polinomio irreducible g en $\bar{k}[x,y]$, y supongamos que g tiene al menos un coeficiente en k. Sea E la extensión de k generado por los coeficientes de g.*

  a) Si ocurre que E/k es separable, y $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ son representantes de las clases $\mathrm{Gal}(\bar{k}/k)/\mathrm{Gal}(\bar{k}/E)$ entonces $\prod_{i=1}^n \sigma_i(g(x,y))$ pertenece a $k[x,y]$ y divide a $f(x,y)$.

  b) Si E/k es puramente inseparable de grado p^e, y si $r \geq 1$ es el entero más chico tal que $g^{p^r} \in k[x,y]$ (de la definición de puramente inseparable se tiene $r \leq e$) entonces g^{p^r} es irreducible en $k[x,y]$ y divide a f.

Demostración. i) Tenemos que $h = f/g \in k(x,y)$, y entonces $h \in k(x,y) \subseteq \bar{k}(x,y)$ y $h \in \bar{k}[x,y]$. Se obtiene entonces que $h \in k[x,y]$.

ii) a) Como $f \in k[x,y]$, tenemos que $\sigma_i(g)$ divide a f para toda $1 \leq i \leq n$. Además, $\sigma_i \neq \sigma_j$ si $i \neq j$, ya que E es el generado por los coeficientes de g y si ocurriera $\sigma_i(g) = \sigma_j(g)$ entonces $(\sigma_i \circ \sigma_j^{-1})(E) = E$ y por tanto σ_i y σ_j estarían en la misma clase, contradiciendo la hipótesis. Además, como g tiene al menos un coeficiente en k se obtiene que σ_i no puede ser un múltiplo constante de α_j si $i \neq j$ (pues σ_i, σ_j fijan a dicho elemento en k). Así, se obtiene $\prod_{i=1}^n \sigma_i(g)$ divide a f.

b) Sea E/k puramente inseparable. Sea r el menor entero positivo tal que $\alpha^{p^r} \in k$ para todos los coeficientes α de g. Entonces $g^{p^r} \in k[x,y]$ es irreducible, ya que los únicos factores de g^{p^r} son de la forma g^i con $i \leq p^r$, y ninguno de

estos factores pertenece a $k[x,y]$ si $i < p^r$. Sea h un factor irreducible de g (en $k[x,y]$) divisible por g en $\bar{k}[x,y]$. Entonces g^{p^r} divide a h^{p^r}. Como g^{p^r} es irreducible en $k[x,y]$, se obtiene que g^{p^r} divide a h, y por tanto divide a f. $\square$

Proposición 2.4.3. *Sea k cualquier campo. Sea $f \in k[x,y]$ irreducible. Supongamos que $g \in \bar{k}[x,y]$ es irreducible y divide a f, y supongamos que al menos uno de los coeficientes de g pertenece a k. Sea E el campo que se obtiene adjuntando a k los coeficientes de g, y sea $E_0 \subseteq E$ el subcampo maximal de E que es separable sobre k. Entonces:*

- *i) El campo $k(Z_f)$ contiene un subcampo isomorfo a E_0, es decir, existe un homomorfismo de campos $\varphi : E_0 \to k(Z_f)$ tal que $\varphi_{|k} = \mathrm{Id}_{|k}$*
- *ii) Si existe un coeficiente γ de g tal que $E = E_0(\gamma)$ entonces $k(Z_f)$ contiene un subcampo isomorfo a E.*

Demostración. Supongamos primero que E/k es separable, es decir, $E = E_0$. Sea $\{\sigma_1, \ldots, \sigma_n\}$ el conjunto de representantes de $\mathrm{Gal}(\bar{k}/k)/\mathrm{Gal}(\bar{k}/E)$. Del lema 2.4.2, inciso ii), subinciso a) se obtiene que $f = c\prod_{i=1}^{n} \sigma_i(g)$ en $k[x,y]$, con $c \in k^*$. Consideramos la función natural $\mathrm{i} : k[x,y]/(f) \to E[x,y]/(g)$. Notamos que i es inyectiva, ya que si $h \in k[x,y]$ es divisible por $g(x,y)$ en $E[x,y]$ entonces del lema 2.4.2,ii),a) se obtiene que $f(x,y)$ divide a $h(x,y)$.

Ahora, como i es inyectiva, induce una función (inyectiva) i entre los campos de fracciones correspondientes. Notamos primero que se cumple la proposición cuando g es lineal en $\bar{k}[x]$, ya que en este caso tendríamos $g(x) = x - a$, para algún $a \in \bar{k} \setminus k$. Entonces $E_0 = E = k(a)$, y como a no es algebraico sobre k entonces $k(a)$ es isomorfo como k-álgebra al campo de funciones racionales $k(x) \hookrightarrow k(Z_f)$. Se obtiene de lo anterior que i) y ii) se cumplen. Supongamos entonces que g no es un polinomio en $\bar{k}[x]$, o equivalentemente, que $E[x]$ se inyecta en $E[x,y]/(g)$. Sean $\deg_y(g)$ y $\deg_y(f)$ los grados en y de los polinomios $g(x,y)$ y $f(x,y)$, respectivamente. Notamos que $\deg_y(f) = n\deg(g)$. Además, $[k(Z_f) : k(x)] = \deg_y(f)$ y $[E(Z_g) : E(x)] = \deg_y(g)$. Del lema 2.4.5 abajo se obtiene que $[E(x) : k(x)] = [E : k] = n$, y como $E(Z_g)$ es una extensión de $k(Z_g)$ (mediante la función inyectiva i), se obtiene entonces que $[E(Z_g) : k(Z_g)] = 1$, y por lo tanto la función i es un isomorfismo. Luego, $k(Z_f)$ contiene a un subcampo isomorfo a E siempre que E/k sea separable.

Supongamos ahora que $[E : E_0] = p^e > 1$, y sea r el menor entero tal que $g^{p^r} \in E_0[x,y]$. Entonces g^{p^r} es irreducible en $E_0[x,y]$ y divide a f (por el lema 2.4.2, ii, b)). Tenemos que E_0 es el subcampo de $\bar{k}$ que se obtiene adjuntando a k los coeficientes de g^{p^r}, y entonces aplicando el procedimiento seguido anteriormente al caso g^{p^r}, se obtiene que que $k(Z_f)$ es isomorfo a $E_0(Z_{g^{p^r}})$ sobre k.

Consideramos el siguiente diagrama:

$$\begin{array}{ccc} E_0(x)[y]/(g^{p^r}) & \longrightarrow & E(x)[y]/(g) \\ \uparrow{\scriptstyle p^r \deg_y(g)} & & \uparrow{\scriptstyle \deg_y(g)} \\ E_0(x) & \xrightarrow{p^e} & E(x) \end{array}$$

donde las flechas indican las extensiones y los valores junto a las flechas indican el grado de la extensión.

Por el lema 2.4.5 que se verá después, se tiene que $[E(x) : E_0(x)] = [E : E_0]$, y entonces del diagrama se obtiene que $E(x)[y]/(g)$ tiene grado p^{e-r} sobre $E_0(x)[y]/(g^{p^r})$. Además, si existe γ coeficiente de g tal que $E = E_0(\gamma)$ entonces se tiene que $e = r$ (pues notamos que $r \leq e$ y $g^{p^r} \in E_0 \Rightarrow \lambda^{p^r} \in E_0$, pero el polinomio mínimo de λ sobre E_0 es de la forma $x^{p^n} - a \in E_0[x]$, por ser E/E_0 puramente inseparable, y tiene grado p^e, pues $E = E_0(\lambda)$ y $[E : E_0] = p^e$, por lo que $n = e$ y se obtiene entonces que $e \leq r$), y por lo tanto, $E_0(x)[y]/(g^{p^r})$ es isomorfo a $E_(x)[y]/(g)$. Se obtiene entonces que $k(Z_f)$ es isomorfo a $E(Z_g)$. Por lo tanto, $k(Z_f)$ contiene a una copia de E. □

Observación 2.4.4. *Sea E/F cualquier extensión finita, y sea $\alpha \in E$. Sea $f(y) \in F[y]$ el polinomio mínimo de α sobre F. Entonces $f(y)$ también es el polinomio mínimo de α sobre $F(x)$. Para verlo, sea $g(y) \in F(x)[y]$ el polinomio mínimo de α sobre $F(x)$. Notamos que $f(\alpha) = 0 = g(\alpha)$, y además que $f(y) \in F[y] \subseteq F(x)[y]$, y se obtiene entonces que $g|f$. Por tanto, $g(y) \in F[y]$, y se obtiene entonces que $f|g$. Obtenemos entonces que $f = g$.*

Lema 2.4.5. *Sea E/k cualquier extensión algebraica. Entonces las extensiones $E(x)/k(x)$ y E/k son ambas o de grado infinito, o de grado finito, y en este último caso se cumple $[E(x) : k(x)] = [E : k]$.*

Demostración. Supongamos que E/k no es una extensión finita. Sea $k \subset E_1 \subset \ldots \subset E_n \subset \ldots \subset E$ una cadena de subextensiones distintas de E/k. Consideramos la cadena $k(x) \subset E_1(x) \subset \ldots \subset E_n(x) \subset \ldots \subset E(x)$. Como E_i es algebraicamente cerrada en $E_i(x)$ pero ya no es algebraicamente cerrada en $E_{i+1}(x)$ (pues $E_i \subset E_{i+1} \subset E_{i+1}(x)$ y E_{i+1}/E_i es extensión algebraica) entonces $E_i(x) \neq E_{i+1}(x)$, y por tanto $E(x)/k(x)$ no es extensión finita.

Supongamos ahora que E/k es una extensión finita. Entonces se obtiene que $E = k(\alpha_1, \ldots \alpha_s)$ y consideramos la cadena $k(x) \subset k(x)(\alpha_1) \subset \ldots \subseteq k(x)(\alpha_1, \ldots, \alpha_s) = E(x)$. Queremos ver primero que si $F(\alpha)/F$ es cualquier extensión algebraica entonces $[F(\alpha)(x) : F(x)] = [F(\alpha) : F]$. Para verlo, sea $f(y) \in F[y]$ el polinomio mínimo de α sobre F. Por la observación 2.4.4 tenemos que $f(y)$ también es el polinomio mínimo de α sobre $F(x)$. Obtenemos entonces que $[F(\alpha)(x) : F(x)] = \deg(f) = [F(\alpha) : F]$, y aplicando esto a cada contención de la cadena $k(x) \subset k(x)(\alpha_1) \subset \ldots \subseteq k(x)(\alpha_1, \ldots, \alpha_s) = E(x)$, se obtiene que $[E(x) : k(x)] = [E : k]$. □

Lema 2.4.6. *Sea k cualquier campo. Sea $L/k(x)$ una extensión finita. Sea E la cerradura algebraica de k en L. Entonces E/k es una extensión finita.*

Demostración. Notamos que $k(x) \subseteq E(x) \subseteq L$. Como $L/k(x)$ es finita entonces también $E(x)/k(x)$ es finita. Por el lema 2.4.5 se obtiene entonces que E/k también es finita. □

Proposición 2.4.7. *Sea k cualquier campo. Sea $f \in k[x,y]$ un polinomio irreducible. Sea E/k la maxima extensión algebraica de k contenida en $k(Z_f)$. Entonces E/k es una extensión finita, y f se factoriza en $\bar{k}[x,y]$ como un producto de $[E:k]$ polinomios irreducibles. Más aún, existe un factor irreducible g de f que tiene al menos un coeficiente en k tal que E es el subcampo de $k(Z_f)$ generado por los coeficientes de g. Además, si E_0 es la maxima extensión separable de k contenida en E entonces E/E_0 es extensión simple y f es una $[E:E_0]$-ésima potencia en $\bar{k}[x,y]$.*

Demostración. Se puede verificar que la proposición se cumple en el caso $f \in k[x]$. Supongamos que $\deg_y(f) > 0$. Entonces $k(Z_f)/k(x)$ es una extensión finita. Tenemos que $k(Z_f) = E(x)(y)$. Sea $h(x,Y) \in E(x)[Y]$ el polinomio mínimo de y sobre $E(x)$. Entonces $h(x,Y)$ divide a $f(x,Y)$ en $E(x)[Y]$ (pues $f(x,Y)_{|_y} = 0$ en $k(Z_f) = E(x)(y)$). Por el lema de Gauss, se obtiene que $g(x,Y) := \mathrm{cont}(h(x,Y))^{-1}h(x,Y) \in E[x][Y]$ divide a $f(x,Y)$ (pues $f = hh'$, con $f \in k[x,Y] \subseteq E[x][Y]$, y $h, h' \in E(x)[Y]$, y por el corolario 1.26.4 se tiene que $f = \mathrm{cont}(f)h_1h_1'$, con $h_1, h_1' \in E[x][Y]$, donde en particular $h = \mathrm{cont}(h)h_1$, y por tanto $\mathrm{cont}(h)^{-1}h = h_1 \in E[x][Y]$ divide a f en $E[x][Y]$. Por tanto,

$$\deg_Y(f) = [k(Z_f) : k(x)] = [k(Z_f) : E(x)][E(x) : k(x)] = \deg_Y(g)[E : k]$$

donde en la última igualdad se usó que $[k(Z_f) : E(x)] = [E(x)(y) : E(x)] = \deg_Y(h) = \deg_Y(g)$.

Podemos asumir, sin pérdida de generalidad, que uno de los coeficientes no cero de g pertenece a k (podemos multiplicar g por el inverso de algún coeficiente de g, obteniendo $1 \in k$). Sea F la extensión de k generada por los coeficientes de g. Sea F_0 la maxima extensión separable de k contenida en F. Sea r el menor entero tal que $g^{p^r} \in F_0[x,y]$. Sean $\sigma_1, \ldots, \sigma_s$ los distintos encajes de F_0 en $\bar{k}$. Por el lema 2.4.2 inciso ii) se obtiene que $f = c(\sigma_1(g) \cdots \sigma_s(g))^{p^r}$. se obtiene entonces que $\deg_Y(f) = p^r[F_0 : k]\deg_Y(g)$. Como $F \subseteq E$ (pues F está generado por los coeficientes de g, entre ellos un coeficiente de k, por lo que F/k es una extensión finita y por tanto algebraica), se obtiene que $F = E$ y que $F_0 = E_0$. Como $[E : E_0] = p^r$, obtenemos que el polinomio mínimo sobre E_0 de al menos un coeficiente a de g es de la forma $y^{p^r} - a^{p^r}$ (pues E/E_0 es puramente inseparable). Por tanto, $E = E_0(a)$. □

Teorema 2.4.8. *Sea k un campo perfecto. Sea $f \in k[x,y]$ irreducible. Entonces k es algebraicamente cerrado en $k(Z_f)$ si y sólo si f es absolutamente irreducible.*

Demostración. Tenemos que si k no es algebraicamente cerrado en $k(Z_f)$ entonces f no es absolutamente irreducible, ya que si fuera absolutamente irreducible entonces por la proposición 2.4.7 sabemos que existe g factor irreducible de f con al menos un coeficiente en k tal que E está generado por los coeficientes de g (donde E es la máxima extensión algebraica de k contenida en $k(Z_f)$), pero por ser f absolutamente irreducible se obtiene que $f = \alpha g$, $\alpha \in \overline{k}$, $\alpha \neq 0$. Observamos entonces que cualquier coeficiente de f es el producto de α por un coeficiente de g, y como $f \in k[x,y]$ y g tiene al menos un coeficiente en k, se obtiene que $\alpha \in k$. De aquí, se obtiene que $g \in k[x,y]$, y por tanto $E = k$, contradiciendo que k no es algebraicamente cerrado en $k(Z_f)$.

Supongamos ahora que f no es absolutamente irreducible. Sea $g \in \bar{k}[x,y]$ un factor irreducible de f. Podemos asumir que al menos uno de los coeficientes de g pertenece a k. Tenemos por hipótesis que $E \neq k$, y entonces sea $E_0 \subseteq E$ la máxima extensión separable de k contenida en E. Por la proposición 2.4.3, se tiene que $k(Z_f)$ contiene a un subcampo isomorfo a E_0, y como k es perfecto, se obtiene que $E_0 = E$, y por tanto $E_0 \neq k$. De aquí, se obtiene que k no puede ser algebraicamente cerrado en $k(Z_f)$ (pues de la definición de que E_0 sea separable sobre k se tiene, en particular, que es una extensión algebraica). □

Lema 2.4.9. *Sea k cualquier campo. Sean $L/k(x)$ y $K/k(y)$ dos extensiones finitas. Supongamos que $k(x)$ y $k(y)$ son ambos isomorfos al campo de funciones racionales en una variable, y supongamos que $K \subseteq L$. Entonces L/K es una extensión finita. En particular, si α no es algebraico sobre k entonces $L/k(\alpha)$ es una extensión finita.*

Demostración. Como $L/k(x)$ es finita, se obtiene que $k(x,y)/k(x)$ también es finita. Sea $f(x,Y) \in k(x)[Y]$ el polinomio mínimo de y sobre $k(x)$. Notamos que y no es algebraico sobre k ($k(x)$ y $k(y)$ isomorfos al campo de funciones racionales en una variable), por lo que se tiene $f \notin k[Y]$. Por tanto, x es algebraico sobre $k(y)$ y por tanto la extensión $k(x,y)/k(y)$ es finita, y como $L/k(x,y)$ es finita, se obtiene que $L/k(y)$ también es finita, y de aquí se obtiene que L/K es finita.

Si α no es algebraico sobre k entonces $k(\alpha)$ es un campo de funciones racionales en una variable sobre k, y aplicando un procedimiento análogo a lo anterior al caso $K = k(\alpha)$, $x = y = \alpha$, obtenemos el caso particular. □

Lema 2.4.10. *Sea L/K una extensión algebraica. Sea $v : L^* \to \mathbb{Z}$ una valoración. Si $v|_{K^*}$ es trivial entonces v es trivial en todo L^*.*

Demostración. Veamos primero lo siguiente: si $a, b \in L$ y $v(a) \neq v(b)$ entonces $v(a+b) = \min\{v(a), v(b)\}$. Tenemos que $v(a+b) \geq \min\{v(a), v(b)\}$. Podemos asumir que $v(a) > v(b)$. Supongamos que $v(a+b) > v(b)$. Tenemos

$$v(b) = v(a+b-a) \geq \min\{v(a+b), v(-a)\} = \min\{v(a+b), v(a)\} > v(b)$$

donde la segunda igualdad se tiene porque $v(-a) = v((-1)\cdot a) = v(-1)+v(a) = v(a)$, y la última desigualdad se tiene porque $v(a), v(a+b) > v(b)$ (por hipótesis). De la contradicción obtenida, se obtiene el resultado.

Ahora, sea $\alpha \in L$, y sea $f(x) = a_n x^n + \cdots + a_0 \in K[x]$ tal que $f(\alpha) = 0$. Supongamos que $v(\alpha) \neq 0$. Notamos entonces que $v(a_i\alpha^i) \neq v(a_j\alpha^j)$ si $i \neq j$. Utilizando lo mencionado antes, se obtiene entonces que

$$\infty = v(0) = v(f(\alpha)) = \min\{v_1(a_1\alpha), \ldots, v_n(a_n\alpha^n)\} = v(a_k)+v(\alpha^k) = kv(\alpha) < \infty$$

para algún $1 \leq k \leq n$. De la contradicción, se obtiene el lema. □

Teorema 2.4.11. *Sea k cualquier campo. Sea L/k de grado de trascendencia uno sobre k. Sea $\mathcal{V}(L/k)$ el conjunto de valoraciones suprayectivas $v : L^* \to \mathbb{Z}$ triviales en k. Sea $k' \subseteq L$ la máxima extensión algebraica de k contenida en L. Entonces k'/k es finita y*

$$k' = \bigcap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v$$

Demostración. Como L/k es de grado de trascendencia 1, existe $x \in L$ tal que $L/k(x)$ es finita y $k(x)$ es isomorfo al campo de funciones racionales en una variable sobre k. Aplicando entonces el lema 2.4.6 obtenemos que k'/k es finita. Sea $\alpha \in L$ algebraico sobre k. Como $v \in \mathcal{V}(L/k)$ entonces por el lema 2.4.10 se obtiene que $v(\alpha) = 0$. Por tanto, $\alpha \in \mathcal{O}_v$ $\forall v \in \mathcal{V}(L/k)$ y se tiene $\alpha \in \bigcap_{v\in\mathcal{V}(L/k)} \mathcal{O}_v$. Ahora, sea $\alpha \in \bigcap_{v\in\mathcal{V}(L/k)} \mathcal{O}_v$ pero supongamos que $\alpha \notin k'$. Por el caso particular del lema 2.4.9 se obtiene que $L/k(\alpha)$ es finita. Sea B' la cerradura entera de $k[1/\alpha]$ en L. Por la proposición 5.1.4 se tiene que B' es un $k[1/\alpha]$-módulo finitamente generado. Tenemos que el ideal $(1/\alpha)$ en $k[1/\alpha]$ es no trivial, y por tanto podemos factorizar en un producto no vacío de ideales maximales al ideal generado $(1/\alpha)B' = \mathcal{B}_1^{e_1} \cdots \mathcal{B}_s^{e_s}$. Entonces $0 < e_1 = v_{\mathcal{B}_1}(1/\alpha)$, y se obtiene por tanto que $v_{\mathcal{B}_1}(\alpha) = -v_{\mathcal{B}_1}(1/\alpha) < 0$, contradiciendo el hecho de $\alpha \in \mathcal{O}_{v_{\mathcal{B}_1}}$. Por tanto, se debe tener que $\alpha \in k'$. □

Proposición 2.4.12. *Sea k cualquier campo. Sea L/k una extensión de grado de trascendencia 1 sobre k. Sea $\alpha \in L^*$. Entonces el conjunto*

$$\{v \in \mathcal{V}(L/k) | v(\alpha) \neq 0\}$$

es un conjunto finito.

Demostración. Supongamos que $S := \{v \in \mathcal{V}(L/k) | v(\alpha) < 0\}$ es finito. Si hubiera algún α tal que $v(\alpha) > 0$ para una infinidad de v entonces $0 = v(1) = v(\alpha\alpha^{-1}) = v(\alpha) + v(\alpha^{-1}) \Rightarrow v(\alpha^{-1}) < 0$ para una infinidad de v, lo que contradice la hipótesis. Por tanto, $\{v \in \mathcal{V}(L/k) | v(\alpha) > 0\}$ es finito y por tanto $\{v \in \mathcal{V}(L/k) | v(\alpha) \neq 0\}$ también lo es.

Ahora veamos que $\forall \alpha \in L^*$ el conjunto S es finito. Sea $\alpha \in L^*$. Si S es vacío entonces $v(\alpha) \geq 0\ \forall v \in \mathcal{V}(L/k) \Rightarrow \alpha \in \bigcap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v$ y por el teorema 2.4.11 se tiene que α es algebraico sobre k y por el lema 2.4.10 se obtiene $v(\alpha) = 0$ $\forall v \in (L/k)$, por lo que se cumple lo que se quería en este caso.

Si S no es vacío entonces por teorema 2.4.11 se tiene que α no es algebraico sobre k, y por el lema 2.4.9 se tiene que $L/k(\alpha)$ es una extensión finita. Sea B' la cerradura entera de $k[1/\alpha]$ en L (i.e., el anillo formado por los elementos en L que son raíz de algún polinomio mónico con coeficientes en $k[1/\alpha]$). Por la proposición 5.1.4 se tiene que B' es un $k[1/\alpha]$-módulo finitamente generado. Factorizando el ideal generado por $1/\alpha$ en B', $(1/\alpha)B'$, en un producto de ideales maximales se tiene $(1/\alpha)B' = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_s^{e_s}$ $(e_\mathrm{i} > 0)$ y como $v_{\mathfrak{B}_\mathrm{i}}(1/\alpha) = e_\mathrm{i} > 0$ entonces $v_{\mathfrak{B}_\mathrm{i}}(\alpha) < 0\ \forall \mathrm{i} = 1, 2, \dots, s$. Notamos que las $v_{\mathfrak{B}_\mathrm{i}}$ son las únicas valoraciones tales que $v_{\mathfrak{B}_\mathrm{i}}(\alpha) > 0$, ya que si hubiera otra valoración $v_\mathfrak{B}$ con $v_\mathfrak{B}(\alpha) < 0$ entonces $v_\mathfrak{B}(1/\alpha) > 0$ y por tanto el ideal $\mathfrak{B}^{v_\mathfrak{B}(1/\alpha)}$ debe aparecer en la factorización de $(1/\alpha)B'$, y por la unicidad de la factorización se tiene $\mathfrak{B}^{v_\mathfrak{B}(1/\alpha)} = \mathfrak{B}_\mathrm{i}^{e_\mathrm{i}}$ para algún i. Como α pertenece a la cerradura entera B de $k[\alpha]$ en L entonces $v(\alpha) \geq 0$ si v es una valoración tal que $\mathcal{O}_v \supset B$. Por el teorema 2.3.9 y el corolario 2.3.11 se obtiene que $\mathcal{V}(L/k) = \{v | \mathcal{O}_v \supset B\} \sqcup \{v_{\mathfrak{B}_1}, \dots, v_{\mathfrak{B}_s}\}$ y de aquí se obtiene que S es finito. □

Recordamos la siguiente definición que ya teníamos desde antes: Sea k cualquier campo. Decimos que una extensión L/k es un campo de funciones sobre k si L es de grado de trascendencia 1 sobre k, y si k es algebraicamente cerrado en L.

Sea X/k cualquier curva completa no singular. Notamos entonces que $k(X)/k$ es campo de funciones (ya que $\mathcal{O}_X(X) = k$, donde recordamos que si $U \subseteq X$ es un abierto no vacío entonces $\mathcal{O}_X(U) := \bigcap_{P \in U} \mathcal{O}_P$, llamado anillo de funciones sobre U). Llamamos a los elementos de k las funciones constantes sobre X, y al campo k lo llamamos el campo de constantes del campo de funciones $k(X)$.

Ahora, sea X/k una curva completa no singular, y consideramos $\overline{k(X)}$ una cerradura algebraica fija de $k(X)$. Sea $\bar{k}$ la cerradura algebraica de k contenida en $\overline{k(X)}$. Notamos entonces que $\bar{k}$ es algebraicamente cerrado y por tanto $\bar{k}$ es una cerradura algebraica de k. Sea $k' \subset \bar{k}$ cualquier extensión de k. Denotamos por $k'(X)$ al producto $k' \cdot k(X)$, es decir, al subcampo de $\overline{k(X)}$ generado por k' y $k(X)$.

Lema 2.4.13. *Sea k un campo perfecto y sea $k(X)/k$ un campo de funciones. Si k'/k es cualquier extensión de k en $\bar{k}$ entonces $k'(X)/k'$ es un campo de funciones. Más aún, si la extensión k'/k es finita entonces $[k'(X) : k(X)] =$*

$[k' : k]$.

Demostración. Sea $x \in k(X)$ tal que $k(X)/k(x)$ es una extensión finita separable (corolario 5.1.7). Sea $y \in k(X)$ tal que $k(X) = k(x)(y)$ (corolario 5.1.7). Sea $f(x, Y) \in k(x)[Y]$ el polinomio mínimo de y sobre $k(x)$. Sin pérdida de generalidad, podemos asumir que $f \in k[x, Y]$. Entonces, como k es perfecto y algebraicamente cerrado en $k(X)$, podemos aplicar el teorema 2.4.8 para obtener que $f(x, Y)$ es absolutamente irreducible. De aquí, se obtiene que $[k'(X) : k'(x)] = \deg_Y(f) = [k(X) : k(x)]$ (donde la primera igualdad se obtiene notando que $k'(X) = k'(x)(y)$ y que el polinomio mínimo de y sobre $k'(x)$ sigue siendo igual a $f(x, Y)$ por ser un polinomio absolutamente irreducible, y por tanto irreducible en $k'[x, Y]$, donde se anula y).

Supongamos que la extensión k'/k es finita. Del lema 2.4.5 obtenemos que $[k'(x) : k(x)] = [k' : k]$, y como $k'(x)/k(x)$ es finita, similarmente obtenemos que $[k'(X) : k(X)] = [k'(x) : k(x)]$. Por tanto, $[k'(X) : k(X)] = [k' : k]$. Sea E la máxima extensión algebraica de k' en $k'(X)$. Entonces $k'(X) = E(X)$. Haciendo un procedimiento similar a lo anterior aplicado a la extensión E/k, podemos obtener que $[E(X) : k(X)] = [E : k]$. Y como $[k' : k] = [k'(X) : k(X)] = [E(X) : k(X)] = [E : k]$, se obtiene que $E = k'$. Por tanto, $k'(X)/k'$ es un campo de funciones.

Supongamos ahora que k'/k no es necesariamente finito. Sea $\alpha = \sum_{i=1}^{s} a_i \gamma_i$ un elemento de $k'(X)$ algebraico sobre k', con $a_i \in k'$ y $\gamma_i \in k(X)$, $\forall i = 1, \ldots, s$. Sea $F := k(a_1, \ldots, a_s)$. Entonces $\alpha \in F(X)$. Aplicando el caso anterior, tenemos que $F(X)/F$ es campo de funciones, por lo que debe ocurrir que $\alpha \in F$, pero notamos que $F \subset k'$, por lo que $\alpha \in k'$. Se obtiene que $k'(X)/k'$ es campo de funciones. □

Con todo lo visto en esta sección, podemos dar la siguiente definición.

Definición 2.4.14. *Sea k campo perfecto. Consideramos X/k una curva completa no singular con $k(X)/k$ su campo de funciones asociado, y fijamos una cerradura algebraica $\overline{k(X)}$ de $k(X)$. Sea k'/k cualquier extensión algebraica de k contenida en la cerradura algebraica $\overline{k}$ de k contenida en $\overline{k(X)}$, y consideramos el campo $k'(X) = k' \cdot k(X)$. Sea $X_{k'}/k'$ la curva completa no singular asociada al campo de funciones $k'(X)/k'$. Decimos que la curva $X_{k'}/k'$ se obtiene de X/k por cambio de base (o por una extensión de campos constante o por extensión de los escalares). A la extensión $k'(X)/k(X)$ se le llama una extensión de campos constante.*

2.5. Morfismos entre curvas completas no singulares

Definición 2.5.1. *Sea X/k, Y/k dos curvas completas no singulares sobre k. Un morfismo no constante $\varphi : X \to Y$ de curvas completas no singulares sobre k se define como una función dada por un homomorfismo de k-álgebras $\varphi^* : k(Y) \to k(X)$ como sigue: si $P \in X$ corresponde a la valoración v_P entonces $\varphi(P)$ corresponde en Y a la única valoración suprayectiva inducida por la valoración $v_P \circ \varphi^*$.*

La unicidad se obtiene pues para cualquier valoración $v : K^* \to \mathbb{Z}$ se tiene que $v(K^*) = r\mathbb{Z}$, donde r es el menor valor positivo que toma v (de hecho, $v(\pi) = r$, donde π es el generador del ideal maximal $\mathcal{M}_v$ de $\mathcal{O}_v$). Aplicando esto a la valoración $(v_P \circ \varphi^*) : k(Y)^* \to \mathbb{Z}$ cuya imagen es de la forma $e\mathbb{Z}$ para alguna e, obtenemos una única valoración asociada suprayectiva de $k(Y)$ trivial en k, $v_{\varphi(P)} := \frac{1}{e}(v_P \circ \varphi^*)$.

De la definición anterior se obtiene que $\mathcal{O}_{\varphi(P)} = (\varphi^*)^{-1}(\mathcal{O}_P)$. Además, el mapeo φ está bien definido, pues $\varphi^*(k(Y))$ es un campo de funciones sobre k, con $\varphi^*(k(Y)) \subset k(X)$ ($\varphi^*(k(Y))/k$ es de grado de trascendencia 1 y k algebraicamente cerrado en $\varphi^*(k(Y))$, pues $k(X)/k$ es de grado de trascendencia 1 y k es algebraicamente cerrado en $k(X)$). Además, del lema 2.4.9 se obtiene que el grado de cualquier extensión de campos de funciones sobre k es finita, por lo que $k(X)/\varphi^*(k(Y))$ es una extensión finita y por tanto algebraica. Sea v la valoración de $k(X)$ correspondiente al punto P en X. Entonces, del lema 2.4.10 se obtiene que el que $k(X)/\varphi^*(k(Y))$ sea algebraica implica que $v|_{(\varphi^*(k(Y))^*)}$ no puede ser la valoración trivial.

Supongamos ahora que $\varphi^* : k(Y) \to k(X)$ está dado por una inclusión $k \subseteq k(Y) \subseteq k(X)$. Se obtiene entonces que $\mathcal{O}_{\varphi(P)} = \mathcal{O}_P \cap k(Y)$.

Definición 2.5.2. *Sea $\varphi : X \to Y$ un morfismo no constante de curvas completas no singulares sobre k, y sea $\varphi^* : k(Y) \to k(X)$ el morfismo de k-álgebras que induce a φ. Al grado (finito) $[k(X) : \varphi^*(k(Y))]$ se le llama el grado de φ. Además, decimos que el morfismo φ es separable si $k(X)/\varphi^*(k(Y))$ es separable.*

Decimos que dos curvas completas no singulares sobre k, X/k y Y/k, son isomorfos si sus campos de funciones son isomorfos como k-álgebras. Dado el isomorfismo de k-álgebras entre $k(X)$ y $k(Y)$, el morfismo asociado de curvas completas no singulares sobre k se le llama un isomorfismo de curvas. Un automorfismo σ de una curva X/k es un morfiso de curvas sobre k asociado a un automorfismo de k-álgebras $\sigma^* : k(X) \to k(X)$.

Notamos que un automorfismo tiene grado 1 y es separable. Notamos además que si $\varphi : X \to Y$ es un morfismo sobre k entonces las curvas completas no singulares sobre k definidas por los campos de funciones $k(Y)/k$ y $\varphi^*(k(Y))/k$ son isomorfos.

Sea X/k cualquier curva completa no singular. Como $k(X)/k$ es campo de funciones entonces si $\alpha \in k(X) \setminus k$ se tiene que α no es algebraico sobre k. Entonces $k(\alpha)$ es isomorfo al campo de funciones racionales en una variable sobre k. Por tanto, la inclusión $k(\alpha) \subset k(X)$ induce un morfismo $\varphi_\alpha : X \to \mathbb{P}^1$, con $\mathcal{O}_{\varphi_\alpha(P)} = \mathcal{O}_P \cap k(\alpha)$ (donde $\mathbb{P}^1$ es la curva completa no singular asociada al campo de funciones $k(\alpha)/k$, donde por ser α no algebraico sobre k se obtiene que la extensión es de grado de transcendencia 1, y que k es enteramente cerrado en $k(\alpha)$).

Observación 2.5.3. *Por el teorema 2.3.9 se tiene que el dominio V de α en X es un abierto afín. Sea $\{P_1, \ldots, P_s\}$ el complemento de V en X, es decir, los polos de α. Si $\infty \in \mathbb{P}^1$ es el punto de $\mathbb{P}^1$ correspondiente a $k[1/\alpha]_{(1/\alpha)}$ entonces ∞ es la imagen de los puntos $P_1, \ldots, P_s$ bajo el morfismo φ_α. Para verlo, notamos primero que si $P \in \mathbb{P}^1$ es el punto correspondiente al ideal $(1/\alpha) \subseteq k[1/\alpha]$ entonces $\mathcal{O}_P = k[1/\alpha]_{(1/\alpha)}$ (lema 5.2.14). Luego, por el teorema 2.3.9 sabemos que el complemento del dominio $V \subseteq X$ de α es igual al conjunto (finito) de todos los puntos $P_i \in X$ tales que $\mathcal{O}_{P_i} \supseteq k[1/\alpha]_{(1/\alpha)}$. Notamos entonces que $\mathcal{O}_{P_i} \cap k(\alpha) = k[1/\alpha]_{(1/\alpha)}$ (pues como $k[1/\alpha]$ es dominio de ideales principales entonces es de Dedekind y su localización $k[1/\alpha]_{(1/\alpha)}$ también lo es, y además $k(\alpha)$ es su campo de fracciones, pues $k[1/\alpha] \subseteq k[1/\alpha]_{1/\alpha} \subseteq k(\alpha)$, y como $k[1/\alpha]_{(1/\alpha)} \subseteq \mathcal{O}_{P_i}$, y como $\mathcal{O}_{P_i} \cap k(\alpha) \neq k(\alpha)$ entonces podemos aplicar el lema 5.2.15 al anillo de valoraciones discreto $\mathcal{O}_P = k[1/\alpha]_{(1/\alpha)}$ con campo de fracciones $k(\alpha)$ y a la contención $\mathcal{O}_P = k[1/\alpha]_{(1/\alpha)} \subseteq \mathcal{O}_{P_i} \cap k(\alpha)$, para obtener la igualdad deseada). Se seguirá entonces, por lo mencionado en el párrafo anterior, que $\mathcal{O}_{\varphi_\alpha(P_i)} = \mathcal{O}_{P_i} \cap k(\alpha) = k[1/\alpha]_{(1/\alpha)}$, y por tanto el conjunto de puntos en X cuya imagen es ∞ es igual al complemento de V.*

Por el mismo teorema 2.3.9, también se tiene que la función que viene dada por $V \to \mathrm{Max}(\mathcal{O}_X(V))$ y que manda un punto P al ideal maximal $\mathcal{M}_P \cap \mathcal{O}_X(V)$, es una biyección; y además, $\mathcal{O}_X(V)$ es la cerradura entera de $k[\alpha]$ en $k(X)$. Y por la observación 2.3.8 se tiene que $k[\alpha] = \mathcal{O}_{\mathbb{P}^1}(\mathbb{P}^1 \setminus \{\infty\})$, y se puede verificar que la función $\varphi_\alpha|_V : V \to \mathbb{P}^1 \setminus \{\infty\}$ se puede identificar con la función $\mathrm{Max}(\mathcal{O}_X(V)) \to \mathrm{Max}(k[\alpha])$, $M \mapsto M \cap k[\alpha]$. Para verlo, sabemos que hay una biyección $V \mapsto \mathrm{Max}(\mathcal{O}_X(V))$ mediante $P \mapsto \mathcal{M}_P \cap \mathcal{O}_X(V)$ (con $P \in V$), y usando de nuevo la observación 2.3.8 y el teorema 2.3.9, obtenemos una biyección entre el dominio $V' = \mathbb{P}^1 \setminus \{\infty\}$ de α en $\mathbb{P}^1$ y $\mathrm{Max}(\mathcal{O}_{\mathbb{P}^1}(V'))$ mediante $P' \mapsto \mathcal{M}_{P'} \cap \mathcal{O}_{\mathbb{P}^1}(V')$ (con $P' \in V'$). Por tanto, la función $\varphi_\alpha|_V : V \to V'$, con $P \mapsto P'$, define una función natural $\mathrm{Max}(\mathcal{O}_X(V)) \to \mathrm{Max}(k[\alpha])$, con $\mathcal{M}_P \cap \mathcal{O}_X(V) \mapsto \mathcal{M}_{P'} \cap k[\alpha]$. Y además, de la inclusión $k(\alpha) \subseteq k(X)$ y como la imagen de P es P', se tiene que $\mathcal{O}_{P'} = \mathcal{O}_P \cap k(\alpha)$, y se obtiene que $\mathcal{M}_{P'} = \mathcal{M}_P \cap k(\alpha)$, y de aquí, la función natural mencionada es la misma que la función $\mathrm{Max}(\mathcal{O}_X(V)) \to \mathrm{Max}(k[\alpha])$, con $\mathcal{M}_P \cap \mathcal{O}_X(V) \mapsto \mathcal{M}_P \cap k[\alpha]$. Como todos los ideales maximales de $\mathcal{O}_X(V)$ son de la forma $\mathcal{M}_P \cap \mathcal{O}_X(V)$ $(P \in V)$ y todos los ideales maximales de $k[\alpha]$ son de la forma $\mathcal{M}_{P'} \cap k[\alpha]$ $(P' \in V')$, se obtiene que la función natural mencionada es la misma función que la función $\mathrm{Max}(\mathcal{O}_X(V)) \to \mathrm{Max}(k[\alpha])$, con $M \mapsto M \cap k[\alpha]$.

Observación 2.5.4. *De manera análoga a la observación 2.5.3, tomando V' el dominio de $1/\alpha$ se tiene que su complemento en X es el conjunto de ceros de α en X. Sea 0 el punto de $\mathbb{P}^1$ correspondiente al anillo local $k[\alpha]_{(\alpha)}$. Entonces la función $\varphi_\alpha|_{V'} : V' \to \mathbb{P}^1 \setminus \{0\}$ puede identificarse con la función* $\mathrm{Max}(\mathcal{O}_X(V')) \to \mathrm{Max}(k[1/\alpha])$.

En la demostración del siguiente lema se dará un esbozo de la demostración, la cual puede encontrarse en [9] (lema 5.5, página 247).

Lema 2.5.5. *Sea k cualquier campo. Sea $\varphi : X \to Y$ un morfismo no constante de curvas completas no singulares sobre k. Supongamos que φ está dado por la inclusión de campos $k(Y) \subseteq k(X)$. Entonces existe una cubierta abierta afín $\{U_1, U_2\}$ de Y con las siguientes propiedades:*

- *(1) Si $V_i := \varphi^{-1}(U_i)$, $i = 1, 2$ entonces los conjuntos V_i. $i = 1, 2$ son abiertos afines, y la inclusión $\mathcal{O}_Y(U_i) \subset \mathcal{O}_X(V_i)$ implica que $\mathcal{O}_X(V_i)$ es un $\mathcal{O}_Y(U_i)$-módulo finitamente generado.*
- *(2) La función $\varphi|_{V_i} : V_i \to U_i$ se puede identificar de manera natural con la función* $\mathrm{Max}(\mathcal{O}_X(V_i)) \to \mathrm{Max}(\mathcal{O}_Y(U_i))$, $\mathcal{M} \mapsto \mathcal{M} \cap \mathcal{O}_Y(U_i)$
- *(3) Sea $Q \in Y$. Entonces la cerradura entera C de $\mathcal{O}_Q$ en $k(X)$ es un $\mathcal{O}_Q$-módulo finitamente generado y un Dominio de Dedekind.*

Demostración. Sea $\alpha \in k(Y) \setminus k$. Sean V_1 y U_1 los dominios de α en X y en Y, respectivamente. Sean V_2 y U_2 los dominios de $1/\alpha$ en X y en Y, respectivamente. Entonces $\varphi^{-1}(U_1) = V_1$, pues si $P \in \varphi^{-1}(U_1)$ entonces $\varphi(P) \in U_1$, es decir, $\alpha \in \mathcal{O}_{\varphi(P)} \subseteq k(Y)$, pero $\mathcal{O}_{\varphi(P)} = \mathcal{O}_P \cap k(Y)$ y por tanto, $\alpha \in \mathcal{O}_P \subseteq k(X) \Rightarrow P \in V_1$. Recíprocamente, si $Q \in V_1$ entonces $\alpha \in \mathcal{O}_Q \subseteq k(X)$, y por hipótesis tenemos $\alpha \in k(Y)$, por lo que $\mathcal{O}_{\varphi(Q)} = \mathcal{O}_Q \cap k(Y)$, y se obtiene que $\alpha \in \mathcal{O}_{\varphi(Q)} \subseteq k(Y)$, es decir, $\varphi(Q) \in U_1$, y así $Q \in \varphi^{-1}(U_1)$. Análogamente, se puede ver que $\varphi^{-1}(U_2) = V_2$. Por el lema 2.3.7 se obtiene que $\{U_1, U_2\}$ y $\{V_1, V_2\}$ son cubiertas de Y y X, respectivamente, y del teorema 2.3.9 se obtiene que son abiertos afines de Y y X, respectivamente. Luego, para probar (1), basta ver que $\mathcal{O}_X(V_1)$ es un $\mathcal{O}_Y(U_1)$-módulo finitamente generado (el otro caso es análogo). Del teorema 2.3.9 tenemos que $\mathcal{O}_X(V_1)$ es la cerradura entera B_1' de $k[\alpha]$ en $k(X)$ y que también es una k-álgebra finitamente generada y un dominio de Dedekind (y notamos también que el campo de fracciones de B_1' es $k(X)$, por la proposición 1.2.15), y similarmente, $\mathcal{O}_Y(U_1)$ es la cerradura entera B_1 de $k[\alpha]$ en $k(Y)$ y un dominio de Dedekind (y también notamos que el campo de fracciones de B_1 es $k(Y)$, por la proposición 1.2.15). Sea B_1'' la cerradura entera de B_1 en $k(X)$. Queremos probar que $B_1' = B_1''$, ya que si se cumple eso entonces de la proposición 5.2.1 se obtendrá que B_1' es un B_1-módulo finitamente generado (notamos que la hipótesis de que $k(X)/k(Y)$ sea extensión finita se cumple por el tercer párrafo de esta sección 2.5 en el capítulo II). Tenemos que $B_1 \subseteq B_1''$, y como B_1'' es entero sobre B_1, y B_1 es entero sobre $k[\alpha]$ entonces B_1'' es entero sobre $k[\alpha]$ (proposición 1.2.14), y entonces $B_1'' \subseteq B_1'$. Y también, como

$B_1 \subseteq B_1'$, y como B_1' es entero sobre $k[\alpha]$ entonces B_1 es entero sobre $k[\alpha]$ y B_1' es entero sobre B_1 (proposición 1.2.14), y en particular B_1' es entero sobre B_1, y por tanto, $B_1' \subseteq B_1''$. Se obtiene entonces la igualdad buscada, y se obtiene la parte (1).

Para probar (3), podemos asumir, sin pérdida de generalidad, que $Q \in U_1$, es decir, que $\alpha \in \mathcal{O}_Q \setminus k$. Tenemos que C es enteramente cerrado, y como $C/\mathcal{O}_Q$ es extensión entera, se obtiene que C tiene dimensión 1 ($\mathcal{O}_Q$ es un dominio de ideales principales, y por tanto un dominio de Dedekind. Entonces es de dimensioón 1, y aplicamos la proposición 1.5.6). Como $\alpha \in \mathcal{O}_Q$, se obtiene que $\mathcal{O}_Q$ es la localización de $\mathcal{O}_Y(U_1)$ en un ideal maximal M_Q (como $\alpha \in \mathcal{O}_Q$ entonces $Q \in U_1$ y se obtiene $\mathcal{O}_Y(U_1) \subseteq \mathcal{O}_Q$, por lo que $v_Q(\mathcal{O}_Y(U_1)) \geq 0$. Además, como U_1 es afín entonces $\mathcal{O}_Y(U_1)$ es la cerradura entera de $k[\alpha]$ en $k(Y)$, y por la proposición 5.1.4 $\mathcal{O}_Y(U_1)$ es un $k[\alpha]$-módulo finitamente generado. Usando entonces el teorema 5.2.11 se llega a que $\mathcal{O}_Y(U_1)$ es un dominio de Dedekind, que además tiene a $k(X)$ como campo de fracciones debido a la proposición 1.2.15. Aplicando el lema 5.2.13 se obtiene el resultado). Por construcción, $\mathcal{O}_X(V_1)$ es la cerradura entera de $\mathcal{O}_Y(U_1)$ en $k(X)$ (por el teorema 2.3.9 tenemos que $\mathcal{O}_Y(U_1)$ es la cerradura entera B' de $k[\alpha]$ en $k(Y)$, y $\mathcal{O}_X(V_1)$ es la cerradura entera B de $k[\alpha]$ en $k(X)$. Sea B'' la cerradura entera de B' en $k(X)$. Si $b \in B''$ entonces es entero sobre B', y por la proposición 1.2.14 se tiene que b es entero sobre $k[\alpha]$, y por tanto, $b \in B$. Recíprocamente, si $b \in B$ entonces en particular $b \in k(X)$ y es un elemento entero sobre $k[\alpha]$. Aplicando de nuevo la proposición 1.2.14 se tiene que b es entero sobre B'. Por tanto, $b \in B''$, y se obtiene la igualdad $B'' = B$). Como $\mathcal{O}_Y(U_1) \setminus M_Q$ es un subconjunto multiplicativo de $\mathcal{O}_X(V_1)$, se obtiene que la cerradura entera C de $\mathcal{O}_Q$ en $k(X)$ es la localización de $\mathcal{O}_X(V_1)$ en un subjunto multiplicativo. Como $\mathcal{O}_X(V_1)$ es un $\mathcal{O}_Y(U_1)$-módulo finitamente generado entonces C es un $\mathcal{O}_Q$-módulo finitamente generado. Se obtiene que C es Noetheriano, ya que $\mathcal{O}_Q$ lo es ($\mathcal{O}_Q$ es dominio de Dedekind, por lo que en particular es noetheriano, y luego aplicamos el corolario 1.4.5). Así, se obtiene el resultado. □

Sea k un cualquier campo. Sea $\varphi : X \to Y$ un morfismo no constante de curvas completas no singulares sobre k dado por una inclusión de campos de funciones $k(Y) \subseteq k(X)$. Sea $P \in X$. Sea C la cerradura entera de $\mathcal{O}_{\varphi(P)}$ en $k(X)$. Entonces $\mathcal{O}_P$ es la localización de C en un ideal maximal (del lema 2.5.5 tenemos que C es un dominio de Dedekind y un $\mathcal{O}_Q$-módulo finitamente generado, con campo de fracciones $k(X)$ y tal que $v_P(C) \geq 0$, esto último ya que la igualdad $\mathcal{O}_Q = \mathcal{O}_P \cap k(Y)$ implica que $\mathcal{O}_Q \subseteq \mathcal{O}_P$ y como $\mathcal{O}_P$ es enteramente cerrado en su campo de fracciones $k(X)$, se obtiene que $C \subseteq \mathcal{O}_P$, y por tanto $v_P(C) \geq 0$. Como las hipótesis del lema 5.2.13 se satisfacen entonces se obtiene el resultado). La inclusión natural $\mathcal{O}_{\varphi(P)} \to \mathcal{O}_P$ induce una función (inyectiva) entre los campos residuales $\mathcal{O}_{\varphi(P)}/\mathcal{M}_{\varphi(P)} \to \mathcal{O}_P/\mathcal{M}_P$. Como C es una $\mathcal{O}_{\varphi(P)}$-álgebra finitamente generada, se tiene que $[\mathcal{O}_P/\mathcal{M}_P : \mathcal{O}_{\varphi(P)}/\mathcal{M}_{\varphi(P)}]$ es finito, y denotamos a este valor como $f_{P/\varphi(P)}$, y lo llamamos el grado residual de P sobre $\varphi(P)$. Además, al entero e_P (denotado también por $e_{P/\varphi(P)}$) tal que $\mathcal{M}_{\varphi(P)}\mathcal{O}_P = \mathcal{M}_P^{e_P}$ se le

llama el índice de ramificación de φ sobre P (o de P sobre $\varphi(P)$). Observamos que existe dicha e_P, ya que $\mathcal{O}_P$ es un dominio de ideales principales local, por lo que es un dominio de Dedekind local. Entonces, el ideal $M_{\varphi(P)}\mathcal{O}_P$ generado por $\mathcal{M}_{\varphi(P)}$ en $\mathcal{O}_P$ se factoriza como un producto único de ideales maximales de $\mathcal{O}_P$, el cual solamente tiene un ideal maximal, $\mathcal{M}_P$, y así $\mathcal{M}_{\varphi(P)}\mathcal{O}_P = \mathcal{M}_P^{e_P}$ para alguna $e_P \in \mathbb{N}$. Tenemos entonces la siguiente definición:

Definición 2.5.6. *Un punto P de X es no ramificado sobre Y si $e_P = 1$ y si el campo residual $\mathcal{O}_P/\mathcal{M}_P$ es separable sobre $\mathcal{O}_{\varphi(P)}/\mathcal{M}_{\varphi(P)}$. El punto P es ramificado si $e_P > 1$ o si el campo residual $\mathcal{O}_P/\mathcal{M}_P$ no es separable sobre $\mathcal{O}_{\varphi(P)}/\mathcal{M}_{\varphi(P)}$. La imagen en Y del conjunto de puntos de ramificación de X se le llama el branch locus de φ.*

Sea $Q \in Y$. La fibra $\varphi^{-1}(Q)$ se puede describir como sigue: Sea C la cerradura entera de $\mathcal{O}_Q$ en $k(X)$. Como $C/\mathcal{O}_Q$ es extensión entera entonces cada ideal maximal de C contiene a $\mathcal{M}_Q$ (observación 1.5.7). Como C es dominio de Dedekind, C tiene únicamente un número finito de ideales maximales (pues al intersectar cualquier ideal maximal de C con $\mathcal{O}_Q$ se obtiene el único ideal maximal $\mathcal{M}_Q$ de $\mathcal{O}_Q$, y entonces del corolario 1.17.4 se obtiene el resultado). Cada uno de estos ideales maximales corresponde a una valoración de $k(X)$ (recordamos que $k(X)/k(Y)$ resulta ser una extensión finita, por lo que tenemos las hipótesis para poder aplicar la proposición 1.2.15 y obtener que $k(X)$ es el campo de fracciones de C. Luego, cada ideal maximal M de C induce una valoración de $k(X)$, a saber, la valoración M-ádica). Sea $\mathcal{O}_{P_i}$, $i = 1, \ldots, s$, los dominios de ideales principales locales asociados a estas valoraciones. Sean $P_1, \ldots, P_s$ los puntos correspondientes en X. Entonces $\varphi^{-1}(Q) = \{P_1, \ldots, P_s\}$. Como C es una $\mathcal{O}_{\varphi(P)}$-álgebra finitamente generada, aplicamos el teorema 1.18.4 para obtener que $\sum_{P \in \varphi^{-1}(Q)} e_{P/Q} f_{P/Q} = \deg(\varphi)$. En particular, la fibra $\varphi^{-1}(Q)$ contiene a lo más $\deg(\varphi)$. Cuando k es algebraicamente cerrado, todos los campos residuales son iguales a k, por lo que $f_{P/Q} = 1$, $\forall\ P \in \varphi^{-1}(Q)$.

Proposición 2.5.7. *Sea k cualquier campo. Sea $\varphi : X \to Y$ un morfismo no constante de curvas completas no singulares sobre k de grado n. Entonces φ es suprayectiva, con fibras finitas de cardinalidad a lo más n. Si φ es un morfismo separable entonces el branch locus es un conjunto finito. En particular, cuando k es algebraicamente cerrado y φ es separable entonces existe un abierto denso $U \subset Y$ tal que, $\forall\ P \in U$, $|\varphi^{-1}(P)| = n$.*

Daremos un esbozo de la demostración de esta proposición. La demostración se puede encontrar en [9] (proposición 5.7, página 249)

Demostración. Para ver que el branch locus es un conjunto finito, sea $\{U_1, U_2\}$ una cubierta abierta de Y como en el lema 2.5.5. Como U_1 es abierto, su complemento en Y es finito. Por tanto, es suficiente probar que el branch locus

restringido a V_1 es un conjunto finito. Por construcción, un punto $Q \in U_1$ es la imagen de un punto de ramificación $P \in V_1$ si y sólo si el ideal maximal $M_Q \cap \mathcal{O}_Y(U_1)$ contiene al ideal discriminante de la extensión $\mathcal{O}_X(V_1)/\mathcal{O}_Y(U_1)$. Como la función φ es separable, este ideal discriminante es distinto del ideal cero. Por tanto, puede haber únicamente un número finito de puntos en U_1 que son la imagen de puntos de ramificación.

Sea U el complemento en Y del branch locus. Por lo anterior, obtenemos que U es abierto siempre que φ sea separable. Si, además, k es algebraicamente cerrado entonces cada una de las fibras de φ de los puntos en U tienen exactamente n puntos distintos. Se obtiene así el resultado. □

2.6. Campos de funciones 2

Supondremos para esta sección que los campos base k son siempre perfectos a menos que se especifique otra cosa.

Consideramos primero la notación siguiente:

Sean $k \subseteq E$ cualquier extensión de campos. Consideramos $\bar{X}/E$ una curva completa no singular. Decimos que $\bar{X}/E$ está definida sobre k si el campo de funciones $E(\bar{X})/E$ contiene a un campo de funciones L/k tal que el menor subcampo de $\overline{E(\bar{X})}$ que contiene a E y L es igual a $E(\bar{X})$, i.e., $EL = E(\bar{X})$. Denotamos por $k(X)$ a L, y X/k a la curva completa no singular asociada a $k(X)/k$.

Consideramos X/k y Y/k curvas completas no singulares. Sea $\pi : X \to Y$ un morfismo de curvas sobre k, inducido por la inclusión $k(Y) \subseteq k(X)$. Fijamos una cerradura algebraica $\overline{k(X)}$ de $k(X)$. Tomamos $\overline{k}$ la cerradura algebraica de k en $\overline{k(X)}$, y sea k'/k cualquier extensión en $\overline{k}$. Decimos que π puede ser extendido al morfismo $\pi_{k'} : X_{k'} \to Y_{k'}$, el cual viene inducido por la inclusión $k'(Y) \to k'(X)$.

Si $k' = \overline{k}$, denotamos a $\pi_{k'}$ por $\overline{\pi}$. Cuando π viene dado por un homomorfismo de campos (inyectivo) $\pi^* : k(Y) \to k(X)$, podemos definir para cualquier extensión de campos $i : k \to k'$ el morfismo extendido $\pi_{k'} : X_{k'} \to Y_{k'}$ como el morfismo asociado a la función $\pi^* \otimes i : k(Y) \otimes_k k' \to k(X) \otimes_k k'$.

Consideramos nuevamente X/k y Y/k dos curvas completas no singulares cualesquiera. Sea $\mu : X_{\overline{k}} \to Y_{\overline{k}}$ cualquier morfismo de curvas sobre $\overline{k}$. Decimos que el morfismo μ está definido sobre una extensión E/k (contenida en $\overline{k}$) si existe un morfismo de curvas $\pi : X_E \to Y_E$ sobre E tal que $\mu = \pi_{\overline{k}}$.

Lema 2.6.1. *Sean X/k y Y/k curvas completas no singulares, y sea $\mu : X_{\overline{k}} \to Y_{\overline{k}}$ cualquier morfismo sobre $\overline{k}$. Entonces μ puede ser definido sobre cualquier extensión finita de k.*

Demostración. Sea $y_1 \in k(Y)$ tal que $k(Y)/k(y_1)$ es extensión finita, y sean $y_2, \ldots, y_s \in k(Y)$ tales que $k(Y) = k(y_1, \ldots, y_s)$. Se obtiene entonces que $\mu^*(y_j) = \sum_{i=1}^{r_j} a_{ij}\alpha_{ij}$, para algunos $a_{ij} \in \overline{k}$ y $\alpha_{ij} \in k(X)$. Definimos $E := k(a_{ij}, 1 \leq i \leq r_j, 1 \leq j \leq s)$, y entonces obtenemos que la imagen de $E(Y)$ bajo $\mu^*|_{E(Y)}$ está contenido en $E(X)$. De aquí, se obtiene que $\mu^*|_{E(Y)}$ define un morfismo $\mu_E : X_E \to Y_E$ de curvas sobre E, tal que μ es un morfismo sobre $\overline{k}$ obtenido de μ_E por extensión de los escalares de E a $\overline{k}$. Para verlo, basta observar que $\overline{k}(Y) = \overline{k} \cdot E(Y)$ y que $\overline{k}(X) = \overline{k} \cdot E(X)$, pues esto implica que $\mu = \mu_{\overline{k}}$, donde $\mu_{\overline{k}}$ viene inducido por la inclusión $\overline{k} \cdot E(Y) \hookrightarrow \overline{k} \cdot E(X)$. Para ver que $\overline{k}(Y) = \overline{k} \cdot E(Y)$, notamos que $k(Y) = k(y_1, \ldots, y_s) \Rightarrow \overline{k}(Y) = \overline{k} \cdot k(Y) = \overline{k}(y_1, y_2, \ldots, y_s)$. Por la misma razón, se tiene que $E(Y) = E \cdot k(Y) = E(y_1, \ldots, y_s)$, y de esto último, se obtiene que $\overline{k} \cdot E(Y) = \overline{k}(y_1, \ldots, y_s)$. Por tanto, $\overline{k}(Y) = \overline{k} \cdot E(Y)$

Análogamente se verifica que $\overline{k}(X) = \overline{k} \cdot E(X)$. Así, se obtiene el resultado deseado. □

Sea X/k una curva completa no singular. Fijamos una cerradura algebraica $\overline{k(X)}$ de $k(X)$. Sea $\overline{k}$ la cerradura algebraica de k en $\overline{k(X)}$. Consideramos la restricción natural $r : \sigma \to \sigma|_{\overline{k}}$ de $\mathrm{Gal}(\overline{k}(X)/k(X))$ a $\mathrm{Gal}(\overline{k}/k)$. Entonces, por ser $\overline{k}(X) = \overline{k} \cdot k(X)$, se tiene que r es inyectivo (pues si tenemos $\sigma, \sigma' \in \mathrm{Gal}(\overline{k}(X)/k(X))$ con $\sigma|_{\overline{k}} = \sigma'|_{\overline{k}}$ entonces por definición σ y σ' fijan a $k(X)$, y además, σ y σ' toman los mismos valores sobre $\overline{k}$ por hipótesis, por lo que toman los mismos valores en $\overline{k} \cdot k(X) = \overline{k}(X)$, y entonces $\sigma = \sigma'$).

Lema 2.6.2. *Sea k un campo perfecto. Sea k'/k una extensión de Galois en $\overline{k}$ de grado d. Entonces $k'(X)/k(X)$ es una extensión de Galois. La función restricción $r_{k'} : \sigma \mapsto \sigma|_{k'}$, de $\mathrm{Gal}(k'(X)/k(X))$ a $\mathrm{Gal}(k'/k)$ es un isomorfismo. Además, toda extensión finita $L/k(X)$ con $L \subseteq \overline{k}(X)$ está contenida en una extensión de la forma $k'(X)$, para alguna extensión finita de Galois k'/k.*

Demostración. Como $k'(X) = k' \cdot k(X)$, obtenemos que $r_{k'}$ es inyectivo de manera análoga a lo que se hizo en el párrafo anterior (antes de enunciar el lema 2.6.2). Del lema 2.4.13 se obtiene que $[k'(X) : k(X)] = [k' : k]$. Por tanto, para probar que $k'(X)/k(X)$ es Galois, basta probar que $|\mathrm{Gal}(k'(X)/k(X))| = [k'(X) : k(X)]$, o equivalentemente, que $r_{k'}$ es suprayectiva (para la equivalencia: si $r_{k'}$ fuera suprayectiva entonces sería biyectiva, implicando que $|\mathrm{Gal}(k'(X)/k(X))| = |\mathrm{Gal}(k'/k)| = [k' : k] = [k'(X) : k(X)]$, y por tanto $k'(X)/k(X)$ es Galois. Recíprocamente, si $k'(X)/k(X)$ es Galois entonces se obtiene la igualdad $|\mathrm{Gal}(k'(X)/k(X))| = |\mathrm{Gal}(k'/k)|$, y esto junto con la inyectividad de r_k, implican que $r_{k'}$ es suprayectiva). Para ver que $r_{k'}$ es suprayectiva, tomamos una base $\{c_1, \ldots, c_d\}$ de k'/k. Sea $\alpha \in k'(X)$. Entonces $\alpha = \sum_{i=1}^{e} \alpha_i \beta_i$, con $\alpha_i \in k'$, $\beta_i \in k(X)$. Como $\alpha_i = \sum_{j=1}^{d} \alpha_{ij} c_j$ para algunos $\alpha_{ij} \in k$, y ocurre para cada i entonces existen elementos $\gamma_1, \ldots, \gamma_d \in k(X)$ tales que $\alpha = \sum_{i=1}^{d} c_i \gamma_i$ ($\gamma_j = \sum_{i=1}^{e} \beta_i \alpha_{ij}$, para cada $j = 1, \ldots, d$). Sea $\sigma' \in \mathrm{Gal}(k'/k)$. Definimos $\sigma(\alpha) := \sum_{i=1}^{d} \sigma'(c_i)\lambda_i$. Entonces σ pertenece a $\mathrm{Gal}(k'(X)/k(X))$, y $r_{k'}(\sigma) = \sigma'$. Para verlo, se puede verificar haciendo cuentas que σ es efectivamente un homomorfismo de campos, por lo que es inyectiva. Para ver que es suprayectiva, notamos que si $C = \{c_1, \ldots, c_d\}$ es una base de la extensión k'/k y $\sigma' \in \mathrm{Gal}(k'/k)$ entonces $\{\sigma'(c_1), \ldots, \sigma'(c_d)\}$ también es una base de dicha extensión. Como α se logró escribir en términos de una base arbitraria C con coeficientes en $k(X)$, en particular se puede usar la base $C' = \{\sigma'(c_1), \ldots, \sigma'(c_d)\}$, y se obtiene entonces que σ es suprayectiva. Para ver que fija a $k(X)$, sea $\alpha \in k(X)$. Entonces $\alpha = 1 \cdot \alpha$, con $1 \in k'$ y $\alpha \in k(X)$. Escribimos $1 = \sum_{i=1}^{d} \alpha_i c_i$, con $\alpha_i \in k$ (notamos entonces que $1 = \sigma'(1) = \sum_{i=1}^{d} \alpha_i \sigma'(c_i)$). Se obtiene de la definición de σ que $\sigma(\alpha) = \sum_{i=1}^{d} \sigma(c_i)(\alpha\alpha_i) \Rightarrow \sigma(\alpha) = \alpha \sum_{i=1}^{d} \alpha_i \sigma'(c_i) = \alpha$. Finalmente, para ver que $r_{k'}(\sigma) = \sigma'$, sea $m \in k'$. Escribimos $m = m \cdot 1$, con $m \in k'$, y $1 \in k(X)$, y

$m = \sum_{i=1}^{d} \alpha_i c_i$. De la definición de σ, se obtiene que $\sigma(m) = \sum_{i=1}^{d} \sigma'(c_i)(\alpha_i \cdot 1)$, pero el lado derecho de esta igualdad es precisamente $\sigma'(m)$, y se obtiene el resultado.

Ahora, sea $L/k(X)$ cualquier extensión finita contenida en $\overline{k}(X)$. Tomamos una base $\{\gamma_1, \ldots, \gamma_n\}$ para la extensión $L/k(X)$. Entonces podemos escribir $\gamma_i = \sum_{i=1}^{s_i} c_{ij}\beta_{ij}$, con $c_{ij} \in \overline{k}$ y $\beta_{ij} \in k(X)$. Sea $E := k(c_{ij}, 1 \leq i \leq n, 1 \leq j \leq s_i)$. Sea k' una extensión de Galois de k que contenga a E. se obtiene entonces que $L \subseteq k'(X)$. Así, se obtiene lo que buscábamos. □

Sea I el conjunto de extensiones finitas de Galois de k contenidas en $\overline{k}$. Se obtiene de la proposición 1.27.5 que el grupo $\mathrm{Gal}(\overline{k}/k)$ es isomorfo al límite proyectivo del sistema proyectivo de los grupos de Galois finitos $\{\mathrm{Gal}(k'/k)\}_{k' \in I}$. Sea $\psi : \mathrm{Gal}(\overline{k}/k) \to \varprojlim(\mathrm{Gal}(k'/k))$ dicho isomorfismo. Del lema 2.6.2, se obtiene que el conjunto $\mathcal{I} := \{k'(X)/k(X) | k' \in I\}$ es cofinal en el conjunto J de todas las extensiones finitas de Galois de $k(X)$ contenidas en $\overline{k}(X)$. Por tanto, de la observación 1.28.6 se obtiene que el grupo de Galois $\mathrm{Gal}(\overline{k}(X)/k(X))$ es isomorfo al límite proyectivo del sistema proyectivo $\{\mathrm{Gal}(k'(X)/k(X))\}_{k'(X) \in \mathcal{I}}$, y sea $\Psi : \mathrm{Gal}(\overline{k}(X)/k(X)) \to \varprojlim(\mathrm{Gal}(k'(X)/k(X)))$.

Notamos que, como conjuntos dirigidos, el conjunto $\mathcal{I}$ está en biyección con el conjunto I. Si denotamos por $r_{k'}$ a la restricción natural $\mathrm{Gal}(k'(X)/k(X)) \to \mathrm{Gal}(k'/k)$ entonces tenemos que $\{r_{k'}\}_{k' \in I}$ es un morfismo entre los sistemas proyectivos $\{\mathrm{Gal}(k'(X)/k(X))\}_{k'(X) \in \mathcal{I}}$ y $\{\mathrm{Gal}(k'/k)\}_{k' \in I}$. Pero como cada $r_{k'}$ es un isomorfismo (del lema 2.6.2) entonces de la proposición 1.28.5, se obtiene que este morfismo de sistemas proyectivos induce un isomorfismo de grupos $\overline{r} : \varprojlim(\mathrm{Gal}(k'(X)/k(X))) \to \varprojlim(\mathrm{Gal}(k'/k))$. Se obtiene entonces de las definiciones que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{k}(X)/k(X)) & \xrightarrow{r} & \mathrm{Gal}(\overline{k}/k) \\ \downarrow \Psi & & \downarrow \psi \\ \varprojlim(\mathrm{Gal}(k'(X)/k(X))) & \xrightarrow{\overline{r}} & \varprojlim(\mathrm{Gal}(k'/k)) \end{array}$$

Así, cuando la extensión $\overline{k}(X)/k(X)$ no es necesariamente finita, usando el lema 2.6.2 y la discusión anterior se obtiene la siguiente proposición:

Proposición 2.6.3. *Sea k un campo perfecto. Entonces r es un isomorfismo de grupos.*

Sea X/k una curva completa no singular. Sea $X_{\overline{k}}/\overline{k}$ el cambio de base de X. Consideramos la siguiente acción de $\mathrm{Gal}(\overline{k}/k)$ sobre $X_{\overline{k}}$: $\forall\ \sigma \in \mathrm{Gal}(\overline{k}/k)$, $\forall\ P \in X_{\overline{k}}$, sea $\sigma \cdot P$ el punto en $X_{\overline{k}}$ correspondiente al dominio de ideales principales local $\mathcal{O}_{\sigma(P)} := \sigma(\mathcal{O}_P)$, donde $\sigma \in \mathrm{Gal}(\overline{k}/k)$ se está identificando con su correspondiente $\sigma \in \mathrm{Gal}(\overline{k}(X)/k(X))$ (proposición 2.6.3).

Notamos que $\mathrm{Gal}(\overline{k}/k)$ actúa sobre $X_{\overline{k}}$ por medio de permutaciones y no por medio de un morfismo de curvas ya que $\sigma : \overline{k}(X) \to \overline{k}(X)$ no es un homomorfismo de k-álgebras.

Ahora, consideramos $I : X_{\overline{k}} \to X$, con $\overline{P} \mapsto P$ tal que $\mathcal{O}_P := \mathcal{O}_{\overline{P}} \cap k(X)$.

En la siguiente proposición se dará un esbozo de la demostración, la cual se puede encontrar en [9](proposición 6.9, página 255).

Proposición 2.6.4. *Sea k un campo perfecto. Sea X/k una curva completa no singular . Entonces I es suprayectivo, y el conjunto X está en biyección con el conjunto de órbitas de $X_{\overline{k}}$ bajo la acción de* $\mathrm{Gal}(\overline{k}/k)$.

Demostración. Para probar que I está bien definido, observamos que si una valoración de $\overline{k}(X)$ es trivial sobre $k(X)^*$ entonces es trivial sobre k^*, y de aquí se obtiene que es trivial sobre $\overline{k}^*$ (lema 2.4.10). Y como $\overline{k}(X) = \overline{k} \cdot k(X)$, se obtiene entonces que también es trivial sobre $\overline{k}(X)^*$. Por tanto, una valoración de $\overline{k}(X)$ no trivial sobre $\overline{k}(X)^*$ es no trivial sobre $k(X)^*$, por lo que si $\overline{\mathcal{O}}$ es un dominio de ideales principales local (es decir, corresponde a una valoración no trivial) entonces también $\overline{\mathcal{O}} \cap k(X)$ lo es.

Sea $P \in X$ y $v : k(X) \to \mathbb{Z}$ la correspondiente valoración suprayectiva. Consideramos el conjunto Σ de parejas (L, w) tales que $k(X) \subseteq L \subseteq \overline{k}(X)$ y $w : L^* \to \mathbb{Z}$ tal que $w|_{k(X)} = v$. Definimos el siguiente orden parcial para el conjunto Σ como sigue:

$$(L, w) \leq (L', w') \text{ si y sólo si } L \subseteq L' \text{ y } w'|_{L^*} = w.$$

Notamos que $\leq$ es efectivamente un orden parcial y que las condiciones del Lema de Zorn se satisfacen. Por tanto, Σ tiene al menos un elemento maximal, y sea (M, ω) dicho elemento. Queremos probar que $M = \overline{k}(X)$. Supongamos que $M \neq \overline{k}(X)$ entonces existe un elemento algebraico $\alpha \in \overline{k} \setminus M$ (de lo contrario, se tendría $\overline{k} \subseteq M$, y como tenemos $k(X) \subseteq M$, se tendría $\overline{k}(X) \subseteq M$, por lo que $\overline{k}(X) = M$). Sea $\mathcal{O}_w$ el dominio de ideales principales local asociado a w. Consideramos la extensión $M(\alpha)/M$ contenida en $\overline{k}(X)$. Sea B la cerradura entera de $\mathcal{O}_w$ en $M(\alpha)$. Sea $\mathcal{M} \in \mathrm{Max}(B)$. Por la proposición 1.20.1 se obtiene que la extensión $B/\mathcal{O}_w$ es no ramificada. Por tanto, $v_{\mathcal{M}}$ extiende a ω. Para verlo, primero observamos que w es suprayectiva, pues al restringirse a $k(X)$ resulta ser igual a v, que ya es suprayectiva. Usando la observación 5.2.18 se obtiene que M es el campo de fracciones de $\mathcal{O}_w$. Por el teorema 2.2.10 notamos que w es la valoración $\mathcal{M}_w$-ádica, $v_{\mathcal{M}_v} : M^* \to \mathbb{Z}$. Notamos entonces que las condiciones del 5.2.16, se satisfacen para el dominio de Dedekind $\mathcal{O}_w$ con campo de fracciones M, $M(\alpha)/M$ extensión finita separable (pues k es perfecto), B la cerradura entera de $\mathcal{O}_w$ en $M(\alpha)$ y la valoración $v_{\mathcal{M}}$ (como $\mathcal{O}_w$ es local con ideal maximal único $\mathcal{M}_w$ entonces $\mathcal{M} \cap \mathcal{O}_w = \mathcal{M}_w$, y por tanto $\mathcal{M}$ aparece en la factorización de $\mathcal{M}_w B$). Como $B/\mathcal{O}_w$ es no ramificada entonces se tiene que $e_{\mathcal{M}/\mathcal{M}_w} = 1$ y $B/\mathcal{M}$ es separable sobre $\mathcal{O}_w/\mathcal{M}_w$. En particular, $e_{\mathcal{M}/\mathcal{M}_w} = 1$, y utilizando el 5.2.16, se obtiene que $v_{\mathcal{M}}$ extiende a ω. Esto contradice el hecho de que (M, ω) es maximal. Por tanto, $(M, \omega) = (\overline{k}(X), \omega)$ y cumple que $\omega|_{k(X)^*} = v$, y de esto

último y de las definiciones de $\mathcal{O}_w$ y $\mathcal{O}_v$ se obtiene que $\mathcal{O}_v = \mathcal{O}_w \cap k(X)$, por lo que P es la imagen bajo I del punto en $X_{\overline{k}}$ correspondiente a $\mathcal{O}_w$, y así, I es suprayectiva.

Ahora, sea $P \in X$. Queremos probar que la imagen inversa de P bajo I es una órbita bajo la acción de $\mathrm{Gal}(\overline{k}/k)$. Sean $\overline{\mathcal{O}}_1$ y $\overline{\mathcal{O}}_2$ dos dominios de ideales principales locales de $\overline{k}(X)/\overline{k}$ cuya imagen bajo I es P, i.e., $\overline{\mathcal{O}}_1 \cap k(X) = \mathcal{O}_P = \overline{\mathcal{O}}_2 \cap k(X)$. Consideramos el conjunto Θ de tripletas (L_1, L_2, σ) tales que $k(X) \subseteq L_1, L_2 \subseteq \overline{k}(X)$, $\sigma : L_1 \to L_2$ es un isomorfismo de campos, y $\sigma(\overline{\mathcal{O}}_1 \cap L_1) = \overline{\mathcal{O}}_2 \cap L_2$. Damos un orden parcial al conjunto Θ como sigue:

$(L_1, L_2, \sigma) \leq (L_1', L_2', \sigma')$ si y sólo si $L_1 \subseteq L_1', L_2 \subseteq L_2'$, y $\sigma'|_{L_1} = \sigma$.

Notamos entonces que $\leq$ es efectivamente un orden parcial, y además que se cumplen las condiciones del lema de Zorn. Por tanto, Θ tiene al menos un elemento maximal, y sea (M_1, M_2, σ) dicho elemento. Queremos ver que $M_1 = \overline{k}(X)$. Para verlo, suponemos $M_1 \neq \overline{k}(X)$, por lo que existe un elemento algebraico $\alpha \in \overline{k} \setminus M_1$. Sea N_1 la menor extensión de Galois de $M_1(\alpha)$ contenida en $\overline{k}(X)$ que es Galois sobre M_1. Elegimos cualquier extensión σ' de σ a N_1, y sea $N_2 := \sigma'(N_1)$. Sea $\mathcal{O}_2 := \overline{\mathcal{O}}_2 \cap M_2$. Sea B_2 la cerradura entera de O_2 en N_2. Los anillos $\sigma'(\overline{\mathcal{O}}_1 \cap N_1)$ y $\overline{\mathcal{O}}_2 \cap N_2$ son las localizaciones de B_2 en posiblemente dos ideales maximales $\mathcal{M}_1$ y $\mathcal{M}_2$, respectivamente (como la extensión N_1/M_1 es de Galois entonces N_2/M_2 es separable. Aplicando el teorema 5.2.11 y la observación 5.2.12 al dominio de Dedekind $\mathcal{O}_2$ con campo de fracciones M_2 y con extensión finita separable N_2/M_2, se obtiene que B_2 es de Dedekind (con campo de fracciones N_2). Luego, como las valoraciones inducidas por $\sigma'(\overline{\mathcal{O}}_1) \cap N_1$ y $\overline{\mathcal{O}}_2 \cap N_2$ son mayores o iguales a cero en $\mathcal{O}_2$ entonces aplicamos el lema 5.2.13 para obtener lo buscado). Por la proposición 1.21.1 existe una elemento $\tau \in \mathrm{Gal}(N_2/M_2)$ tal que $\tau(M_1) = M_2$. De aquí, se obtiene que $(N_1, N_2, \tau \circ \sigma') \geq (M_1, M_2, \sigma)$. Por tanto, esta contradicción prueba que $M_1 = \overline{k}(X)$. Y como $\sigma(\overline{k}) = \overline{k}$, se obtiene que $M_2 = \overline{k}(X)$. Por tanto, $\sigma \in \mathrm{Gal}(\overline{k}(X)/k(X))$, con $\sigma(\overline{\mathcal{O}}_1) = \overline{\mathcal{O}}_2$. □

Sea X/k una curva completa no singular. Sea $X_{\overline{k}}/\overline{k}$ la curva completa no singular obtenida por extensión de los escalares de $\overline{k}$. El grupo de Galois $\mathrm{Gal}(\overline{k}/k)$ actúa sobre $X_{\overline{k}}$ como se describió antes. Sea $P \in X_{\overline{k}}$. El campo de definición de P sobre k, denotado por $k(P)$, se define como el subcampo de $\overline{k}$ fijado por el subgrupo $\mathrm{Stab}(P) := \{\sigma \in \mathrm{Gal}(\overline{k}/k) \mid \sigma(P) = P\}$. En otras palabras, tenemos

Definición 2.6.5. *El campo de definición de P sobre k, denotado por $k(P)$, es el subcampo de $\overline{k}$ dado por $k(P) := \overline{k}^{\mathrm{Stab}(P)} = \{c \in \overline{k} | \sigma(c) = c, \forall\, \sigma \in \mathrm{Stab(P)}\}$.*

Lema 2.6.6. *Sea k un campo perfecto. Sea X/k una curva completa no singular. Sea $P \in X_{\overline{k}}$. Entonces la extensión $k(P)/k$ es finita, y la órbita de P bajo la acción de $\mathrm{Gal}(\overline{k}/k)$ contiene $[k(P) : k]$ elementos.*

Demostración. Sea $\overline{\mathcal{O}}$ el dominio de ideales principales local correspondiente a P. Sea $\mathcal{O} := \overline{\mathcal{O}} \cap k(X)$. Sea π el generador del ideal maximal del anillo $\mathcal{O}$.

Entonces, $\forall\ \sigma \in \mathrm{Gal}(\overline{k}/k)$, $\sigma(\pi) = \pi$ pertenece a $\sigma(\overline{\mathcal{O}})$ (donde se identifica al elemento $\sigma \in \mathrm{Gal}(\overline{k}/k)$ con su correspondiente $\sigma \in \mathrm{Gal}(\overline{k}(X)/k(X))$, por lo que σ fija, en particular, al elemento $\pi \in \mathcal{O} = \overline{\mathcal{O}} \cap k(X) \subseteq \overline{\mathcal{O}}$). Por tanto, se obtiene que el valor $(v_P \circ \sigma)(\pi)$ es positiva, $\forall\ \sigma \in \mathrm{Gal}(\overline{k}/k)$ (notamos que $v_P \circ \sigma : \overline{k}(X) \to \mathbb{Z}$ es valoración). Asociando a cada $v_P \circ \sigma$ el conjunto $\sigma(\overline{\mathcal{O}})$, se obtiene de la proposición 2.4.12 que $\{\sigma(\overline{\mathcal{O}}) \mid \sigma \in \mathrm{Gal}(\overline{k}/k)\}$ es finito. Y como $\mathrm{Gal}(\overline{k}/k)/\mathrm{Stab}(P)$ está en biyección con la órbita de P y este último es finito, de la proposición 1.28.7 se obtiene que $k(P) = \overline{k}^{\mathrm{Stab}(P)}$ es extensión finita de k de grado igual a la cardinalidad de la órbita de P. □

En la proposición siguiente se dará un esbozo de la demostración, la cual se encuentra en [9] (proposición 6.12, página 256).

Proposición 2.6.7. *Sea k un campo perfecto. Sea X/k cualquier curva completa no singular. Sea $\overline{k}$ la cerradura algebraica de k en una cerradura algebraica fija $\overline{k(X)}$ de $k(X)$. Sea $P \in X_{\overline{k}}$, y sea $\overline{\mathcal{O}}$ su dominio de ideales principales local asociado, con ideal maximal $\overline{\mathcal{M}}$. Sea $\mathcal{O} := \overline{\mathcal{O}} \cap k(X)$ y $\mathcal{M} := \overline{\mathcal{M}} \cap k(X)$. Entonces el isomorfismo natural $\overline{k} \to \overline{\mathcal{O}}/\overline{\mathcal{M}}$ se restringe a un isomorfismo de k-álgebras de $k(P)$ a $\mathcal{O}/\mathcal{M}$.*

Demostración. Supongamos primero que la inyección natural $k \to \mathcal{O}/\mathcal{M}$ es un isomorfismo, y queremos ver que en ese caso se tiene $k(P) = k$. Sea E/k cualquier extensión de Galois de k contenida en $\overline{k}$. Escribimos $E = k(\alpha)$ para algún $\alpha \in E$ con polinomio mínimo $f(y) \in k[y]$. Sea B la cerradura entera de $\mathcal{O}$ contenida en $E(X)$. Entonces $B = \mathcal{O}[\alpha]$ (por la proposición 1.20.1). Además, $f(y)$ es irreducible sobre $\mathcal{O}/\mathcal{M}$ ($\cong k$), y entonces esto implica que $\mathcal{M}B$ es primo en B. De aquí, se obtiene que $B = \overline{\mathcal{O}} \cap E(X)$. Similarmente, tenemos que $\sigma(\overline{\mathcal{O}}) \cap E(X) = B$, $\forall\ \sigma \in \mathrm{Gal}(\overline{k}/k)$. Supongamos que existe $\sigma \in \mathrm{Gal}(\overline{k}/k)$ tal que $\sigma(\overline{\mathcal{O}}) \neq \overline{\mathcal{O}}$. Como $\sigma(\overline{\mathcal{O}}) \subseteq \overline{\mathcal{O}}$ implica $\sigma(\overline{\mathcal{O}}) = \overline{\mathcal{O}}$ (pues $\sigma : \overline{k}(X) \to \overline{k}(X)$ es un automorfismo, y entonces $\sigma(\overline{\mathcal{O}})$ es un dominio de ideales principales local contenido en $\overline{\mathcal{O}}$ de cardinalidad igual a la de $\overline{\mathcal{O}}$), podemos asumir que $\exists \beta \in \overline{\mathcal{O}}$ tal que $\sigma(\beta) \neq \overline{\mathcal{O}}$. Entonces, del lema 2.6.2 se tiene que existe una extensión finita de Galois E/k tal que $L := k(X)(\sigma(\beta)) \subseteq E(X)$. Como $\sigma(\beta) \in \sigma(\overline{\mathcal{O}}) \cap E(X) = \overline{\mathcal{O}} \cap E(X)$ entonces tal β no puede existir, por lo que $\sigma(\overline{\mathcal{O}}) = \overline{\mathcal{O}}$, $\forall\ \sigma \in \mathrm{Gal}(\overline{k}/k)$, y entonces $\mathrm{Stab}(P) = \mathrm{Gal}(\overline{k}/k)$ y se tiene $k(P) = k$.

Supongamos que $\mathcal{O}/\mathcal{M}$ es cualquier extensión finita de k (del corolario 2.3.12 se sabe que $\mathcal{O}/\mathcal{M}$ siempre es finita sobre k). Sea $k' \subset \overline{k}$ la preimagen de $\mathcal{O}/\mathcal{M}$ bajo el isomorfismo natural $\overline{k} \to \overline{\mathcal{O}}/\overline{\mathcal{M}}$ (el morfismo natural $\mathcal{O}/\mathcal{M} \to \overline{\mathcal{O}}/\overline{\mathcal{M}}$ es inyectivo, pues si $r + \mathcal{M}, s + \mathcal{M} \in \mathcal{O}$ cumplen $r + \overline{\mathcal{M}} = s + \overline{\mathcal{M}}$ entonces $r - s \in \overline{\mathcal{M}}$, y además $r - s \in \mathcal{O} \subseteq k(X)$, y así $r - s \in \overline{\mathcal{M}} \cap k(X)$). Sea $\alpha \in k'$, con polinomio mínimo $f(y) \in k[y]$, tal que $k' = k(\alpha)$ (k' es la preimagen de la extensión finita $\mathcal{O}/\mathcal{M}$ sobre k, por lo que k'/k es finita, y es separable por ser k es perfecto, y por tanto es simple). La cerradura entera B de $\mathcal{O}$ en $k'(X)$ es igual a $\mathcal{O}[\alpha]$ (proposición 1.20.1). Sea $M' := \overline{\mathcal{M}} \cap B$. Notamos que la imagen de la función natural $B \to B/M'$ está contenido en $\mathcal{O}/\mathcal{M}$. Entonces la inclusión

natural $\mathcal{O}/\mathcal{M} \to B/M'$ es un isomorfismo. Sea $\mathcal{O}' := \overline{\mathcal{O}} \cap k'(X) = B_{M'}$. Sea $\mathcal{M}'$ el ideal maximal de $\mathcal{O}'$. Entonces podemos aplicar la discusión anterior al caso $\mathcal{O}'$ para obtener que $\mathrm{Stab}(P) \supseteq \mathrm{Gal}(\overline{k}/k')$. De aquí, se obtiene que $\overline{k}^{\mathrm{Stab}(P)} \subseteq k'$.

Supongamos ahora que k'/k es una extensión de Galois, y queremos ver que $k(P) = k'$. Se puede verificar el aso general en que k'/k es cualquier extensión separable. El ideal maximal $\mathcal{M}$ de $\mathcal{O}$ se factoriza en $B = \mathcal{O}[\alpha]$ como un producto de $\deg(f)$ ideales maximales distintos de B. Si ocurriera que $k(P) \neq k'$ entonces sea M el ideal maximal de $\overline{\mathcal{O}} \cap k(P)(X)$. Existen $[k' : k(P)] > 1$ ideales maximales distintos de B que contienen a M. Como $k'(X)/k(P)(X)$ es una extensión de Galois entonces podemos encontrar $\mu \in \mathrm{Gal}(k'/k(P))$ tal que $\mu(M) \neq M$. Por tanto, existe $\overline{\mu} \in \mathrm{Gal}(\overline{k}/k(P))$ tal que $\mu = \overline{\mu}|_{k'}$, y tal que $\overline{\mu}(\overline{\mathcal{O}} \neq \overline{\mathcal{O}}$. Esto contradice que $\mathrm{Gal}(\overline{k}/k(P)) = \mathrm{Stab}(P)$. De aquí, se obtiene que $k(P) = k'$, y se obtiene el resultado deseado. □

Definición 2.6.8. *Sea X/k una curva completa no singular, y tomamos k'/k cualquier extensión de k en $\overline{k}$. El conjunto de puntos k'-racionales de la curva X/k, el cual denotamos por $X(k')$, es el conjunto dado por*

$$X(k') := \{P \in X_{\overline{k}} | k(P) \subseteq k'\}$$

Observamos que $X(\overline{k}) = X_{\overline{k}}$ y que $X(k) = X(\overline{k})^{\mathrm{Gal}(\overline{k}/k)}$. Notamos también que $X(k')$ depende también de X/k y no solamente de $X_{\overline{k}}/\overline{k}$.

Sea E/k cualquier extensión en $\overline{k}$. Se obtiene de las definiciones que $X_{\overline{k}} = (X_E)_{\overline{k}}$. Sea $P \in X_{\overline{k}}$. Entonces el campo de definición de P sobre E, $E(P)$, es igual a $E \cdot k(P)$. Para verlo, sea Stab(P) el estabilizador de P bajo la acción de $\mathrm{Gal}(\overline{k}/k)$. El estabilizador de P bajo la acción de $\mathrm{Gal}(\overline{k}/E)$ es el subgrupo $\mathrm{Gal}(\overline{k}/E) \cap \mathrm{Stab}(P)$. Se obtiene entonces que

$$E(P) := \overline{k}^{\mathrm{Gal}(\overline{k}/E) \cap \mathrm{Stab}(P)} = \overline{k}^{\mathrm{Gal}(\overline{k}/E)} \overline{k}^{\mathrm{Stab}(P)} = E \cdot k(P)$$

donde la igualdad de enmedio es una de las consecuencias del teorema 1.27.6 mencionadas ahí. Sea k'/k cualquier extensión que contenga a E. Entonces $X(k') = X_E(k')$, ya que podemos utilizar que $k(P) \subseteq k'$ si y sólo si $E(P) \subseteq k'$ (lo cual se cumple pues si $k(P) \subseteq k'$ entonces como $E(P) = E \cdot k(P)$, y como $E \subseteq k'$, $k(P) \subseteq k'$, se obtiene que $E(P) \subseteq k'$ ($E(P)$ es el menor subcampo que contiene a $k(P)$ y E), y recíprocamente, si $E(P) \subseteq k'$, se obtiene que $E \cdot k(P) = E(P) \subseteq k'$ implica que $k(P) \subseteq k'$) para obtener $P \in X(k') \Leftrightarrow k(P) \subseteq k' \Leftrightarrow E(P) \subseteq k' \Leftrightarrow P \in X_E(k')$.

Lema 2.6.9. *Sea $\pi : X \to Y$ un morfismo de curvas completas no singulares sobre k. Sea $\overline{\pi} : X_{\overline{k}} \to Y_{\overline{k}}$ la extensión de π a $\overline{\pi}$.*

1. *Sea $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Entonces, $\forall\ P \in X_{\overline{k}}$, $\overline{\pi}(\sigma(P)) = \sigma(\overline{\pi}(P)))$. En particular, $\forall\ P \in X_{\overline{k}}$, $k(P) \supseteq k(\overline{\pi}(P))$.*

2. *Sea E/k cualquier extensión de k en $\overline{k}$. Entonces el morfismo $\overline{\pi}$ induce un morfismo natural $X(E) \to Y(E)$.*

Demostración. Supongamos que π está inducido por la inclusión $k(Y) \subseteq k(X)$. La restricción de $\mathrm{Gal}(\overline{k}(X)/k(X))$ a $\mathrm{Gal}(\overline{k}(Y)/k(Y))$ compuesta con la restricción de $\mathrm{Gal}(\overline{k}(Y)/k(Y))$ a $\mathrm{Gal}(\overline{k}/k)$ es igual a la restricción de $\mathrm{Gal}(\overline{k}(X)/k(X))$ a $\mathrm{Gal}(\overline{k}/k)$. Además, cada uno de estas tres restricciones es un isomorfismo, por el lema 2.6.2. Un elemento $\sigma \in \mathrm{Gal}(\overline{k}/k)$ actúa sobre $\overline{k}(X)$ como un automorfismo, y sobre $\overline{k}(Y)$ como la restricción de dicho automorfismo a $\overline{k}(Y)$, y denotamos a σ, al automorfismo de $\overline{k}(X)$ y a la restricción de éste a $\overline{k}(Y)$ simplemente por σ.

1. Para probar que $\overline{\pi}(\sigma(P)) = \sigma(\overline{\pi}(P))$, de las definiciones se obtiene que hay que probar que se cumple $\sigma(\mathcal{O}_P) \cap \overline{k}(Y) = \sigma(\mathcal{O}_P \cap \overline{k}(Y))$. Notamos que se cumple $\sigma(\mathcal{O}_P \cap \overline{k}(Y)) \subseteq \sigma(\mathcal{O}_P) \cap \overline{k}(Y)$ (pues σ es, en particular, un automorfismo de $\overline{k}(Y)$, por lo que $\sigma(\overline{k}(Y)) = \overline{k}(Y)$). Entonces, sea $f \in \sigma(\mathcal{O}_P) \cap \overline{k}(Y)$. Entonces $\sigma^{-1}(f) \in \mathcal{O}_P \cap \overline{k}(Y)$. Por tanto, $f \in \sigma(\mathcal{O}_P \cap \overline{k}(Y))$. Por tanto, se cumple la igualdad que se quería probar. Luego, se obtiene que $\mathrm{Stab}(P) \subseteq \mathrm{Stab}(\overline{\pi}(P))$, ya que si $\sigma \in \mathrm{Stab}(P)$ entonces por definición se tiene $\sigma(\mathcal{O}_P) = \mathcal{O}_P$, y usando la igualdad probada se obtiene $\mathcal{O}_P \cap \overline{k}(Y) = \sigma(\mathcal{O}_P \cap \overline{k}(Y))$, y como $\mathcal{O}_P \cap \overline{k}(Y)$ corresponde al punto $\overline{\pi}(P)$, se obtiene que $\sigma \in \mathrm{Stab}(\overline{\pi}(P))$. Finalmente, de la contención probada se obtiene $k(P) \supseteq k(\overline{\pi}(P))$, lo cual se obtiene de las definiciones.

2. Basta ver que $\overline{\pi} : X_{\overline{k}} \to Y_{\overline{k}}$ restringido al conjunto $X(E) := \{P \in X_{\overline{k}} \mid k(P) \subseteq E\}$ tiene a su imagen contenida en el conjunto $Y(E) := \{P \in Y_{\overline{k}} \mid k(P) \subseteq E\}$ (recordamos que el $\sigma \in \mathrm{Gal}(\overline{k}/k)$ que define la acción sobre las curvas $X_{\overline{k}}$ y $Y_{\overline{k}}$, así como el $\sigma \in \mathrm{Gal}(\overline{k}(Y)/k(Y))$ son solamente las restricciones de $\sigma \in \mathrm{Gal}(\overline{k}(X)/k(X))$ a $\overline{k}$ y a $\overline{k}(Y)$, respectivamente, y por eso denotamos a las tres por σ). Sea $P \in X(E)$ (es decir, se cumple que $k(P) \subseteq E$). Entonces basta ver que $\overline{\pi}(P) \in Y(E)$ (es decir, que $k(\overline{\pi}(P)) \subseteq E$), pero de (1) tenemos que $k(\overline{\pi}(P)) \subseteq k(P) \subseteq E$, y se obtiene el resultado. □

Definición 2.6.10. *Sea k cualquier campo, y X/k una curva completa no singular. Sea $Q \in X$ con dominio de ideales principales local asociado $\mathcal{O}_Q$ en $k(X)$. El grado de Q, denotado por* $\deg(Q)$*, es el entero* $[\mathcal{O}_Q/\mathcal{M}_Q : k]$.

Definición 2.6.11. *Sea k un campo perfecto, y X/k una curva completa no singular. Sea $Q \in X(\overline{k})$. El grado de P, denotado por* $\deg(P)$*, es el entero* $[k(P) : k]$

Notamos que de la proposición 2.6.7 se obtiene que, cuando k es perfecto, el grado de $P \in X(\overline{k})$ y el grado de la imagen Q de P bajo el morfismo natural $X_{\overline{k}} \to X$, son iguales.

Por otro lado, sea $X/\mathbb{F}_q$ una curva completa no singular. Fijamos una cerradura algebraica $\overline{\mathbb{F}_q(X)}$ de $\mathbb{F}_q(X)$. Sea $\mathbb{F}_{q^n}$ el único subcampo de $\overline{\mathbb{F}}_q$ de grado n sobre $\mathbb{F}_q$.

Lema 2.6.12. *Sea $X/\mathbb{F}_q$ una curva completa no singular. Entonces, $\forall\ n \in \mathbb{N}$, el conjunto $X(\mathbb{F}_{q^n})$ es finito.*

Demostración. Sea $x \in \mathbb{F}_q(X)$ tal que $\mathbb{F}_q(X)/\mathbb{F}_q(x)$ es extensión separable y finita (corolario 5.1.7). Por la observación 5.2.12 se obtiene que la cerradura entera B de $\mathbb{F}_q[x]$ en $\mathbb{F}_q(X)$ es dominio de Dedekind. Por la proposición 2.1.6 se obtiene que B tiene cocientes finitos. Por otro lado, notamos que para probar que $X(\mathbb{F}_{q^n})$ es finito, basta probar que el conjunto de puntos $P \in X_{\overline{\mathbb{F}_q}}$ tales que $\mathbb{F}_q(P)$ tiene cardinalidad menor o igual a q^n es un conjunto finito. Sea $\overline{\mathcal{O}}$ el dominio de ideales principales local asociado a P con ideal maximal $\overline{M}$, y tomamos $\mathcal{O} = \overline{\mathcal{O}} \cap \mathbb{F}_q(X)$, $\mathcal{M} = \overline{\mathcal{M}} \cap \mathbb{F}_q(X)$. De la proposición 2.6.7, tenemos que si $|\mathbb{F}_q(P)| \leq q^n$ entonces $|\mathcal{O}/\mathcal{M}| \leq q^n$. Como el dominio U de x en X tiene complemento finito (teorema 2.3.9) entonces podemos asumir, sin pérdida de generalidad, que $\mathcal{O}$ corresponde a un punto perteneciente a U (si correspondiera a un punto P' en el complemento de U en X entonces tendríamos de la demostración de la proposición 2.6.4 que la órbita de P tiene como imagen a P' bajo I, y del lema 2.6.6 se tiene que esta órbita es finita, y como $X \setminus U$ es finito entonces los puntos $P \in X_{\overline{\mathbb{F}_q}}$ que cumplen que $|\mathbb{F}_q(P)| \leq \mathbb{F}_{q^n}$ resulta ser finito también). Del teorema 2.2.10 se obtiene que $\mathcal{O}$ corresponde, de manera única, al ideal maximal $\mathcal{M} \cap B$ de B (recordamos que para una curva completa no singular X/k, tenemos $\mathcal{V}(k(X)/k) = \{v_{\mathcal{B}} \mid \mathcal{B} \in \mathrm{Max}(B)\} \sqcup \{v_{\mathcal{B}_i} \mid (1/x)B' = \prod_i^n \mathcal{B}_i^{e_i}\}$, donde B' es la cerradura entera de $k[1/x]$ en $k(X)$), y que $\mathcal{O}/\mathcal{M}$ es isomorfo a $B/B \cap \mathcal{M}$, por lo que la cardinalidad de este último cociente es menor o igual a q^n, y del lema 2.1.7 se obtiene que el conjunto de los ideales maximales M de B (que corresponden de manera única a puntos en el dominio U, por el teorema 2.3.9) tales que $|B/M| \leq q^n$ es finito. Por tanto, se obtiene que el conjunto de dominios de ideales principales locales $\mathcal{O}$ en $\mathbb{F}_q(X)$ tales que $|\mathcal{O}/\mathcal{M}| \leq q^n$ es un conjunto finito, y entonces el resultado quedará probado si logramos ver que el conjunto de dominios de ideales principales locales $\overline{\mathcal{O}}'$ en $\overline{\mathbb{F}_q}(X)$ tales que $\overline{\mathcal{O}}' \cap \mathbb{F}_q(X) = \mathcal{O}$ es finito. Pero de la demostración de la proposición 2.6.4 se sique que los elementos $\overline{\mathcal{O}}'$ que cumplen lo anterior son los elementos de la órbita de $\overline{\mathcal{O}}$, y del lema 2.6.6 se obtiene que este conjunto es finito. Se obtiene entonces el resultado. □

Proposición 2.6.13. *Sea $X/\mathbb{F}_q$ una curva completa no singular. Sea $N_n := |X(\mathbb{F}_{q^n})|$. Sea $b_d := |\{Q \in X | \deg(Q) = d\}|$. Entonces $N_n := \sum_{d|n} d b_d$.*

Demostración. Veamos primero que el conjunto de órbitas de $X(\mathbb{F}_{q^n})$ bajo la acción de $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ está en biyección con la unión $\cup_{d|n}\{Q \in X |\ |\mathcal{O}_Q/\mathcal{M}_Q| = q^d\}$, donde la asignación es como sigue: se toma una órbita cuyo representante

sea un punto $P \in X(\mathbb{F}_{q^n})$, y esta órbita es mandada al elemento $Q := I(P) \in X$ (donde I es la función de la proposición 2.6.4)

Veamos que esta asignación está bien definida. Sea P como en el párrafo anterior. Entonces de la proposición 2.6.7 se obtiene que $\mathbb{F}_q(P)$ es isomorfo a $\mathcal{O}_Q/\mathcal{M}_Q$. Además, como $\mathbb{F}_q(P) \subseteq \mathbb{F}_{q^n}$, se obtiene que $\mathbb{F}_q(P)$ tiene cardinalidad igual a q^d, para algún d que divida a n, y por tanto, $\mathcal{O}_Q/\mathcal{M}_Q$ también. Por tanto, la asignación está bien definida.

Para ver la suprayectividad, sea $Q \in X$ tal que $|\mathcal{O}_Q/\mathcal{M}_Q| = q^d$, con $d|n$. De la proposición 2.6.4 y su demostración, se obtiene que la imagen inversa de Q bajo la función I es igual a la órbita de cualquier punto P cuya imagen bajo I sea Q, y también que a Q le corresponde de manera única dicha órbita (pues los puntos en X están en biyección con las órbitas obtenidas bajo la acción de $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ sobre $X_{\overline{\mathbb{F}_q}}$). Sea $P \in I^{-1}(Q)$. Queremos ver que $P \in X(\mathbb{F}_{q^n})$. De la proposición 2.6.7, tenemos que $\mathcal{O}_Q/\mathcal{M}_Q$ es isomorfo a $\mathbb{F}_q(P)$, y por tanto este último tiene cardinalidad igual a q^d, y como $d|n$ entonces se obtiene que $\mathbb{F}_q(P) \subseteq \mathbb{F}_{q^n}$. Por tanto, se tiene la suprayectividad (en particular, de lo anterior notamos que la imagen inversa de Q es una órbita contenida en $X(\mathbb{F}_{q^n})$).

Para la inyectividad, notamos que si tenemos dos órbitas cuya imagen sea un mismo punto $Q \in X$ entonces de la proposición 2.6.4 y su demostración se obtiene que cada una de estas órbitas es la imagen inversa de Q bajo I, y por tanto las dos órbitas son iguales. Por tanto, se tiene la biyección buscada.

Luego, como $X(\mathbb{F}_{q^n})$ es la unión disjunta de dichas órbitas entonces podemos agruparlas como sigue: tomamos un representante P de cada órbita, y por el lema 2.6.6 tenemos que la cardinalidad de dicha órbita es igual a $[\mathbb{F}_q(P) : \mathbb{F}_q] = [\mathcal{O}_Q/\mathcal{M}_Q : \mathbb{F}_q] = \deg(Q)$ (donde la primera igualdad se obtiene de la proposición 2.6.7), y agrupamos entonces las órbitas cuya cardinalidad sea igual a $\deg(Q)$. Y como $\mathbb{F}_q(P) \subseteq \mathbb{F}_{q^n}$ entonces se obtiene que $\deg(Q) = d$, para algún $d|n$, y entonces el número de dichas órbitas es igual a b_d. Así, de esto y de la biyección, se obtiene el resultado. □

Lema 2.6.14. *Sea $X/\mathbb{F}_q$ una curva completa no singular. Fijamos un entero $e \geq 1$. Sea $k' := \mathbb{F}_{q^e}$. Sea $N'_n :=|X_{k'}(\mathbb{F}_{q^{en}})|$. Entonces $N'_n = N_{en}$.*

Demostración. Tenemos que N'_n es el número de puntos $Q' \in X_{k'}$ tales que $k'(Q') \subseteq \mathbb{F}_{(q^e)^n}$, y que N_{en} es el número de puntos $Q \in X$ tales que $\mathbb{F}_q(Q) \subseteq \mathbb{F}_{q^{en}}$. Si $Q' \in X_{k'}$ cumple lo primero entonces el conjunto de puntos contenidos en $\overline{k'}$, tales que cada uno de ellos es fijado por todos los elementos del $\mathrm{Stab}(Q')$, es un conjunto contenido en $\mathbb{F}_{(q^e)^n} = \mathbb{F}_{q^{en}}$, pero notamos que como $k' = \mathbb{F}_{q^e}$ entonces su cerradura entera es igual a $\overline{\mathbb{F}_q}$, y por tanto, se obtiene que $Q' \in X(\mathbb{F}_{q^{en}})$. Recíprocamente, si $Q \in X$ es tal que $\mathbb{F}_q(P) \subseteq \mathbb{F}_{q^{en}}$ entonces el conjunto de puntos contenidos en $\overline{\mathbb{F}_q}$, tales que cada uno de ellos es fijado por todos los elementos del $\mathrm{Stab}(Q)$, es un conjunto contenido en $\mathbb{F}_{q^{en}} = \mathbb{F}_{(q^e)^n}$, y como $k' = \mathbb{F}_{q^e}$ entonces la cerradura algebraica de $\mathbb{F}_q$ es igual a $\overline{k'}$, y por tanto, se obtiene que $Q \in X_{k'}(\mathbb{F}_{(q^e)^n})$. Así, se obtiene que $N'_n = N_{en}$. □

2.7. Grupo de clases de divisores

Sea A un dominio conmutativo. Recordamos que el conjunto $\mathcal{M}(A)$ de todos los ideales no triviales de A es un monoide conmutativo bajo la multiplicación de usual de ideales:

- (i) Dados $I, J \in \mathcal{M}(A)$, $IJ \in \mathcal{M}(A)$.
- (ii) El ideal $(1) = A$ es el elemento identidad bajo la multiplicación de ideales.

Cuando A no es un campo, el monoide $\mathcal{M}(A)$ no es un grupo, ya que si $a \in A \setminus \{0\}$ es un elemento invertible, entonces no existe ningún ideal $J \in \mathcal{M}(A)$ tal que $(a)J = A$. Por tanto, el ideal aA no es invertible en $\mathcal{M}(A)$. Sin embargo, cuando A es un dominio de Dedekind entonces el monoide es un grupo.

Sea $\mathcal{P}(A)$ el conjunto de ideales principales no triviales de A. El conjunto $\mathcal{P}(A)$ es un submonoide de $\mathcal{M}(A)$. Más aún, A es un dominio de ideales principales si y sólo si $\mathcal{P}(A) = \mathcal{M}(A)$

Recordamos también que si $\mathcal{M}$ es cualquier monoide con elemento unitario 1 entonces una relación de congruencias sobre $\mathcal{M}$ es una relación de equivalencia $\equiv$ tal que , para todo $I, I', J, J' \in \mathcal{M}$ con $I \equiv I'$ y $J \equiv J'$, se tiene $II' \equiv JJ'$. Sea $\overline{\mathcal{M}} := \mathcal{M}/\equiv$ el conjunto de clases de equivalencia de $\mathcal{M}$ bajo la relación de equivalencia $\equiv$. Cuando la relación de equivalencia $\equiv$ es una relación de congruencias entonces el conjunto $\overline{M}$ es un monoide bajo la multiplicación

$$\overline{\mathcal{M}} \times \overline{\mathcal{M}} \to \overline{\mathcal{M}}$$

$$(\text{clase de } I)(\text{clase de } J) \mapsto \text{clase de } IJ$$

Para que $\overline{\mathcal{M}}$ sea un grupo, es necesario y suficiente que para cada $I \in \mathcal{M}$ exista $J \in \mathcal{M}$ con $IJ \equiv 1 \equiv JI$. Entonces la clase de I en $\overline{\mathcal{M}}$ es igual al inverso de la clase de I.

Sea $\mathcal{M}$ un monoide conmutativo y $\mathcal{P}$ cualquier submonoide de $\mathcal{M}$. Se puede verificar que el submonoide $\mathcal{P}$ define una relación de congruencias sobre $\mathcal{M}$ como sigue: sean $I, J \in \mathcal{M}$. Entonces $I \equiv J$ si y sólo si existen $\alpha, \beta \in \mathcal{P}$ tales que $\alpha I = \beta J$.

Si A un dominio conmutativo entonces consideramos el monoide conmutativo $\mathcal{M}(A)$ que consiste de los ideales no cero de A (con el producto usual de ideales y elemento neutro $(1) = A$), el cual define una relación de congruencias

$$I \equiv J \iff \exists \alpha, \beta \in A \setminus \{0\} \text{ tal que } (\alpha)I = (\beta)J$$

Como $\equiv$ es una relación de equivalencia asociada a un submonoide de $\mathcal{A}$ (a saber, $\mathcal{P}(A)$) entonces es una relación de congruencias sobre $\mathcal{M}(A)$. Definimos $\mathrm{Cl}(A) := \mathcal{M}(A)/\equiv$.

Cuando A es un dominio de Dedekind entonces $\mathrm{Cl}(A)$ es un grupo con elemento identidad la clase de (1). Para verlo, sea $I \in \mathcal{M}(A)$, $I \neq A$, y sea $\alpha \in I$,

$\alpha \neq 0$. Como los ideales no triviales de A tienen una factorización única en un producto de ideales maximales, podemos escribir $(\alpha) = IJ$ para algún ideal $J \in \mathcal{M}(A)$. Entonces $IJ \subseteq (1)$, y la clase de J es el inverso de la clase de I en $\mathrm{Cl}(A)$.

Definición 2.7.1. *Sea A un dominio de Dedekind. Al grupo $\mathrm{Cl}(A)$ se le llama el grupo de clases de ideales de A.*

Lema 2.7.2. *Sea A un dominio conmutativo. Entonces $\mathrm{Cl}(A) = \{(1)\}$ si y sólo si A es un dominio de ideales principales.*

Demostración. Supongamos que $\mathrm{Cl}(A) = \{(1)\}$. Sea $I \in \mathcal{M}(A)$. Entonces existen $a, b \in A$ tales que $(a)I = (b)$. En particular, $b = ac$, para algún $c \in I$. Notamos entonces que $I = (c)$, ya que si $x \in I$ entonces $ax = bd$ para algún $d \in A$. De aquí, se obtiene que $a(x - cd) = 0$. Como A es un dominio, se obtiene que $x = cd \in (c)$. □

Sea B un dominio de Dedekind con campo de fracciones L. Sea $\mathcal{V}(L)$ el conjunto de todas las valoraciones no suprayectivas triviales de L. Sea

$$\mathrm{Div}(B) := \oplus_{\substack{v \in \mathcal{V}(L) \\ v(B) \geq 0}} \mathbb{Z} x_v$$

El grupo $\mathrm{Div}(B)$ es el grupo abeliano libre generado por el conjunto $\{x_v \mid \in \mathcal{V}(L) \text{ con } v(B) \geq 0\}$. Un elemento D de $\mathrm{Div}(B)$ es una suma de la forma $\sum_v a_v x_v$ con $a_v = 0$ para todos excepto para un número finito de valoraciones $v \in \mathcal{V}(L)$ con $v(B) \geq 0$. Sea

$$\mathrm{div}_B : L^* \to \mathrm{Div}(B)$$

$$f \mapsto \sum_{\substack{v \in \mathcal{V}(L) \\ v(B) \geq 0}} v(f) x_v$$

La función div_B está bien definida, pues todo elemento f de L^* es el cociente de dos elementos g y h en B. Como B es noetheriano, los ideales (gB) y (hB) están contenidos en únicamente un número finito de ideales maximales de B, digamos $M_1, \ldots M_r$. El teorema 2.2.10 nos dice que cada valoración de L que es no negativo sobre B es una valoración M-ádica, para algún $M \in \mathrm{Max}(B)$. Por la observación 1.17.7 se obtiene que $v(f) = 0$ para todas las valoraciones $v \in \mathcal{V}(L)$, $v(B) \geq 0$, excepto quizá para $v_{M_1}, \ldots, v_{M_r}$.

Proposición 2.7.3. *(Descripción aditiva del grupo de clases de ideales.) Sea B un dominio de Dedekind con campo de fracciones L. El homomorfismo de grupos*

$$\mathrm{cl} : \mathrm{Div}(B) \to \mathrm{Cl}(B)$$

$$x_v \mapsto \text{clase de } M_v \cap B$$

induce un isomorfismo de grupos de $\mathrm{Div}(B)/\mathrm{div}_B(L^*)$ *a* $\mathrm{Cl}(B)$.

Demostración. La función cl es suprayectiva. Para verlo, notamos que todo elementos $\mathcal{C} \in \mathrm{Cl}(B)$ es igual a un elemento de la forma 'clase de I' para algún ideal no cero I en B. Factorizamos $I = \prod_{i=1}^{r} M_i^{a_i}$. Recordamos que $M_i = \mathcal{M}_{v_{M_i}} \cap B$. Entonces $\mathrm{cl}(\sum_i a_i x_{v_{M_i}}) = \text{clase de } I = \mathcal{C}$.

Ahora, sea $f \in L^*$. Entonces $f = a/b$ con $a, b \in B$. Por tanto, $\mathrm{div}_B(f) = \mathrm{div}_B(a) - \mathrm{div}_B(b)$ y

$$\mathrm{cl}(\mathrm{div}_B(f)) = (\text{clase de } aB) \cdot (\text{clase de } bB)^{-1}$$

$$= \text{clase de } B$$

Se obtiene entonces $\mathrm{div}_B(L^*) \subseteq \mathrm{Ker}(\mathrm{cl})$. Sea $D \in \mathrm{Div}(B)$, y supongamos que $\mathrm{cl}(D) = (1)$. Escribimos $D = D_0 - D_\infty$, donde $D_0 = \sum a_v x_v$ y $D_\infty = \sum b_v x_v$ son tales que $a_v, b_v \geq 0$, para todo $v \in \mathcal{V}(L)$, $v(B) \geq 0$. Sean $I_{D_0} := \prod_v (M_v \cap B)^{a_v}$ y $I_{D_\infty} := \prod_v (M_v \cap B)^{b_v}$ inducidos por D_0 y D_∞, respectivamente. Entonces

$$\mathrm{cl}(D) = \text{clase de } B = (\text{clase de } I_{D_0})(\text{clase de } I_{D_\infty})^{-1}$$

En particular, clase de I_{D_0} = clase de I_{D_∞}. Por tanto, existen $\alpha, \beta \in B$ tales que $\alpha I_{D_0} = \beta I_{D_\infty}$. Escribiendo las factorizaciones de estos ideales explícitamente, obtenemos

$$\prod_v (\mathcal{M}_v \cap B)^{v(\alpha)} \prod_v (\mathcal{M}_v \cap B)^{a_v} = \prod_v (\mathcal{M}_v \cap B)^{v(\beta)} \prod_v (\mathcal{M}_v \cap B)^{b_v}$$

De la propiedad de factorización única de ideales se obtiene entonces que

$$\mathrm{div}_B(\alpha) + D_0 = \mathrm{div}_B(\beta) + D_\infty$$

Por tanto, $D = D_0 - D_\infty = \mathrm{div}_B(\beta/\alpha) \in \mathrm{div}_B(L^*)$.

Así, se obtiene que $\mathrm{div}_B(L^*) = \mathrm{Ker}(\mathrm{cl})$ y se obtiene el resultado. □

Sea L/k una extensión. Tomamos el conjunto de valoraciones suprayectivas de L triviales en k, $\mathcal{V}(L/k)$. Suponiendo que $\mathcal{V}(L/k) \neq \emptyset$, consideramos el grupo abeliano libre $\mathrm{Div}(L/k)$ generado por el conjunto $\{x_v | v \in \mathcal{V}(L/k)\}$, a saber,

$$\mathrm{Div}(L/k) := \oplus_{v \in \mathcal{V}(L/k)} \mathbb{Z} x_v$$

Definición 2.7.4. *El grupo* $\mathrm{Div}(L/k)$ *es el grupo el grupo de divisores de* L/k.

Un elemento D en $\mathrm{Div}(L/k)$ (llamado divisor) es de la forma $D = \sum a_v x_v$ con $a_v \in \mathbb{Z}$ y $a_v = 0$ para todos excepto para un número finito de elementos

$v \in \mathcal{V}(L/k)$. Si $a_v \geq 0, \forall v \in \mathcal{V}(L/k)$ entonces llamamos a D un divisor efectivo. Consideramos la función

$$\mathrm{div}_L : L^* \to \mathrm{Div}(L/k)$$

$$f \longmapsto \mathrm{div}_L(f) := \sum_{v \in \mathcal{V}(L/k)} v(f)x_v$$

Si no hay confusión, denotamos por div a la función div_L. Por la proposición 2.4.12 se obtiene que cuando L es una extensión finita de $k(x)$ entonces la función div está bien definida, ya que $\{v \in \mathcal{V}(L/k) | v(f) \neq 0\}$ es finito y por tanto $\sum_{v \in \mathcal{V}(L/k)} v(f)x_v \in \mathrm{Div}(L/k)$.

Se puede verificar que $\mathrm{div}(L^*)$ es un subgrupo de $\mathrm{Div}(L/k)$, y tenemos entonces

Definición 2.7.5. *Sea $L/k(x)$ una extensión finita. Definimos el grupo de Picard* $\mathrm{Pic}(L/k)$ *como el grupo cociente* $\mathrm{Div}(L/k)/\mathrm{div}(L^*)$.

Ahora, consideramos el caso de una curva completa no singular, y definiremos de manera similar su grupo de Picard.

Sea k un campo. Sea $k(X)/k$ un campo de funciones, y sea X/k la curva completa no singular asociada. Cada punto $P \in X$ tiene asociado un dominio de ideales principales $\mathcal{O}_P$ con valoración v_P. Entonces, definimos $\mathrm{Div}(X/k) := \oplus_{P \in X} \mathbb{Z}P$, y $\mathrm{div} : k(X)^* \to \mathrm{Div}(X/k)$, con $f \mapsto \sum_{P \in X} v_P(f)P$. Notamos que se puede identificar al conjunto X con $\mathcal{V}(k(X)/k)$, y por tanto se puede identificar el grupo $\mathrm{Div}(X/k)$ con el grupo $\mathrm{Div}(k(X)/k)$ de manera que la función div se identifica con $\mathrm{div}_{k(X)}$. Por el teorema 2.4.11, se obtiene que el kernel de la función div es igual a k^*, ya que $k(X)/k$ es campo de funciones y por tanto $k' = k$ en el teorema 2.4.11, por lo que $\mathrm{div}(f) = 0 \Rightarrow v_P(f) = 0 \forall P \in X \Rightarrow f \in \bigcap_{v_P \in \mathcal{V}(k(X)/k)} \mathcal{O}_P \Rightarrow f \in k' = k$. Recíprocamente, si $f \in k$ entonces $v_P = 0 \forall P \in X \Rightarrow \mathrm{div}(f) = 0$. Denotamos por $\mathrm{Pic}(X/k)$ al cociente de $\mathrm{Div}(X/k)$ por la imagen de div, es decir, $\mathrm{Pic}(X/k) := \mathrm{Div}(X/k)/\mathrm{div}(k(X)^*)$.

Sea k cualquier campo. Sea X/k cualquier curva completa no singular. Definimos la función grado $\deg : \mathrm{Div}(X/k) \to \mathbb{Z}$ como $\deg(\sum_{P \in X} a_P P) = \sum_{P \in X} a_P \deg(P)$ donde $\deg(P) := [\mathcal{O}_P/\mathcal{M}_P : k]$ (notamos que cada punto P tiene grado 1 si k es algebraicamente cerrado, donde recordamos también que $k \hookrightarrow \mathcal{O}_P/\mathcal{M}_P$ ya que $\mathcal{M}_P \cap k^* = \emptyset$).

Sea $\pi : X \to Y$ un morfismo de curvas completas no singulares sobre k de grado n. Por la proposición 2.5.7 tenemos que π es suprayectiva. Sea $P \in X$ y $\pi(P) \in Y$. Consideramos el grado residual $f_{P/\pi(P)} = [\mathcal{O}_P/\mathcal{M}_P : \mathcal{O}_{\pi(P)}/\mathcal{M}_{\pi(P)}]$. De las definiciones, se tiene que $\deg(P) = f_{P/\pi(P)} \deg(\pi(P))$. Además, a la extensión $k(X)/k(Y)$ se le asoció una función norma $N_{k(X)/k(Y)}$ (sección 1.22

del capítulo I). Consideramos entonces la siguiente función:

$$\mathrm{Norm}_{X/Y} : \mathrm{Div}(X/k) \to \mathrm{Div}(Y/k)$$

$$\sum_{P\in X} a_P P \mapsto \sum_{P\in X} a_P f_{P/\pi(P)}\pi(P)$$

Tenemos entonces:

Proposición 2.7.6. *Sea $\pi : X \to Y$ como antes. Entonces el siguiente diagrama es conmutativo:*

$$\begin{array}{ccccc} k(X)^* & \xrightarrow{\mathrm{div}} & \mathrm{Div}(X/k) & \xrightarrow{\deg} & \mathbb{Z} \\ \downarrow{\scriptstyle N_{k(X)/k(Y)}} & & \downarrow{\scriptstyle \mathrm{Norm}_{X/Y}} & & \downarrow \\ k(Y)^* & \xrightarrow{\mathrm{div}} & \mathrm{Div}(Y/k) & \xrightarrow{\deg} & \mathbb{Z} \end{array}$$

Demostración. Por el lema 2.2.5 se tiene que $\forall\ \alpha \in k(X)^*$, y $\forall\ Q \in Y$,

$$v_Q(N_{k(X)/k(Y)}(\alpha)) = \sum_{\{P\in X|\pi(P)=Q\}} f_{P/\pi(P)} v_P(\alpha)$$

Así, se tiene que

$$\sum_{Q\in Y} v_Q(N_{k(X)/k(Y)}(\alpha))Q = \sum_{Q\in Y} \Big(\sum_{\{P\in X|\pi(P)=Q\}} f_{P/\pi(P)} v_P(\alpha)\Big)Q$$

$$= \sum_{P\in X} v_P(\alpha) f_{P/\pi(P)}\pi(P)$$

por lo que el diagrama cuadrado izquierdo conmuta. Además, de las definiciones se obtiene que $\deg(P) = f_{P/\pi(P)}\deg(\pi(P))$, y por tanto,

$$\sum_{P\in X} a_P f_{P/\pi(P)}\pi(P) = \sum_{P\in X} a_P \deg(P)$$

y se obtiene que el diagrama cuadrado derecho también conmuta. Se obtiene entonces que el diagrama completo también conmuta. □

Teorema 2.7.7. *Sea k cualquier campo. Sea X/k una curva completa no singular. Entonces, $\forall\ \alpha \in k(X)^*$, $\deg(\mathrm{div}(\alpha) = 0)$.*

Demostración. Sea $x \in k(X)$ tal que $k(X)/k(x)$ es una extensión finita. Sea $\pi : X \to \mathbb{P}^1$ el morfismo de curvas asociado. Sea $\alpha \in k(X)^*$. Por la proposición 2.7.6, tenemos que $\deg(\mathrm{div}(\alpha)) = \deg(\mathrm{div}(N_{k(X)/k(x)}(\alpha)))$. Por tanto, si probamos que, $\forall\ \beta \in k[x]^*$, $\deg(\mathrm{div}(\beta)) = 0$ entonces quedará probado este

teorema (notamos que si B es la cerradura entera de $k[x]$ en $k(X)$ entonces de la proposición 1.2.15 se obtiene que $k(X)$ es el campo de fracciones de B, y como div es multiplicativa, basta ver el caso en que $\alpha \in B$. Pero también por el corolario 1.22.2 se obtiene entonces que $N_{k(X)/k(x)}(\alpha) \in k[x]$. Por tanto, basta que $\forall\ \beta \in k[x] \setminus \{0\}$, se cumple $\deg(\mathrm{div}(\beta)) = 0$). Si $\beta \in k[x] \setminus \{0\}$, escribimos la factorización de β en $k[x]$ como

$$\beta = \prod_{g(x) \text{ irreducible}} g(x)^{v_{g(x)}(\beta)}$$

De aquí, se obtiene que $\sum (\text{grado de } g(x)) v_{g(x)}(\beta) = \text{grado de } \beta = -v_\infty(\beta)$. Por la proposición 2.3.6 se tiene que $\mathcal{V}(k(x)/k) = \{v_{g(x)} | g(x) \text{ es irreducible en } k[x]\} \sqcup \{v_\infty\}$. Como $[\mathcal{O}_{v_{g(x)}}/\mathcal{M}_{v_{g(x)}} : k] = \text{grado de } g(x)$ y como $[\mathcal{O}_{v_\infty}/\mathcal{M}_{v_\infty} : k] = 1$, se obtiene que

$$\begin{aligned} \deg(\mathrm{div}(\beta)) &= \textstyle\sum_{v_P \in \mathcal{V}(k(x)/k)} v_P(\beta)\deg(P) \\ &= v_\infty(\beta) + \textstyle\sum_{g(x) \text{ irreducible}} v_{g(x)}(\beta)[k_{v_{g(x)}} : k] \\ &= 0 \end{aligned}$$

donde $k_{v_{g(x)}} := \mathcal{O}_{v_{g(x)}}/\mathcal{M}_{v_{g(x)}}$. Así, se obtiene el resultado deseado. □

Corolario 2.7.8. *Sea X/k una curva completa no singular. Entonces la función* $\deg : \mathrm{Div}(X/k) \to \mathbb{Z}$ *induce un homomorfismo de grupos no trivial,* $\deg' : \mathrm{Pic}(X/k) \to \mathbb{Z}$*, con* $D + \mathrm{div}(k(X)^*) \mapsto \deg(D)$.

Demostración. La función $\deg'$ está bien definida, pues si $D + \mathrm{div}(k(X)^*) = D' + \mathrm{div}(k(X)^*)$ entonces $D - D' \in \mathrm{div}(k(X)^*)$, por lo que $D - D' = \mathrm{div}(\alpha)$, para algún $\alpha \in k(X)^*$. De la definición de deg se obtiene $\deg(D - D') = \deg(D) - \deg(D')$, y entonces se obtiene que $\deg(D) - \deg(D') = \deg(D - D') = \deg(\mathrm{div}(\alpha)) = 0$, donde en la última igualdad se usó el teorema 2.7.7, por lo que $\deg(D) = \deg(D')$. Por tanto $\deg'$ está bien definida.

De la definición de deg, se obtiene que $\deg(D + D') = \deg(D) + \deg(D')$, y de esto se deduce que $\deg'$ es homomorfismo de grupos. Y como $\mathrm{Div}(X/k)$ contiene a un divisor efectivo cuya imagen bajo deg es positivo, se se obtiene que $\deg'$ es no trivial. Se obtiene así lo buscado. □

Denotamos de aquí en adelante como deg a la función $\deg'$.

Observación 2.7.9. *Sea X/k una curva completa no singular. Sea $\alpha \in k(X) \setminus k$. Entonces α define un morfismo no constante de curvas completas no singulares sobre k, $\pi : X \to \mathbb{P}^1$, inducido por la extensión $K(X)/k(\alpha)$. Sea $0 \in \mathbb{P}^1$ el punto correspondiente a la valoración (α)-ádica de $k[\alpha]$, y sea $\infty \in \mathbb{P}^1$ el punto correspondiente a la valoración $(1/\alpha)$-ádica de $k[1/\alpha]$. Definimos $(\alpha)_0 := \sum_{P \in \pi^{-1}(0)} v_P(\alpha)P$, y similarmente $(\alpha)_\infty = -\sum_{P \in \pi^{-1}(\infty)} v_P(\alpha)P$. Entonces, de las observaciones 2.5.3 y 2.5.4 se tiene*

$$\mathrm{div}(\alpha) = (\alpha)_0 - (\alpha)_\infty$$

y el teorema 1.18.4 implica que $\deg((\alpha)_0) = \deg((\alpha)_\infty) = [k(X) : k(\alpha)]$

Sea X/k una curva completa no singular. Sea $\mathrm{Div}^0(X/k)$ el kernel de la función $\deg : \mathrm{Div}(X/k) \to \mathbb{Z}$, y sea $\mathrm{Pic}^0(X/k)$ el kernel de la función $\deg : \mathrm{Pic}(X/k) \to \mathbb{Z}$. Se obtiene entonces que $\mathrm{Pic}^0(X/k) = \mathrm{Div}^0(X/k)/\mathrm{div}(k(X)^*)$, y se obtiene entonces de las definiciones que la sucesión

$$(1) \to k^* \to k(X)^* \overset{\mathrm{div}}{\to} \mathrm{Div}^0(X/k) \to \mathrm{Pic}^0(X/k) \to (0)$$

es exacta, donde div está bien definida por el teorema 2.7.7.

Proposición 2.7.10. *Sea k cualquier campo. Entonces la función*

$$\deg : \mathrm{Pic}(\mathbb{P}^1/\mathbb{Z}) \to \mathbb{Z}$$

es un isomorfismo. En particular, $\mathrm{Pic}^0(\mathbb{P}^1/k) = \{0\}$.

Demostración. Notamos que el conjunto $\mathcal{V}(k(x)/k)$ siempre contiene a una valoración correspondiente a un punto en $\mathbb{P}^1$ de grado 1, a saber v_∞ ($[k_\infty : k] = 1$, pues $\mathcal{O}_\infty/\mathcal{M}_\infty \cong k[1/x]_{(1/x)}/(1/x)k[1/x]_{(1/x)} \cong k[1/x]/(1/x) \cong k$), con $v_\infty(f) = -(\text{grado de } f(x))$ (lema 2.2.7). Por tanto, para toda $n \in \mathbb{Z}$, escribimos $n\{\infty\} + \mathrm{div}(k(x)^*)$ (∞ es el punto de $\mathbb{P}^1$ correspondiente a v_∞), y notamos que la imagen de este elemento bajo la función $\deg : \mathrm{Pic}(\mathbb{P}^1/k) \to \mathbb{Z}$ es igual a n, y se obtiene entonces que deg es suprayectiva. Veamos que $\mathrm{Pic}(k(x)/k) \cong \{nx_{v_\infty} + \mathrm{div}_{k(x)}(k(x)^*) \mid n \in \mathbb{Z}\}$. Por la proposición 2.3.6 sabemos que $\mathcal{V}(k(x)/k) = \{v_{g(x)} \mid g(x) \in k[x] \text{ es irreducible}\} \cup \{v_\infty\}$. Sea $g(x) \in k[x]$ irreducible. Se tiene entonces

$$\mathrm{div}_{k(x)}(g(x)) = \sum_{v \in \mathcal{V}(k(x)/k)} v(g(x))x_v = 1 \cdot x_{v_{g(x)}} - (\text{grado de } g(x))x_{v_\infty}$$

(pues tenemos que la factorización (única) en ideales maximales de $k[x]$ del ideal $(g(x)) \subseteq k[x]$ es $(g(x))$ mismo, el cual es maximal por ser $g(x)$ irreducible en $k[x]$, y entonces por definición $v_{f(x)}(g(x)) = 1$ si $f(x) = g(x)$ y $v_{f(x)}(g(x)) = 0$ si $f(x) \neq g(x)$, con $f(x)$ irreducible en $k[x]$, además de que $v_\infty(g(x)) = -(\text{grado de } g(x))$ (lema 2.2.7), y de aquí se obtiene que, en $\mathrm{Pic}(k(x)/k)$,

$$x_{v_{g(x)}} + \mathrm{div}_{k(x)}(k(x)^*) = (\text{grado de } g(x))x_{v_\infty} + \mathrm{div}_{k(x)}(k(x)^*)$$

Y como $\mathrm{Div}(k(x)/k)$ está generado por el conjunto $\{x_v \mid v \in \mathcal{V}(k(x)/k)\}$, se obtiene que $\mathrm{Pic}(k(x)/k)$ está generado por el elemento $\{x_{v_\infty} + \mathrm{div}_{k(x)}(k(x)^*)\}$. Además, notamos que este elemento no puede tener orden finito en $\mathrm{Pic}(k(x)/k)$, ya que deg es un homomorfismo de grupos y $\deg(x_{v_\infty}) = 1$ (donde identificamos a $\deg(x_{v_\infty})$ con $\deg(\{\infty\})$, que es igual a 1). Por tanto, $\deg : \mathrm{Pic}(k(x)/k) = \{nx_{v_\infty} + \mathrm{div}_{k(x)}(k(x)^*) \mid n \in \mathbb{Z}\} \to \mathbb{Z}$ es un isomorfismo. □

Teorema 2.7.11. *Sea k un campo finito. Sea X/k una curva completa no singular. Entonces* $\mathrm{Pic}^0(X/k)$ *es un conjunto finito.*

Demostración. Sea $d \in \mathbb{N}$. Sea $\mathrm{Pic}^d(X/k)$ el subconjunto de elementos pertenecientes a $\mathrm{Pic}(X/k)$ cuya imagen bajo deg es igual a d. Como $\deg : \mathrm{Pic}(X/k) \to \mathbb{Z}$ es homomorfismo de grupos, se obtiene que los conjuntos $\mathrm{Pic}^d(X/k)$ y $\mathrm{Pic}^0(X/k)$ están en biyección (si tenemos dos divisores $D, D' \in \mathrm{Pic}^d(X/k)$ entonces $\deg(D - D') = 0$, por ser homomorfismo de grupos, y por tanto $D - D' \in \mathrm{Pic}^0(X/k)$, y si fijamos D y tomamos $D'' \in \mathrm{Pic}^d(X/k)$ con $D' \neq D''$, se obtiene que las restas $D - D'$ y $D - D''$ son distintas y pertenecen ambas a $\mathrm{Pic}^0(X/k)$, y como $|\{D - D' \mid D' \in \mathrm{Pic}^d(X/k)\}| = |\mathrm{Pic}^d(X/k)|$, se obtiene que $|\mathrm{Pic}^d(X/k)| \leq |\mathrm{Pic}^0(X/k)|$. Similarmente, si $D' \in \mathrm{Pic}^0(X/k)$ y $D \in \mathrm{Pic}^d(X/k)$ entonces $\deg(D' + D) = d$, por ser homomorfismo de grupos, por lo que $D + D' \in \mathrm{Pic}^d(X/k)$, y si fijamos a D y tomamos $D'' \in \mathrm{Pic}^0(X/k)$ con $D' \neq D''$ entonces se tiene que las sumas $D + D'$ y $D + D''$ son distintas y pertenecen ambas a $\mathrm{Pic}^d(X/k)$, y como $|\{D + D' \mid D' \in \mathrm{Pic}^0(X/k)\}| = |\mathrm{Pic}^0(X/k)|$, se obtiene entonces que $|\mathrm{Pic}^0(X/k)| \leq |\mathrm{Pic}^d(X/k)|$, y por tanto se obtiene la igualdad $|\mathrm{Pic}^d(X/K)| = |\mathrm{Pic}^0(X/k)|$). Se obtiene entonces que $\mathrm{Pic}^d(X/K)$ es finito si y sólo si $\mathrm{Pic}^0(X/k)$ es finito. Sea $\mathrm{Eff}^d(X/k)$ el conjunto de divisores efectivos en $\mathrm{Div}(X/k)$ de grado d. Consideramos la restricción cl^d de la función $\mathrm{cl} : \mathrm{Eff}^d(X/k) \to \mathrm{Pic}^d(X/k)$, es decir,

$$\mathrm{cl}^d : \mathrm{Eff}^d(X/k) \to \mathrm{Pic}^d/(X/k)$$

Por la observación 4.2.3, se tiene que cl^d es suprayectivo si d es suficientemente grande. Por tanto, basta probar que $\mathrm{Eff}^d(X/k)$ es finito si d es suficientemente grande. Sea $x \in k(X)$ tal que $k(X)/k(x)$ es una extensión finita separable (corolario 5.1.7). Sea B la cerradura entera de $k[x]$ en $k(X)$. Como k es campo finito, se obtiene que B tiene cocientes finitos, por la proposición 2.1.6 y por el lema 2.1.7 se tiene que el número de ideales maximales $M \subset B$ con $|B/M| \leq d$ es finito. Ahora, por un lado el teorema 2.3.9 nos dice que el dominio U de x cumple que U es abierto afín y que $B = \mathcal{O}_X(U)$, y por definición el que sea afín implica que U está en biyección con $\mathrm{Max}(\mathcal{O}_X(U)) = \mathrm{Max}(B)$. Además, por el corolario 2.3.11 sabemos que el conjunto $\mathcal{V}(k(X)/k)$ es igual al conjunto de valoraciones $v_{\mathcal{B}}$, con $B \in \mathrm{Max}(B)$, unión con otro conjunto finito de valoraciones. Y ahora por otro lado, del teorema 2.2.10 obtenemos que $B/\mathcal{B} \cong \mathcal{O}_{v_{\mathcal{B}}}/\mathcal{M}_{v_{\mathcal{B}}}$, para todo $\mathcal{B} \in \mathrm{Max}(B)$, y por tanto tienen la misma cardinalidad. Así, juntando estos dos hechos, se obtiene que el número de valoraciones v en $\mathcal{V}(k(X)/k)$ cuyo campo residual $\mathcal{O}_v/\mathcal{M}_v$ tiene a lo más d elementos es un conjunto finito. Se concluye entonces que el número de puntos P en X tales que $\deg(P) = [\mathcal{O}_P/\mathcal{M}_P : k] \leq n$ es finito, para cualquier $n \in \mathbb{N}$ suficientemente grande. Así, obtenemos que el número de divisores $D = \sum a_P P$, tales que $a_P \geq 0$, $\forall\ P \in X$, y tales que $\sum a_P \deg(P) \leq d$, es también finito, y se obtiene el resultado. $\square$

3. Capítulo III - La racionalidad y la ecuación funcional de la función zeta sobre campos finitos

3.1. La racionalidad

En esta sección definimos la función zeta de una curva completa no singular sobre un campo finito y demostramos la racionalidad de dicha función.

Definición 3.1.1. *La función zeta de una curva completa no singular $X/\mathbb{F}_q$ es la serie de potencias* $\mathbf{Z}(X/\mathbb{F}_q, T) := \prod_{P\in X}(1-T^{\deg(P)})^{-1}$.

Sea $b_d := \{P \in X|\ |\mathcal{O}_P/\mathcal{M}_P| = q^d\}$. Sea $N_n = |X(\mathbb{F}_{q^n})|$. Entonces la proposición 2.6.13 muestra que $N_n = \sum_{d|n} db_d$. Veamos entonces que $\mathbf{Z}(T) := \mathbf{Z}(X/\mathbb{F}_q, T) = \exp(\sum_{n=1}^{\infty} N_n T^n/n)$. Observamos que si $|\mathcal{O}_P/\mathcal{M}_P| = q^d$ entonces $\deg(P) = [\mathcal{O}_P/\mathcal{M}_P : \mathbb{F}_q] = d$, ya que si $\deg(P) = d'$ entonces por ser $|\mathbb{F}_q| = q$ y del hecho de que todo elemento de $\mathcal{O}_P/\mathcal{M}_P$ se escribe de manera única como una combinación lineal de los elementos de la base con coeficientes en $\mathbb{F}_q$, se obtiene que $|\mathcal{O}_P/\mathcal{M}_P| = q^{d'}$, por lo que $d = d'$. Por tanto, $\{P \in X \mid |\mathcal{O}_P/\mathcal{M}_P| = q^d\} = \{P \in X \mid \deg(P) = d\}$, y podemos escribir

$$\mathbf{Z}(T) = \prod_{P\in X}(1-T^{\deg(P)})^{-1} = \prod_{d=1}^{\infty}(1-T^{\deg(P)})^{-b_d}$$

Recordando la sección 1.1 del capítulo 1 obtenemos que

$$\log(\mathbf{Z}(T)) = -\sum_{d=1}^{\infty} b_d \log(1-T^{\deg(P)})$$

Recordamos que

$$-\log(1-x) = x + x^2 + x^3 + \cdots = \sum_{n=1}^{\infty}\frac{x^n}{n}$$

Por tanto, se obtiene que

$$\log(\mathbf{Z}(T)) = \sum_{d=1}^{\infty} b_d(\sum_{i=1}^{\infty}\frac{(T^d)^i}{i})$$

Reordenando, se llega a que

$$\log(\mathbf{Z}(T)) = \sum_{n=1}^{\infty}(\sum_{d|n} db_d)\frac{T^n}{n} = \sum_{n=1}^{\infty} N_n\frac{T^n}{n}$$

y sacando la exponencial en cada lado de la última igualdad, se obtiene

$$\mathbf{Z}(T) = \exp(\sum_{n=1}^{\infty} N_n \frac{T^n}{n})$$

Se obtiene así el resultado.

Observación 3.1.2. *Notamos que el procedimiento utilizado para probar la igualdad* $\mathbf{Z}(T) = \exp(\sum_{n=1}^{\infty} N_n T^n/n)$ *puede usarse recíprocamente para probar que, si definimos la función zeta como*

$$\mathbf{Z}(T) := \exp(\sum_{n=1}^{\infty} N_n T^n/n)$$

donde $N_n = |X(\mathbb{F}_{q^n})|$ *entonces* $\mathbf{Z}(T) = \prod_{P \in X}(1 - T^{\deg(P)})^{-1}$. *En otras palabras, la definición 3.1.1 y la definición 3.1.3 siguiente son equivalentes.*

Definición 3.1.3. *La función zeta de una curva completa no singular* $X/\mathbb{F}_q$ *es* $\mathbf{Z}(X/\mathbb{F}_q, T) := \sum_{n=1}^{\infty} N_n \frac{T^n}{n}$, *donde* $N_n = |X(\mathbb{F}_{q^n})|$.

Notamos que, al ser $\mathbb{F}_q$ un campo finito, es un campo perfecto. Entonces podemos aplicar varias de las ideas vistas en la sección 2.4 del capítulo II al caso $k = \mathbb{F}_q$. Así, fijamos una cerradura algebraica $\overline{\mathbb{F}_q(X)}$ de $\mathbb{F}_q(X)$. Sea $\overline{\mathbb{F}_q}$ el subcampo de $\overline{\mathbb{F}_q(X)}$ isomorfo a la cerradura algebraica de $\mathbb{F}_q$. Sea e cualquier entero positivo primo relativo con p. Sea $\mathbb{F}_{q^e}$ el único subcampo de $\overline{\mathbb{F}_q}$ de grado e sobre $\mathbb{F}_q$. Como $\mathbb{F}_q$ es algebraicamente cerrado en $\mathbb{F}_q(X)$, el campo

$$\mathbb{F}_{q^e}(X) := \mathbb{F}_{q^e} \cdot \mathbb{F}_q(X) \subset \overline{\mathbb{F}_q(X)}$$

es un campo de funciones sobre $\mathbb{F}_{q^e}$, y su grado sobre $\mathbb{F}_q(X)$ también es igual a e. Sea $X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}$ la curva completa no singular asociada a $\mathbb{F}_{q^e}(X)/\mathbb{F}_{q^e}$. Las funciones zeta $\mathbf{Z}(X/\mathbb{F}_q, T)$ y $\mathbf{Z}(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T)$ están relacionadas como sigue:

Lema 3.1.4. $\mathbf{Z}(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e) = \prod_{i=1}^{e} \mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T)$, *donde* ξ_e *es una raíz primitiva e-ésima de la unidad.*

Demostración. Sea $N'_n := |X_{\mathbb{F}_{q^e}}(\mathbb{F}_{q^{ne}})|$. Por el lema 2.6.14 se tiene $N'_n = N_{ne}$. Recordamos también que $\sum_{i=1}^{e} (\xi_e^i)^m$ es igual a e si $e|m$, de lo contrario es igual a cero. Luego, tenemos que

$$\begin{aligned}
\log\left(\prod_{i=1}^{e} \mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T)\right) &= \sum_{i=1}^{e} \log(\mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T)) \\
&= \sum_{i=1}^{e} (\sum_{m=1}^{\infty} N_m (\xi_e^i)^m T^m/m) \\
&= \sum_{m=1}^{\infty} N_m (\sum_{i=1}^{e} (\xi_e^i)^m) T^m/m \\
&= \sum_{n=1}^{\infty} N_{en} T^{en}/n = \sum_{n=1}^{\infty} N'(T^e)^n/n \\
&= \log(\mathbf{Z}(X/\mathbb{F}_{q^e}/\mathbb{F}_{q^e}, T^e))
\end{aligned}$$

Así, se obtiene el resultado. □

Sea $X/\mathbb{F}_q$ cualquier curva completa no singular. Veremos que la serie de potencias $\mathbf{Z}(X/\mathbb{F}_q, T)$ es igual al cociente de dos polinomios. Tomamos el subconjunto de $\mathrm{Div}(X/\mathbb{F}_q)$ consistente de los divisores efectivos, $\mathrm{Eff}(X/\mathbb{F}_q)$.

Tenemos entonces que

$$\begin{aligned}
\mathbf{Z}(X/\mathbb{F}_q, T) &= \prod_{P \in X} (1 - T^{\deg(P)})^{-1} \\
&= \prod_{P \in X} (1 + T^{\deg(P)} + T^{2\deg(P)} + T^{3\deg(P)} + \cdots) \\
&= \sum_{D \in \mathrm{Eff}(X/\mathbb{F}_q)} T^{\deg(D)} \\
&= \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 0}} \Big(\sum_{\substack{D \in \mathrm{Eff}(X/\mathbb{F}_q) \\ \text{clase de } (D) = \zeta}} T^{\deg(D)} \Big)
\end{aligned}$$

Sea $\zeta \in \mathrm{Pic}(X/\mathbb{F}_q)$ y $E_\zeta := \{D \in \mathrm{Eff}(X/\mathbb{F}_q) | \text{ clase de } (D) = \zeta\}$.

Tenemos entonces

$$\sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 0}} \Big(\sum_{\substack{D \in \mathrm{Eff}(X/\mathbb{F}_q) \\ \text{clase de } (D) = \zeta}} T^{\deg(D)} \Big) = \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 0}} |E_\zeta| T^{\deg(\zeta)}$$

y así, se tiene

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 0}} |E_\zeta| T^{\deg(\zeta)} \tag{1}$$

Por el corolario 2.7.8 se obtiene que todos los divisores $D \in E_\zeta$ tienen el mismo grado d, a saber, $d = \deg(\zeta)$. En la demostración del teorema 2.7.11 se vio que, para todo $d \geq 0$, el número de divisores efectivos de grado d es finito, y por un corolario (4.2.9) del teorema de Riemann-Roch (teorema 4.2.8) se obtuvo que E_ζ no es vacío si d es suficientemente grande.

Además, el teorema de Riemann-Roch muestra la existencia de un entero $g \geq 0$, llamado el género de $X/\mathbb{F}_q$, tal que si $\deg(\zeta) \geq 2g - 1$ entonces

$$|E_\zeta| = \frac{q^{\deg(\zeta)+1-g} - 1}{q - 1}$$

Teorema 3.1.5. *Sea $X/\mathbb{F}_q$ una curva completa no singular de género g. Entonces*

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \frac{f(T)}{(1 - T)(1 - qT)}$$

donde $f(T) \in \mathbb{Z}[T]$ es un polinomio de grado a lo más $2g$. La función zeta tiene un polo simple en $T = 1$, y

$$\lim_{T \to 1} (T - 1)\mathbf{Z}(X/\mathbb{F}_q, T) = \frac{h}{q - 1}$$

donde $h := |\mathrm{Pic}^0(X/\mathbb{F}_q)|$ (llamado el número clase).

Demostración. Supongamos que $g \geq 1$. Usando (1), se obtiene

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0 \leq \deg(\zeta) \leq 2g-2}} |E_\zeta| T^{\deg(\zeta)} + \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 2g-1}} |E_\zeta| T^{\deg(\zeta)}$$

El teroema 2.7.11 muestra que la función $\deg : \mathrm{Pic}(X/\mathbb{F}_q) \to \mathbb{Z}$ tiene kernel finito $\mathrm{Pic}^0(X/\mathbb{F}_q)$ de cardinalidad h, y además, que para todo $d \in \mathbb{N}$, el conjunto $\mathrm{Pic}^d(X/\mathbb{F}_q) = \{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) | \deg(\zeta) = d\}$ es o vacío, o tiene cardinalidad h.

Sea e es el menor entero positivo que puede tomar la imagen $\deg(\mathrm{Pic}(X/\mathbb{F}_q))$, y sea ζ el elemento donde alcanza dicho valor. Entonces, si $\zeta' \in \mathrm{Pic}(X/\mathbb{F}_q)$ con $\deg(\zeta') \geq 0$, y si no es múltiplo de e entonces existen q, r únicos tales que $\deg(\zeta') = qe + r$, con $0 < r < e$, luego $\deg(\zeta' - q\zeta) = r$, con $\zeta' - q\zeta \in \mathrm{Pic}(X/\mathrm{F}_q)$, contradiciendo la hipótesis. Entonces $\deg(\zeta')$ es múltiplo de e, y siguiendo un proceso parecido se puede ver que $\deg(\zeta')$ sigue siendo múltiplo de e si $\deg(\zeta') < 0$.

Entonces, sea $e \in \mathbb{N}$ el único entero tal que

$$\mathrm{Pic}(X/\mathbb{F}_q) = e\mathbb{Z}$$

Se obtiene que

$$\sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 2g-1}} |E_\zeta| T^{\deg(\zeta)} = h \sum_{\substack{d \\ de \geq 2g-1}} \frac{q^{de+1-g} - 1}{q-1} T^{de}.$$

Si d_0 es el menor entero tal que $d_0 e \geq 2g-1$, se obtiene

$$\begin{aligned} \tfrac{h}{q-1}\Big(\sum_{de \geq 2g-1} (q^{de+1-g} - 1) T^{de}\Big) &= \\ \tfrac{h}{q-1}\Big(q^{d_0 e+1-g} T^{d_0 e}\Big(\sum_{d=0}^{\infty} (qT)^{de}\Big) - T^{d_0 e}\Big(\sum_{d=0}^{\infty} T^{de}\Big)\Big) &= \tfrac{h}{q-1}\Big(\tfrac{q^{d_0 e+1-g} T^{d_0 e}}{1-q^e T^e} - \tfrac{T^{d_0 e}}{1-T^e}\Big) \end{aligned}$$

$$= h \cdot \frac{u(T^e)}{(1-q^e T^e)(1-T^e)} \tag{2}$$

con

$$u(T^e) = \frac{(q^{d_0 e+1-g} T^{d_0 e})(1-T^e) - T^{d_0 e}(1-q^e T^e)}{q-1} \tag{3}$$

el cual se verifica que tiene coeficientes enteros. Además, como d_0 es el menor entero tal que $d_0 e \geq 2g-1$, y poniendo $T' = T^e$, se obtiene que $u(T^e)$ es un polinomio en T' de grado a lo más $2g$.

Por otro lado, observando la expresión

$$\sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \leq 2g-2}} |E_\zeta| T^{\deg(\zeta)} = h \sum_{\substack{d \\ 0 \leq de \leq 2g-2}} r_d T^{de} \tag{4}$$

donde r_d depende de los valores $|E_\zeta|$, encontramos que T está elevado a una potencia que es múltiplo de e, menor o igual a $2g-2$, por lo que escribiendo

nuevamente $T' = T^e$, obtenemos que la expresión es un polinomio en T' con coeficientes enteros de grado a lo más $2g-2$.

Sumando (2) y (4), obtenemos una expresión de la forma $\frac{f(T^e)}{(1-q^eT^e)(1-T^e)}$, donde $f(T^e)$ es un polinomio, con coeficientes enteros, igual a

$$h[(\sum_d r_d T^{de}(1-q^eT^e)(1-T^e))] + hu(T^e) \tag{5}$$

El segundo sumando es de grado a lo más $2g$ en la variable $T' = T^e$, mientras que el primer sumando tiene grado a lo más $2g-2+e+e$ en la variable T, por lo que es de grado a lo más $2g$ en $T' = T^e$.

Por tanto, $f(T^e)$ es de grado a lo más $2g$.

Además, se obtiene

$$\lim_{T\to 1}(T-1)\mathbf{Z}(X/\mathbb{F}_q) = \lim_{T\to 1}(T-1)\frac{f(T^e)}{(1-q^eT^e)(1-T^e)}$$

Por tanto, de la identidad $1-T^e = (1-T)(1+T+\cdots+T^{e-1})$, de (5) y de (3), se obtiene que

$$\lim_{T\to 1}(T-1)\mathbf{Z}(X/\mathbb{F}_q, T) = \frac{h}{(q-1)e} \tag{6}$$

Notamos entonces que, para el caso $g \geq 1$, el teorema se cumplirá si logramos probar que $e = 1$.

Supongamos que $g = 0$. Entonces, se deduce que $|E_\zeta| = (q^{\deg(\zeta)+1}-1)/(q-1)$ si $\deg(\zeta) \geq 0$, y por tanto

$$\begin{aligned}
\mathbf{Z}(X/\mathbb{F}_q, T) &= \sum_{\substack{\zeta \\ \deg(\zeta)\geq 0}} |E_\zeta| T^{\deg(\zeta)} \\
&= h\sum_{\substack{d \\ de\geq 0}} (\frac{q^{de+1}-1}{q-1})T^{de} \\
&= \tfrac{h}{q-1}(q\textstyle\sum_{\substack{d \\ de\geq 0}} q^{de}T^{de} - \sum_{\substack{d \\ de\geq 0}} T^{de}) \\
&= \tfrac{h}{q-1}(\tfrac{q}{1-(qT)^e} - \tfrac{1}{1-T^e}) \\
&= \tfrac{f(T^e)}{(1-(qT)^e)(1-T^e)}
\end{aligned}$$

donde

$$f(T^e) = h[\frac{q(1-T^e)-(1-(qT)^e)}{q-1}] \tag{7}$$

De (7) notamos que $f(T^e)$ es un polinomio en la variable $T' = T^e$ y se puede verificar que tiene coeficientes enteros. Sin embargo, de (7) también notamos que si $e = 1$ entonces $f(T^e) = h$, es decir, es un polinomio de grado a lo más $0 = 2g$, y también se cumple que $\lim_{T\to 1}(T-1)(\mathbf{Z}(X/\mathbb{F}_q, T)) = \frac{h}{q-1}$. Por tanto, si probamos la siguiente proposición entonces el teorema quedará probado. □

Proposición 3.1.6. *Sea $X/\mathbb{F}_q$ una curva completa no singular. La función* $\deg : \mathrm{Pic}(X/\mathbb{F}_q) \to \mathbb{Z}$ *es suprayectiva (i.e., $e = 1$).*

Demostración. Sea $e \in \mathbb{N}$ tal que $\deg(\mathrm{Pic}(X/\mathbb{F}_q)) = e\mathbb{Z}$. Consideramos la curva $X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}$, obtenida de $X/\mathbb{F}_q$ por cambio de base. Sea ξ_e una raíz e-ésima de la unidad en $\overline{\mathbb{Q}}$. Por lema 3.1.4 se tiene que

$$\mathbf{Z}(X_{q^e}/\mathbb{F}_{q^e}, T^e) = \prod_{i=1}^{e} \mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T)$$

Notamos que, haciendo $T' = T^e$, el lado izquierdo de la igualdad tiene un polo simple en $T' = 1$, pues podemos aplicar la fórmula (6) a la función zeta $\mathbf{Z}(X_{q^e}/\mathbb{F}_{q^e}, T^e)$, mientras que el lado derecho de la igualdad tiene un polo de orden e, esto último debido a que

$$\prod_{i=1}^{e} \mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T) = \left(\frac{f(T^e)}{(1 - q^e T^e)(1 - T^e)}\right)^e$$

En particular, el lado derecho tiene un polo de orden e en $T' = 1$.

Se obtiene de la igualdad y de la comparación del orden del polo en $T' = 1$ que $e = 1$. □

Se concluye así la proposición y la demostración del teorema.

Escribimos la función $f(T) \in \mathbb{Z}[T]$ de la forma $f(T) = c_0 + c_1 T + \cdots + c_{2g} T^{2g}$, con los $c_i \in \mathbb{Z}$, $i = 1, \ldots, 2g$, no necesariamente distintos de cero (pues $f(T)$ es de grado a lo más $2g$, no necesariamente igual a 2g). Observamos de la definición de $\mathbf{Z}(T) = \mathbf{Z}(X/\mathbb{F}_q, T)$ que $\mathbf{Z}(0) = 1$. Y por otro lado, usando el teorema 3.1.5, se obtiene que $\mathbf{Z}(0) = f(0)$. Por tanto, se obtiene $c_0 = 1$. Así, podemos factorizar a $f(T) \in \mathbb{Z}[T]$ como un producto en $\overline{\mathbb{Q}}[T]$ de la forma

$$f(T) = \prod_{i=1}^{2g} (1 - w_i T)$$

con $w_i \in \overline{\mathbb{Q}}$, $i = 1, \ldots, 2g$, enteros algebraicos no necesariamente distintos de cero (notamos que son efectivamente algebraicos, ya que si definimos $h(s) := s^{2g} f(1/s)$ entonces $h(s)$ es mónico de grado a lo más $2g$ en $\mathbb{Z}[s]$ y se cumple que $h(w_i) = 0$, $\forall\ i = 1, \ldots, 2g$). Sin embargo, veremos en la siguiente parte que el grado de $f(T)$ es exactamente igual a $2g$, por lo que se seguirá que $w_i \neq 0\ \forall$ $i = 1, \ldots, 2g$.

3.2. La ecuación funcional

En esta sección demostramos la ecuación funcional de la función zeta de una curva completa no singular sobre un campos finito.

Tenemos, de la racionalidad de la función zeta, que $\mathbf{Z}(T) := \mathbf{Z}(X/\mathbb{F}_q, T) = \prod_{i=1}^{c}(1 - w_i T)/(1 - qT)(1 - T)$ (con $c \leq 2g$), y suponiendo que $w_i \neq 0$ para cada i (lo cual será cierto al probar el siguiente teorema), es decir, suponiendo que $c = 2g$, encontramos que

$$\begin{aligned}
\mathbf{Z}(1/qT) &= \prod_{i=1}^{c}(1 - \frac{w_i}{qT})/(1 - \frac{1}{T})(1 - \frac{1}{qT}) \\
&= qT^2 \cdot \tfrac{1}{(1-qT)(1-T)} \prod_{i=1}^{c}(1 - w_i/qT) \\
&= (-1)^c(\prod_{i=1}^{c} w_i) q^{1-c} T^{2-c} \cdot \frac{\prod_{i=1}^{c}(1 - \frac{q}{w_i}T)}{(1 - qT)(1 - T)} \qquad (*)
\end{aligned}$$

Teorema 3.2.1. *Sea $X/\mathbb{F}_q$ una curva completa no singular de género g. Entonces, tomando $\mathbf{Z}(T) = \frac{f(T)}{(1-qT)(1-T)}$, se tiene que $f(T)$ tiene grado exactamente igual a $2g$, y además, se cumplen las siguientes condiciones equivalentes:*

- *(i) $\mathbf{Z}(1/qT) = (qT^2)^{1-g}\mathbf{Z}(T)$.*
- *(ii) $\prod_{i=1}^{2g} w_i = q^g$, y la función $w_i \mapsto q/w_i$, del conjunto $\{w_1, w_2, \cdots, w_{2g}\}$ en sí mismo, está bien definida y es biyectiva.*

Notamos que, de (ii), se obtiene que $w_i \neq 0$ para cada i.

Demostración. El teorema 4.2.8 asegura la existencia de un entero, el cual es precisamente g, y, para cada $\zeta \in \mathrm{Pic}(X/\mathbb{F}_q)$, de un entero no negativo $h^0(\zeta)$, tal que

(1) $|E_\zeta| = \frac{q^{h^0(\zeta)}-1}{q-1}$, y

(2) si $\deg(\zeta) \geq 2g - 1$ entonces $h^0(\zeta) = \deg(\zeta) + 1 - g$

Más aún, también nos asegura la existencia de un elemento $\mathcal{K} \in \mathrm{Pic}^{2g-2}(X/\mathbb{F}_q)$ (llamado la clase canónica), tal que , $\forall\ \zeta \in \mathrm{Pic}(X/\mathbb{F}_q)$, se tiene

(3) $h^0(\zeta) = \deg(\zeta) + 1 - g + h^0(\mathcal{K} - \zeta)$

Consideramos esta última condición (3), y veamos primero que (i) se cumple.

Tomemos $\mathbf{Z}'(T) = (q - 1)\mathbf{Z}(T)$. Entonces

$$\mathbf{Z}'(T) = (q - 1) \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 0}} |E_\zeta| T^{\deg(\zeta)}$$

Usando (1), podemos reescribir $\mathbf{Z}'(T)$ como la suma de dos términos $\alpha(T) + \beta(T)$, donde

$$\alpha(T) := \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0 \leq \deg(\zeta) \leq 2g-2}} q^{h^0(\zeta)} T^{\deg(\zeta)}$$

y

$$\beta(T) = \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 2g-1}} q^{h^0(\zeta)} T^{\deg(\zeta)} - \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\zeta) \geq 0}} T^{\deg(\zeta)}$$

Usando (2), obtenemos

$$\begin{array}{rcl} \beta(T) & = & h \sum_{d \geq 2g-1} q^{d+1-g} T^d - h \sum_{d \geq 0} T^d \\ & = & h q^{1-g} (qT)^{2g-1} (\sum_{f \geq 0} (qT)^f) - \frac{h}{1-T} \\ & = & h(\frac{q^g T^{2g-1}}{1-qT}) - h(\frac{1}{1-T}) \end{array}$$

De esto último se obtiene que $\beta(1/qT) = q^{1-g} T^{2-2g} \beta(T)$, ya que, después de hacer los cálculos necesarios, se obtiene que

$$\beta(1/qT) = h(\frac{q^g (1/qT)^{2g-1}}{1 - q(1/qT)}) - h(\frac{1}{1-(1/qT)}) = h(\frac{qT}{1-qT}) - h(\frac{q^{1-g} T^{2-2g}}{1-T})$$

donde la última expresión se puede verificar que es igual a $q^{1-g} T^{2-2g} \beta(T)$.

Consideramos ahora el caso de $\alpha(T)$. Sea $\mathcal{K} \in \mathrm{Pic}^{d_0}(X/\mathbb{F}_q)$ cualquier clase de grado d_0. La función

$$\bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathbb{F}_q) \longrightarrow \bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X(\mathrm{F}_q)$$

$$\zeta \to \mathcal{K} - \zeta$$

está bien definida, ya que si $0 \leq \deg(\zeta) \leq d_0$ (con $\zeta \in \bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathbb{F}_q)$) entonces

$$0 \leq \deg(\mathcal{K} - \zeta) = \deg(\mathcal{K}) - \deg(\zeta) \leq d_0$$

por lo que $\mathcal{K} - \zeta \in \bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathrm{F}_q)$ Además, si

$$\zeta, \zeta' \in \bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathbb{F}_q) \subseteq \mathrm{Pic}(X/\mathbb{F}_q)$$

con $\mathcal{K} - \zeta = \mathcal{K} - \zeta'$, entonces por ser $\mathrm{Pic}(X/\mathbb{F}_q)$ un grupo, se obtiene que $\zeta = \zeta'$, por lo que la función es inyectiva.

También, si $\zeta \in \bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathbb{F}_q)$ entonces ζ es imagen, bajo la función, del elemento $\mathcal{K} - \zeta$ (el cual pertenece a $\bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathrm{F}_q)$, como se vio). Por tanto, la función es suprayectiva. En particular, esta biyección es válida cuando

$\mathcal{K}$ es la clase canónica (es decir, $d_0 = 2g-2$), y utilizando esta biyección, podemos escribir

$$\alpha(T) = \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0 \leq \deg(\zeta) \leq 2g-2}} q^{h^0(\zeta)} T^{\deg(\zeta)} = \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0 \leq \deg(\zeta) \leq 2g-2}} q^{h^0(\mathcal{K}-\zeta)} T^{\deg(\mathcal{K}-\zeta)}$$

Y ahora, aplicando (3), encontramos que

$$\begin{aligned} \alpha(T) &= \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0 \leq \deg(\zeta) \leq 2g-2}} q^{h^0(\zeta)-\deg(\zeta)-1+g} T^{\deg(\mathcal{K})-\deg(\zeta)} \\ &= q^{g-1} T^{\deg(\mathcal{K})} \sum_{\substack{\zeta \in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0 \leq \deg(\zeta) \leq 2g-2}} q^{h^0(\zeta)} \cdot \frac{1}{(qT)^{\deg(\zeta)}} \\ &= q^{g-1} T^{2g-2} \alpha(1/qT) \end{aligned}$$

Es decir, $\alpha(1/qT) = q^{1-g} T^{2-2g} \alpha(T)$.

Por lo tanto, juntando los casos de $\beta(T)$ con $\alpha(T)$ tenemos

$$\begin{aligned} (q-1)\mathbf{Z}(1/qT) &= \alpha(1/qT) + \beta(1/qT) \\ &= q^{1-g} T^{2-2g} \alpha(T) + q^{1-g} T^{2-2g} \beta(T) \\ &= q^{1-g} T^{2-2g} (q-1)\mathbf{Z}(T) \end{aligned}$$

y por tanto se obtiene el resultado.

Ahora, notamos que el hecho de que se cumpla (i) implica que el grado de $f(T)$ es $c = 2g$. Para verlo, notamos que, por un lado, de (*) tenemos

$$\mathbf{Z}(T) = qT^2 \cdot \frac{1}{(1-qT)(1-T)} \cdot \prod_{i=1}^{c} (1 - \frac{w_i}{qT})$$

y por otro lado, de (i) tenemos

$$\mathbf{Z}(1/qT) = (qT^2)^{1-g} \cdot \frac{\prod_{i=1}^{c} (1 - w_i T)}{(1-qT)(1-T)}$$

Así, igualando ambos expresiones y cancelando términos, obtenemos

$$qT^2 \cdot \prod_{i=1}^{c} (1 - \frac{w_i}{qT}) = (qT)^{1-g} \cdot \prod_{i=1}^{c} (1 - w_i T)$$

Desarrollando ambos lados de esta igualdad, luego multiplicando ambos lados por $(qT)^c$, y luego comparando los términos de cada lado de la igualdad (y en particular los términos de mayor grado en cada lado de la igualdad), se puede verificar que $c = 2g$.

Así, sólo resta ver que se cumple la equivalencia. Supongamos que se cumple (ii). Como $\prod_{i=1}^{2g} w_i = q^q$ entonces se obtiene que $w_i \neq 0 \ \forall i = 1, \ldots, 2g$, y entonces podemos aplicar (*). Como $c = 2g$, y sustituyendo $\prod_{i=1}^{2g} w_i = q^g$ y los

elementos q/w_i por w_i en (*) (lo cual es posible por la biyección que se cumple por hipótesis), se obtiene (i). Ahora supongamos que se cumple (i). Haciendo el mismo procedimiento para ver que el grado de $f(T)$ es igual a $2g$ y comparando los términos de mayor grado en cada lado de la igualdad, se puede verificar que $\prod_{i=1}^{2g} w_i = q^g$. Además, como $w_i \neq 0 \ \forall \ i = 1, \ldots, 2g$ entonces de (i) y de (*) se obtiene que el conjunto $\{\frac{q}{w_1}, \ldots, \frac{q}{w_{2g}}\}$ (las soluciones de $\mathbf{Z}(1/qT)$) y el conjunto $\{\frac{1}{w_1}, \ldots, \frac{1}{w_{2g}}\}$ (las soluciones de $\mathbf{Z}(T)$) son el mismo conjunto. Se obtiene que la función dada en (ii) está bien definida y es biyectiva. Así, se obtiene la equivalencia y se obtiene el resultado. □

4. Capítulo IV - El teorema de Riemann-Roch

En este capítulo se prueba el teorema de Riemann-Roch así como algunas consecuencias del mismo que son claves para la demostración de la racionalidad y la ecuación funcional que se expuso en el capítulo 3.

4.1. El k-espacio vectorial $H^0(D)$

Sea X/k cualquier curva completa no singular. Sea O el elemento identidad de $\mathrm{Div}(X/k)$. Consideramos el siguiente orden parcial $\geq$ en el grupo $\mathrm{Div}(X/k)$:

$$D' \geq D \text{ si y sólo si } D' - D \text{ es un divisor efectivo.}$$

En particular, tenemos que D es un divisor efectivo si y sólo si $D \geq O$. A cada $\alpha \in k(X)^*$ se le asocia un divisor $\mathrm{div}(\alpha)$, y podemos agregar un nuevo elemento, denotado por $\mathrm{div}(0)$, al conjunto $\mathrm{Div}(X/k)$ y extendemos el orden parcial $\geq$ al conjunto $\mathrm{Div}(X/k) \bigsqcup \mathrm{div}(0)$ mediante $\mathrm{div}(0) \geq D \ \forall D \in \mathrm{Div}(X/k)$.

Consideremos el siguiente conjunto asociado a cada divisor $D \in \mathrm{Div}(X/k)$: $H^0(D) := \{\alpha \in \mathrm{Div}(X/k) | \mathrm{div}(\alpha) + D \geq O\}$ y notamos lo siguiente.

Observación 4.1.1. *Sea k algebraicamente cerrado. Sea $D = \sum_{i=1}^{s} \geq O$ un divisor efectivo. Entonces se puede verificar que $H^0(D)$ es igual al conjunto de funciones en $k(X)$ con polos de orden a lo más a_i en P_i y sin polos en ningún otro punto, esto es, $\alpha \in H^0(D) \iff |v_{P_i}(\alpha)| \leq a_i$, $1 \leq i \leq s$ y $v_P(\alpha) \geq 0$, $P \neq P_i \ \forall i$. En particular, $H^0(D) \supseteq k$.*

Observación 4.1.2. *Sea $D = O$. Entonces $H^0(D) = k$ ya que por el teorema 2.4.11, tenemos que las únicas funciones en $k(X)$ sin polos son las funciones constantes.*

Similarmente, tenemos que si $\alpha \in k(X)^*$ entonces $H^0(\mathrm{div}(\alpha)) = k\alpha^{-1}$, ya que de la definición se tiene que $\alpha^{-1} \in H^0(\mathrm{div}(\alpha))$ y tomando cualquier otro $\beta \in H^0(\mathrm{div}(\alpha))$, $\beta \neq 0$, se tiene también por definición que $\mathrm{div}(\beta) + \mathrm{div}(\alpha) \geq O$, por lo que $\mathrm{div}(\beta\alpha) \geq O$, y del teorema 2.4.11, obtenemos que $\beta\alpha \in k$, y se obtiene el resultado.

Observación 4.1.3. *Sea $D \in \mathrm{Div}(X/k)$ tal que $\deg(D) < 0$. Entonces $H^0(D) = \{0\}$, ya que si $\alpha \in k(X)^*$ entonces $\deg(\mathrm{div}(\alpha) + D) = 0 + \deg(D) < 0$ (la igualdad se obtiene del teorema 2.7.7), por lo que $\mathrm{div}(\alpha) + D$ no puede ser un divisor efectivo (si lo fuera entonces ocurriría que $\deg(\mathrm{div}(\alpha) + D) \geq 0$, lo cual es una contradicción), y se obtiene que el resultado.*

Observación 4.1.4. *Sea $D \in \mathrm{Div}(X/k)$ tal que $\deg(D) = 0$. Entonces $H^0(D)$ tiene dimensión a lo más uno, ya que suponiendo que $H^0(D)$ tiene dimensión positiva y que contiene una función distinta de cero α, tenemos entonces $\mathrm{div}(\alpha) + D \geq O$. Por el teorema 2.7.7 se obtiene $\deg(\mathrm{div}(\alpha) + D) = 0$, lo que implica que el coeficiente de cada P es igual a 0 (pues $\deg(P) \geq 1$ para cada P),*

por lo que se obtiene que $D = -\mathrm{div}(\alpha)$*, y si* $\beta \in H^0(D)$ *entonces debe ocurrir que* $O \leq \mathrm{div}(\beta) + D = \mathrm{div}(\beta) - \mathrm{div}(\alpha) \Rightarrow \mathrm{div}(\frac{\beta}{\alpha}) \geq O$*, y por el teorema 2.4.11, se obtiene que* $\frac{\beta}{\alpha}$ *es constante, y por tanto* β *es múltiplo de* α*, por lo que se obtiene que* $H^0(D) = k\alpha$ *y se obtiene el resultado.*

Utilizando la observación 4.1.1 se puede verificar que el conjunto $H^0(D)$ tiene estructura de k-espacio vectorial, donde si $\alpha, \beta \in H^0(D)$ y $c \in k$ entonces se tiene que $\alpha + \beta$ y $c\alpha$ pertenecen a $H^0(D)$. Denotamos por $h^0(D)$ a la dimensión de $H^0(D)$.

Lema 4.1.5. *Sea* k *cualquier campo. Sea* X/k *una curva completa no singular. Sea* $\zeta \in \mathrm{Pic}(X/k)$*. Supongamos que* $E_\zeta \neq \emptyset$*, y sea* $D \in E_\zeta$*. Sea* $\psi_D : H^0(D) \setminus \{0\} \to E_\zeta$ *con* $\alpha \to \mathrm{div}(\alpha) + D$*. Entonces la función* ψ_D *es suprayectiva. Más aún, el grupo* k^* *actúa sobre* $H^0(D) \setminus \{0\}$ *mediante*

$$k^* \times H^0(D) \setminus \{0\} \longrightarrow H^0(D) \setminus \{0\}$$

$$(c, \alpha) \mapsto c\alpha$$

y E_ζ *puede ser identificado con el cociente de* $H^0(D) \setminus \{0\}$ *por la acción de* k^**.*

Demostración. Para probar que es suprayectiva hay que ver que, dado $D' \in E_\zeta$, existe $\alpha \in H^0(D) \setminus \{0\}$ tal que $\mathrm{div}(\alpha) + D = D'$, es decir, $\mathrm{div}(\alpha) = D' - D$. Por definición, se tiene que la clase de D' es la misma que la clase de D (a saber, ζ), y se obtiene entonces que la clase de $D' - D$ es cero en $\mathrm{Pic}(X/k)$, lo que por definición implica que $D' - D \in \mathrm{Div}(X/k)$, y entonces $\exists \alpha \in \mathrm{Div}(X/k)^*$ tal que $\mathrm{div}(\alpha) = D' - D$. Luego, notamos que $\mathrm{div}(\alpha) + D = (D' - D) + D = D' \geq O$ (la última desigualdad es porque $D' \in E_\zeta$, que es efectivo por definición), y por tanto $\alpha \in H^0(D) \setminus \{0\}$ y ψ_D es sobre.

Se puede verificar que

$$k^* \times H^0(D) \setminus \{0\} \longrightarrow H^0(D) \setminus \{0\}$$

$$(c, \alpha) \mapsto c\alpha$$

es efectivamente una acción. Entonces, sea $D_0 \in E_\zeta$ y tomamos $\alpha \in \psi_D^{-1}(D_0)$. Queremos ver que $\psi_D^{-1}(D_0) = \{c\alpha \mid c \in k^*\}$. Por un lado, tenemos que, para cualquier $c \in k^*$, $\psi_{D_0}(c\alpha) = \mathrm{div}(c\alpha) + D_0 = \mathrm{div}(\alpha) + D_0 = \psi_{D_0}(\alpha)$, y entonces $c\alpha \in \psi_{D_0}^{-1}(\alpha)$. Por otro lado, si $\beta \in \psi_D^{-1}(D_0)$ entonces $D_0 = \mathrm{div}(\beta) + D = \mathrm{div}(\alpha) + D$. Se obtiene que $\mathrm{div}(\beta/\alpha) = 0$, con $\beta/\alpha \in k(X)^*$, y por el teorema 2.4.11, se obtiene $\beta/\alpha \in k^*$. Luego, $\beta = c\alpha$ para algún $c \in k^*$. Por tanto, $\psi_D^{-1}(D_0) = \{c\alpha \mid c \in k^*\}$ y entonces tenemos que cada elemento en E_ζ define una órbita en $H^0(D) \setminus \{0\}$, y se obtiene el resultado. □

Corolario 4.1.6. *Sea* $\mathbb{F}_q$ *un campo finito de cardinalidad* q*. Sea* $X/\mathbb{F}_q$ *una curva completa no singular. Supongamos que* $E_\zeta \neq \emptyset$*, y sea* $D \in E_\zeta$*. Entonces* $|E_\zeta| = \frac{q^{h^0(D)} - 1}{q - 1}$*.*

Demostración. Aplicando el lema 4.1.5 al caso $k = \mathbb{F}_q$, tenemos que $|E_\zeta|$ puede identificarse con el cociente de $H^0(D) \setminus \{0\}$ bajo la acción de $\mathbb{F}_q^*$, y notando que cada órbita $\{c \cdot \alpha | c \in \mathbb{F}_q^*\}$ tiene $q-1$ elementos, se obtiene que $|E_\zeta|$ es igual al número de elementos de $H^0(D) \setminus \{0\}$ dividido entre $q-1$. Pero por ser $H^0(D)$ de dimensión finita ($h^0(D)$) sobre k, se obtiene que su cardinalidad es $q^{h^0(D)}$, y por tanto $H^0(D) \setminus \{0\} = q^{h^0(D)} - 1$, y por lo tanto $|E_\zeta| = \frac{q^{h^0(D)}-1}{q-1}$. □

4.2. Teorema de Riemann

Sea k cualquier campo. Sea X/k una curva completa no singular. Sea $D = \sum_P a_P P \in \mathrm{Div}(X/k)$. Similarmente a $H^0(D)$, definimos, para cada P, el conjunto

$$\zeta(D)_P := \{\alpha \in k(X) | v_P(\alpha) + a_P \geq 0\}$$

Consideramos la siguiente función entre k-espacios vectoriales

$$\varphi_D : k(X) \longrightarrow \oplus_{P \in X}(k(X)/\zeta(D)_P)$$

$$f \mapsto \oplus_{P \in X}(f \bmod \zeta(D)_P)$$

Por definición, se obtiene que $\mathrm{Ker}(\varphi_D) = H^0(D)$. Sea $H^1(D) := \mathrm{Coker}(\varphi_D)$. Veremos después que $H^0(D)$ y $H^1(D)$ son k-espacios vectoriales de dimensión finita.

Consideramos dos divisores D y D' linealmente equivalentes (i.e. $D - D' \in \mathrm{Div}(X/k)$. Sea α tal que $D' = D + \mathrm{div}(\alpha)$, y tomamos el isomorfismo "multiplicar por α", $m_\alpha : k(X) \to k(X)$. Entonces se induce el siguiente diagrama conmutativo de espacios vectoriales, donde se puede verificar que las flechas verticales son isomorfismos y que el diagrama es conmutativo.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(D') & \longrightarrow & k(X) & \xrightarrow{\varphi_{D'}} & \oplus_{P \in X} k(X)/\zeta(D')_P & \longrightarrow & H^1(D') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle m_\alpha} & & \downarrow & & \downarrow{\scriptstyle \varphi_\alpha} & & \\
0 & \longrightarrow & H^0(D) & \longrightarrow & k(X) & \xrightarrow{\varphi_D} & \oplus_{P \in X} k(X)/\zeta(D)_P & \longrightarrow & H^1(D) & \longrightarrow & 0
\end{array}$$

Supongamos que $H^0(D)$ y $H^1(D)$ son de dimensión finita (de dimensiones $h^0(D)$ y $h^1(D)$, respectivamente) y tomamos un elemento $\zeta \in \mathrm{Pic}(X/k)$ (la clase de D). Como todos los divisores D, cuya clase es ζ, son linealmente equivalentes, se obtiene del diagrama que $h^0(D)$ y $h^1(D)$ son valores que no dependen de la D escogida. Así, podemos definir $h^i(\zeta) := h^i(D)$. $i = 1, 2$. De la observación 4.1.2, se tiene que $h^0(O) = 1$.

Definición 4.2.1. *Sea X/k una curva completa no singular. El entero $h^1(O)$ es el género de X, y se denota por $g = g(X)$*

Veremos que el valor $h^0(D)-h^1(D)-\deg(D)$ es una constante independiente del divisor D elegido. Asumiendo este hecho, tenemos $\forall D \in \mathrm{Div}(X/k)$ que

$$h^0(D) - h^1(D) - \deg(D) = h^0(O) - h^1(O) - \deg(O)$$

y como $\deg(O) = 0$, $h^0(O) = 1$ y $h^1(O) = g$, se tiene

$$h^0(D) = \deg + 1 - g + h^1(D)$$

Como $H^1(D)$ es un espacio vectorial, su dimensión es un entero no negativo, y entonces tenemos:

Corolario 4.2.2. *(Teorema de Riemann) Sea $D \in \mathrm{Div}(X/k)$. Entonces*

$$h^0(D) \geq \deg(D) + 1 - g$$

Observación 4.2.3. *Sea $D \in \mathrm{Div}(X/k)$. El teorema de Riemann implica que, si $\deg(D) \geq g$ entonces $h^0(D) > 0$. En particular, si $d = \deg(D) \geq g$ entonces la función $\mathrm{cl}^{\mathrm{d}} : \mathrm{Eff}^d(X/k) \to \mathrm{Pic}^d(X/k)$ (definida en gupo de clases de divisores) es suprayectiva, ya que si tomamos un elemento $r \in \mathrm{Pic}^d(X/k)$ entonces r es de la forma $r = D + \mathrm{div}(k(X)^*)$, con $\deg(D) = d \geq g$, y como entonces se tiene $h^0(D) > 0$, en particular $H^0(D)$ es no trivial. Tomando cualquier $\alpha \in H^0(D)$, con $\alpha \neq 0$, por definición se tiene $\mathrm{div}(\alpha) + D \geq O$, y escribiendo $D' = \mathrm{div}(\alpha)+D$, se obtiene que D' es efectivo, y además $\deg(D') = \deg(\mathrm{div}(\alpha)+\deg(D)) = \deg(\mathrm{div}(\alpha)) + \deg(D) = 0 + d = d$, donde la penúltima igualdad se obtuvo del teorema 2.7.7. Además, tenemos $D' - D = \mathrm{div}(\alpha) \in \mathrm{div}(k(X)^*)$, y se obtiene entonces que $D' \in \mathrm{Eff}^d(X/k)$, y que $\mathrm{cl}^d(D') = D' + \mathrm{div}(k(X)^*) = D + \mathrm{div}(k(X)^*))$, y así cl^d es suprayectivo.*

A continuación, veremos que $H^0(D)$ tiene dimensión finita. Sean D, E dos divisores con $D \geq E$. De la definición se obtiene que $H^0(D) \supseteq H^0(E)$, y similarmente que $\zeta(D)_P \supseteq \zeta(E)_P$ para cada $P \in X$. Sea π_P el generador del ideal maximal de $\mathcal{O}_P \subset k(X)$. Entonces $\zeta(D)_P = \pi_P^{-a_P}\mathcal{O}_P$ (donde $D = \sum_{P\in X} a_P P$). Para verlo, observamos que si $\alpha \in \zeta(D)_P$ entonces $v_P(\alpha) \geq -a_P$, y entonces $\exists r$ entero no negativo tal que $v_P(\alpha) = -a_P + r$, y como v_P es suprayectiva, $\exists \beta \in k(X)$ con $v_P(\beta) = r$ (y por tanto $\beta \in \mathcal{O}_P$). Además, $v_P(\pi_P) = 1$, por lo que $v_P(\pi_P^{-a_P})$, y obtenemos $v_P(\alpha) = v_P(\pi_P^{-a_P} \cdot \beta) \Rightarrow \alpha(\pi_P^{-a_P} \cdot \beta)^{-1} = l$, $l \in k$ $\Rightarrow \alpha = \pi_P^{-a_P}(\beta \cdot l)$, con $\beta \cdot l \in \mathcal{O}_P$. Recíprocamente, si $\beta \in \pi_P^{-a_P}\mathcal{O}_P$ entonces $\beta = \pi_P^{-a_P}\gamma$, $\gamma \in \mathcal{O}_P$, $\Rightarrow v_P(\beta) = v_P(\pi_P^{-a_P}) + v_P(\gamma) \geq v_P(\pi_P^{-a_P}) = -a_P$. Se tiene entonces el resultado deseado.

Lema 4.2.4. *Si $s \leq t$ entonces $\pi_{P^s}\mathcal{O}_P \supset \pi_{P^t}\mathcal{O}_P$ y el cociente $\pi_{P^s}\mathcal{O}_P/\pi_{P^t}\mathcal{O}_P$ es un k-espacio vectorial de dimensión finita, con dimensión $(t-s)\deg(P)$.*

Demostración. Como $k \subset \mathcal{O}_P$, se obtiene que $\pi_P^s\mathcal{O}_P$, $\pi_P^t\mathcal{O}_P$ y $\pi_P^s\mathcal{O}_P/\pi_P^t\mathcal{O}_P$ son k-espacios vectoriales. Consideramos las inclusiones

$$\pi_P^t \mathcal{O}_P \subset \pi_P^{t-1} \mathcal{O}_P \subset \ldots \subset \pi_P^{s+1} \mathcal{O}_P \subset \pi_P^s \mathcal{O}_P$$

En general, tenemos que si A es un dominio conmutativo, M un A-módulo, y $(0) = M_0 \subset M_1 \subset \ldots \subset M_s = M$ una cadena de A-módulos, con $\text{rank}(M_i/M_{i-1})$ finito $\forall\ i = 1, 2, \cdots s$ entonces $\text{rank}(M) = \sum_{i=1}^{s} \text{rank}(M_i/M_{i-1})$. Aplicando esto a nuestro caso, tendremos que el lema 4.2.4 se cumplirá si

$$\dim_k(\pi_P^l \mathcal{O}_P / \pi_P^{l+1} \mathcal{O}_P) = \deg(P)\ \forall\ l \in \mathbb{Z}$$

Pero, por definición, tenemos $\deg(P) = \dim_k(\mathcal{O}_P/(\pi)_P)$, así que tomamos el isomorfismo de k-espacios vectoriales $\varphi : \mathcal{O}_P \to \pi_P^l \mathcal{O}_P$, con $\alpha \mapsto \pi_P^l \alpha$, que induce de manera natural un isomorfismo $\varphi'' : \mathcal{O}_P/\pi_P \mathcal{O}_P \to \pi_P^l \mathcal{O}_P / \pi_P^{l+1} \mathcal{O}_P$. De aquí, se tiene $\dim_k(\mathcal{O}_P/\pi_P \mathcal{O}_P) = \dim_k(\pi_P^l \mathcal{O}_P / \pi_P^{l+1} \mathcal{O}_P)$, y por tanto se cumple el lema. □

Lema 4.2.5. *Si $D \geq E$ entonces* $\deg(D) - \deg(E) = \dim_k(\oplus_P \zeta(D)_P / \zeta(E)_P)$

Demostración. El lema 4.2.4 nos dice que cada k-espacio vectorial $\zeta(D)_P/\zeta(E)_P$ tiene dimensión $(a_P - b_P)\deg(P)$, con $D = \sum_P a_P P$, $E = \sum_P b_P P$. Como $a_P = b_P = 0$ para todos excepto para algunos P's, se obtiene que $\oplus_P \zeta(D)_P/\zeta(E)_P$ es un k-espacio vectorial de dimensión finita, con dimensión $\sum_P (a_P - b_P) = \deg(D) - \deg(E)$. □

Sean $D \geq E$ dos divisores. Sea $\varphi_1 : H^0(E) \to H^0(D)$ la inclusión. Sea $\varphi_2 : k(X) \to k(X)$ la función identidad. Sea

$$\varphi_3 : \oplus_P k(X)/\zeta(E)_P \to \oplus_P k(X)/\zeta(D)_P$$

la función suprayectiva obtenida como la suma directade las funciones suprayectivas $\varphi_{3,P} : k(X)/\zeta(E)_P \to k(X)/\zeta(D)_P$ inducida por la inclusión $\zeta(E)_P \to \zeta(D)_P$. Consideramos el siguiente diagrama:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(E) & \longrightarrow & k(X) & \xrightarrow{\varphi_E} & \oplus_P k(X)/\zeta(E)_P & \longrightarrow & H^1(E) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_{E,D}} & & \\
0 & \longrightarrow & H^0(D) & \longrightarrow & k(X) & \xrightarrow{\varphi_D} & \oplus_P k(X)/\zeta(D)_P & \longrightarrow & H^1(D) & \longrightarrow & 0
\end{array}$$

donde $\varphi_{E,D}$ es la función natural inducida por φ_3 entre los cokernel de φ_E y φ_D. El lema 4.2.5 muestra que el kernel de φ_3 es un espacio vectorial de dimensión finita, con dimensión $\deg(D) - \deg(E)$.

Por otro lado, notamos que el diagrama anterior induce el siguiente diagrama conmutativo con flechas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k(X)/H^0(E) & \xrightarrow{a} & \oplus_P k(X)/\zeta(E)_P & \xrightarrow{b} & H^1(E) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1'} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_{E,D}} & & \\ 0 & \longrightarrow & k(X)/H^0(D) & \xrightarrow{\alpha} & \oplus_P k(X)/\zeta(D)_P & \xrightarrow{\beta} & H^1(D) & \longrightarrow & 0 \end{array}$$

donde φ_1' es la función natural inducida, a manda un elemento $r + H^0(E)$ al elemento $\oplus_P r + \zeta(E)_P$ (análogamente se define α), y b es la función natural inducida (análogamente β es la función natural inducida). Notamos que a está bien definida, pues si $r + H^0(E) = s + H^0(E)$ entonces $r - s \in H^0(E) = \ker(\varphi_E) \Rightarrow r - s \in \zeta(E)_P \ \forall \ P$, por lo que se obtiene que $\oplus_P r + \zeta(E)_P = \oplus_P s + \zeta(E)_P$. Además, es inyectiva pues si $\oplus_P r + \zeta(E)_P = \oplus_P s + \zeta(E)_P$ entonces $r - s \in \zeta(E)_P \ \forall \ P \Rightarrow r - s \in \ker(\varphi_E) = H^0(E)$, por lo que se obtiene que $r + H^0(E) = s + H^0(E)$. Análogamente se verifica que α está bien definida y es inyectiva. Se puede verificar que el diagrama es conmutativo y con flechas exactas. Aplicando el lema de la serpiente, se obtiene en particular una sucesión exacta

$$0 \to H^0(D)/H^0(E) \to \ker(\varphi_3) \to \ker(\varphi_{E,D}) \xrightarrow{d} \operatorname{coker}(\varphi_1')$$

Tomando la función $\ker(\varphi_3) \to \ker(\varphi_{E,D})$, notamos que si un elemento de la forma $F_P := (\oplus_P f_P + \zeta(E)_P)/\mathrm{Im}(\varphi_E) \in H^1(E)$ pertenece a $\ker(\varphi_{E,D})$ entonces de las definiciones se obtiene que $\exists \ f \in k(X)$ tal que $f_P - f \in \zeta(D)_P \ \forall \ P$, y por tanto, $\oplus_P f_P + \zeta(D)_P = \oplus_P f + \zeta(D)_P$. Por otro lado, de la demostración del lema de la serpiente se obtiene que la imagen del elemento elegido F_P bajo la función d es igual al elemento $f + H^0(D) + (k(X)/H^0(D))$, pero notamos que este elemento es igual a $k(X) + H^0(D)$, es decir, la imagen del elemento F_P bajo la función d es igual al cero de $\operatorname{coker}(\varphi_1')$. Luego, por esto y por ser la sucesión una sucesión exacta, se obtiene que la función $\ker(\varphi_3) \to \ker(\varphi_{E,D})$ es suprayectiva. Por lo tanto, se obtiene la sucesión exacta siguiente:

$$0 \to H^0(D)/H^0(E) \to \ker(\varphi_3) \to \ker(\varphi_{E,D}) \to 0$$

Se obtiene de esta sucesión exacta y del lema 4.2.5 que $\mathrm{Ker}(\varphi_{E,D})$ es un espacio vectorial de dimensión finita, con dimensión

$$\dim_k \mathrm{Ker}(\varphi_{E,D}) = \deg(D) - \deg(E) - \dim_k(H^0(D)/H^0(E)) \qquad (1)$$

Lema 4.2.6. *Sea $D \in \mathrm{Div}(X/k)$ con $\deg(D) \geq 0$. Entonces $h^0(D) \leq \deg(D) + 1$. En particular, $\forall \ D \in \mathrm{Div}(X/k)$, $H^0(D)$ es un espacio vectorial de dimensión finita.*

Demostración. De la observación 4.1.3 tenemos que $\deg(D) < 0$ entonces $h^0(D) = 0$, y de la observación 4.1.4 tenemos que si $\deg(D) = 0$ entonces $h^0 \leq 1$. Sea $n \in \mathbb{N}$, y asumamos, por inducción, que el lema 4.2.6 se cumple para todos los

divisores E con $\deg(E) \leq n$. Sea D un divisor de grado $\deg(D) = n+1$. Entonces, podemos encontrar un divisor $P \in X$ tal que $D \geq D - P$, y aplicando (1), obtenemos que

$$0 \leq \deg(D) - \deg(D-P) - \dim_k(H^0(D)/H^0(D-P))$$

Pero $h^0(D-P) < \infty$, por hipótesis de inducción, y se obtiene de la desigualdad que $h^0(D) < \infty$, y además, que $h^0(D) \leq \deg(P) + h^0(D-P)$, y entonces, de nuevo de la hipótesis de inducción, se obtiene $h^0(D) \leq \deg(D) + 1$.

Asumamos ahora que $H^1(D)$ y $H^1(E)$ son espacios vectoriales de dimensión finita, con dimensiones $h^1(D)$ y $h^1(E)$, respectivamente. Como la función $\varphi_{E,D}$ es suprayectiva, obtenemos que $\dim_k(\mathrm{Ker}(\varphi_{E,D})) + h^1(D) = h^1(E)$, por lo que

$$\dim_k(\mathrm{Ker}(\varphi_{E,D})) = h^1(E) - h^1(D) \qquad (2)$$

De las fórmulas (1) y (2) se deduce que, para $D \geq E$,

$$\deg(D) - h^0(D) + h^1(D) = \deg(E) - h^0(E) + h^1(E) \qquad (3)$$

Sean, ahora, D y E dos divisores arbitrarios, y tomamos otro divisor $M \geq D, E$. Aplicando (3) a $M \geq D$ y $M \geq E$, se deduce que

$$\deg(D) - h^0(D) + h^1(D) = \deg(E) - h^0(E) + h^1(E)$$

Así, resta probar que $H^1(D)$ tiene dimensión finita y entonces habremos probado el lema. □

En la demostración del siguiente teorema daremos un esbozo. La prueba se puede encontrar en [9], teorema 3.8 de la página 313.

Teorema 4.2.7. *Sea k un campo arbitrario. Sea X/k una curva completa no singular. Entonces, dado $D \in \mathrm{Div}(X/k)$, el k-espacio vectorial $H^1(D)$ tiene dimensión finita, denotado por $h^1(D)$. Más aún, $h^0(D) = \deg(D)+1-g+h^1(D)$.*

Demostración. Basta ver que $H^1(D)$ tiene dimensión finita. Sean $D \geq E$ dos divisores como en (3). Veamos primero que $\dim_k(\mathrm{Ker}(\varphi_{E,D}))$ es acotada por una constante independiente de D y E.

Supongamos que $E = O$ y que D es un múltiplo del divisor $(\alpha)_\infty$, para algún elemento $\alpha \in k(X) \setminus k$ (donde se sabe que $\mathrm{div}(\alpha) = (\alpha)_0 - (\alpha)_\infty$). Por la observación 2.7.9 se tiene que $(\alpha)_\infty$ es un divisor efectivo de grado $n = [k(X) : k(\alpha)]$. Elegimos una base $\{\beta_1, \beta_2, \ldots, \beta_n\}$ de la extensión $k(X)/k(\alpha)$ que esté contenida en la cerradura entera de $k[\alpha]$ en $k(X)$ (Corolario 1.2.16). Como cada β_i es entero sobre $k[\alpha]$ entonces un polo P de β_i debe ser también un polo de α, esto es, si P es tal que $\beta_i \notin \mathcal{O}_P$ entonces $\alpha \notin \mathcal{O}_P$, lo cual ocurre ya que si $\alpha \in \mathcal{O}_P$ entonces $\mathcal{O}_P$ contiene a la cerradura entera de $k[\alpha]$ en $k(X)$ ($\mathcal{O}_P$ es enteramente cerrado en su campo de fracciones $k(X)$), y por tanto $\beta_i \in \mathcal{O}_P$.

Se puede verificar que existe un entero positivo m que cumpla que $\beta_1, \ldots, \beta_n \in H^0(m(\alpha)_\infty)$, es decir, que para algún entero positivo m se cumple que

$$\operatorname{div}(\beta_i) = \sum_P v_P(\beta_i)P \geq m \sum_{\{P \in X | \pi(P) = \infty\}} v_P(\alpha)P = -m(\alpha)_\infty$$

para cada $i = 1, 2, \ldots, n$.

Ahora, sea $s \in \mathbb{N}$. Consideramos el siguiente conjunto de $n(s+1)$ elementos

$$S := \{\alpha^i \beta_j \, , 0 \leq i \leq s, \; 1 \leq j \leq n\}$$

Como $\beta_1, \ldots, \beta_n$ son linealmente independientes sobre $k[\alpha]$, el conjunto S es linealmente independiente sobre k, y además, tenemos que $S \subseteq H^0((m+s)(\alpha)_\infty)$. Como $S \subseteq H^0((m+s)(\alpha)_\infty)$ entonces obtenemos que $\forall \; \mu \geq m$, $\mu = m + s$, se cumple

$$h^0(\mu(\alpha)_\infty) \geq n(\mu - m + 1) \tag{4}$$

Sea $D := \mu(\alpha)_\infty$, y $E := O$. De (4) y (1) obtenemos

$$\begin{aligned} \dim_k(\operatorname{Ker}(\varphi_{E,D})) &= \deg(D) - 0 - h^0(D) + 1 \qquad (5) \\ &\leq \mu n - n(\mu - m + 1) + 1 \\ &= nm - n + 1 \end{aligned}$$

De esto último, se deduce que la dimensión de $\operatorname{Ker}(\varphi_{E,D})$ está acotada por la constante $c := nm - n + 1$, independiente de μ. Además, de (5) se deduce que

$$\deg(\mu(\alpha)_\infty) - h^0(\mu(\alpha)_\infty) \leq c \tag{6}$$

Sea $D \in \operatorname{Div}(X/k)$ un divisor arbitrario. Por la observación 2.5.3 se tiene que si $\pi : X \to \mathbb{P}^1$ es el morfismo de curvas inducido por la inclusión $k(\alpha) \to k(X)$ entonces $\{P \in X | \pi(P) = \infty\} = \{P \in X | \alpha \notin \mathcal{O}_P\}$, es decir, es igual al conjunto de polos de α (que es un conjunto finito).

Por definición, tenemos que $(\alpha)_\infty = - \sum_{\{P \in X | \pi(P) = \infty\}} v_P(\alpha)P$, es decir,

$$(\alpha)_\infty = - \sum_{\{P \in X | P \text{ polo de } \alpha\}} v_P(\alpha)P$$

Tomamos una "restricción" de $D = \sum_P a_P P$, a saber

$$D_1 := \sum_{\{P \in X | P \text{ polo de } \alpha\}} a_P P$$

Luego, tomamos $D_2 := D - D_1$. Esto significa que

$$D_2 := \sum_{\{P \in X | P \text{ no polo de } \alpha\}} a_P P$$

Y en particular, si tomamos un coeficiente $a_P \neq 0$ de D_2 entonces para el P asociado a dicho a_P se obtiene $v_P(\alpha) \geq 0$. Para cada $a_P \neq 0$ coeficiente de D_2, sea $g_P(x) \in k[x]$ el polinomio mínimo sobre k de la imagen de α en $\mathcal{O}_P/\mathcal{M}_P$. Escribiendo $g_P(x) = \sum a_i x^i$, con $a_i \in k$, y evaluando el elemento $\alpha + \mathcal{M}_P$ en este polinomio, se obtiene la expresión $\sum a_i \alpha^i + \mathcal{M}_P = \mathcal{M}_P$ (la última igualdad es porque $g_P(x)$ es el polinomio mínimo de $\alpha + \mathcal{M}_P$ sobre k), y si escribimos $g_P(\alpha) := \sum a_i \alpha^i$, se obtiene entonces que el elemento $g_P(\alpha) \in k(X)$ cumple que $g_P(\alpha) \in \mathcal{M}_P$, es decir, $v_P(g_P(\alpha)) > 0$, y esto para cada P tal que $a_P \neq 0$ es coeficiente de D_2.

Sea a un entero positivo. Tomamos

$$z_a := \prod_{\{P \in X | a_P \neq 0 \text{ coeficiente de } D_2\}} g_P(\alpha)^a$$

Entonces $z_a \in k(X)$. Se puede notar que elemento z_a es tal que $v_P(z_a) > 0$ para cada P tal que el coeficiente de D_2 en el punto P no es cero, y además que los polos de z_a están contenidos únicamente en los polos de α. Usando esto, se puede verificar que, para μ y α suficientemente grandes, se tiene $D \leq \mu(\alpha)_\infty + \operatorname{div}(z_a)$. Tenemos entonces que $D - \operatorname{div}(z_a) \leq \mu(\alpha)_\infty$ y por tanto $h^0(D - \operatorname{div}(z_a)) \leq h^0(\mu(\alpha_\infty))$, pero sabemos que $h^0(D - \operatorname{div}(z_a)) = h^0(D)$, y entonces $h^0(D) \leq h^0(\mu(\alpha_\infty))$, y esto para todo $D \in \operatorname{Div}(X/k)$

Por tanto, aplicando esto junto con la igualdad (1) se obtiene que

$$0 \leq \deg(\mu(\alpha)_\infty) - h^0(\mu(\alpha)_\infty) - (\deg(D) - h^0(D)) < \infty \tag{7}$$

Se obtiene de (6) y de (7) que, $\forall\ D \in \operatorname{Div}(X/k)$,

$$\deg(D) - h^0(D) \leq c \tag{8}$$

Ahora, sean $D, E \in \operatorname{Div}(X/k)$ cualesquiera divisores con $D \geq E$. Sea $\varphi_{E,D} : H^1(E) \to H^1(D)$. La igualdad (1) y la desigualdad (8) implican que

$$\dim_k(\operatorname{Ker}(\varphi_{E,D})) \leq 2c \tag{9}$$

Queremos ahora probar que $H^1(E)$ es un espacio vectorial de dimensión finita. Supongamos por contradicción que $H^1(E)$ no tiene dimensión finita. Entonces existe una sucesión infinita $\{e_i\}_{i \in \mathbb{N}}$ de elementos linealmente independientes de $H^1(E)$. Queremos ver que existe una cadena infinita de divisores $D \leq D_1 \leq \cdots \leq D_n \leq \ldots$ tal que $\varphi_{E,D_n}(e_i) = 0\ \forall i = 1, \ldots, n$, ya que esto implicaría que $\dim_k(\operatorname{Ker}(\varphi_{E,D_n})) \geq n\ \forall n \in \mathbb{N}$, contradiciendo (9).

Podemos construir dicha cadena infinita por inducción: para todo $i \in \mathbb{N}$, sea $f_i \in \oplus_P k(X)/\zeta(E)_P$ tal que su imagen en $H^1(E)$ es e_i (notamos que dicha f_i existe, por definición de $H^1(E)$). Entonces f_i es de la forma $(\ldots, f_{iP}, \ldots)$, con $f_{iP} \in k(X)/\zeta(E)_P$ (en particular, $f_i = f_i' + \zeta(E)_P$, para algún $f_i' \in k(X)$), y sean $P_1, \ldots, P_s$ todos los puntos tales que f_{iP} no es cero. Sea $D = \sum_P a_P P$. Notamos que entonces podemos encontrar un divisor $D_1 \geq D \geq E$

tal que, $\forall\ j = 1, \ldots, s$, el elemento f_{iP_j} está en el kernel de la función natural $k(X)/\zeta(E)_{P_j} \to k(X)/\zeta(D_1)_{P_j}$ (es decir, necesitamos un divisor $D_1 = \sum_p b_P P$ tal que $v_{P_j}(f'_{iP_j}) + b_{P_j} \geq 0$ para cada $j = 1, \ldots, s$, donde $f_{iP_j} = f'_{iP_j} + \zeta(E)_{P_j}$. y si $k \notin \{1, \ldots, s\}$ entonces tal que $b_{P_k} \geq 0$; y además tal que $b_P \geq a_P\ \forall\ P$, y en particular podríamos tomar D_1 tal que $b_P = 0$ si $P \notin \{P_1, \ldots, P_s\} \bigcup \{P | a_P \neq 0\}$, y si $P \in \{P_1, \ldots, P_s\} \bigcup \{P | a_P \neq 0\}$ entonces tomar $b_P = \max\{-v_{P_1}(f'_{iP_1}), \ldots, -v_{P_s}(f'_{iP_s}), \{a_P | a_P \text{ coeficiente de } D\}, 0\})$, y por tanto, de la definición de la función natural $\varphi_{R,S}$ para cualesquiera dos divisores $R \leq S$, se obtiene que $\varphi_{E,D_1}(e_i) = 0$. En particular, elegimos $i = 1$ y obtenemos que $\varphi_{E,D_1}(e_1) = 0$. Observamos que el divisor D_1 está determinado completamente por el e_i elegido (es decir, notamos que el divisor D_1 no necesariamente cumple que $\varphi_{E,D_1}(e_j) = 0$ si $j \neq i$). Entonces, supongamos inductivamente que ya hemos construido el divisor D_n tal que $\varphi_{E,D_n}(e_i) = 0\ \forall\ i = 1, \ldots, n$. Ahora, tomamos el elemento e_{n+1}, y nuevamente, sean $P_1, \ldots, P_s$ los puntos donde el f_{n+1,P_j} no es cero, con $j = 1 \ldots, s$, y queremos encontrar un divisor D_{n+1} tal que $D_{n+1} \geq D_n \geq E$, y tal que, $\forall\ j = 1, \ldots, s$, el elemento f_{n+1,P_j} está en el kernel de la función natural $k(X)/\zeta(E)_{P_j} \to k(X)/\zeta(D_{n+1})_{P_j}$. Repitiendo un proceso análogo a lo hecho para E, D, D_1 pero ahora para el caso E, D_n, D_{n+1}, se obtiene un divisor D_{n+1} que cumple que $\varphi_{E,D_{n+1}}(e_{n+1}) = 0$. Pero también notamos que, por hipótesis de inducción, se tiene que $\varphi_{E,D_n}(e_i) = 0$ $\forall\ i = 1, \ldots, n$, y también como tenemos $D_n \leq D_{n+1}$, se obtiene de la definición de $\varphi_{R,S}$ para cualesquiera dos divisores $R \leq S$ que $\varphi_{E,D_{n+1}}(e_i) = (\varphi_{D_n,D_{n+1}} \circ \varphi_{E,D_n})(e_i) = \varphi_{D_n,D_{n+1}}(\varphi_{E,D_n}(e_i)) = \varphi_{D_n,D_{n+1}}(0) = 0$ para $i = 1, \ldots, n$, y por tanto $\varphi_{E,D_{n+1}}(e_i) = 0\ \forall\ i = 1, \ldots, n+1$, y se cumple lo que buscábamos. $\square$

Teorema 4.2.8. *(Riemann-Roch) Sea k cualquier campo. Sea X/k una curva completa no singular. Entonces existe un divisor K en* $\mathrm{Div}(X/k)$ *tal que, $\forall\ D \in \mathrm{Div}(X/k)$, el k-espacio vectorial $H^1(D)^\vee = \mathrm{Hom}_k(H, k)$ es isomorfo al espacio $H^0(K - D)$. En particular, $h^1(D) = h^0(K - D)$ y*

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D)$$

Antes de ver la prueba, podemos ver algunas consecuencias del teorema anterior.

Para algún K como en el teorema, se obtiene del mismo que

$$h^1(O) = h^0(K - O) = g,$$

$$h^1(K) = h^0(K - K) = 1,$$

$$\deg(K) = h^0(K) - 1 + g - h^1(K) = 2g - 2$$

Además, tenemos el siguiente corolario

Corolario 4.2.9. *Sea k cualquier campo. Sea X/k una curva completa no singular. Sea $\zeta \in \mathrm{Pic}(X/k)$. Si $\deg(\zeta) \geq 2g - 1$ entonces $h^0(\zeta) = \deg \zeta + 1 - g$.*

Demostración. Sea D un divisor cuya clase en $\mathrm{Pic}(X/k)$ es ζ. Como $\deg(D) \geq 2g-1 > 2g-2 = \deg(K)$, se tiene que $\deg(K-D) < 0$, y por tanto, $h^0(K-D) = 0$, y se obtiene el corolario. □

Corolario 4.2.10. *Si* $g-1 \leq \deg(D) \leq 2g-2$ *entonces* $h^0(D) \leq g$.

Demostración. Si $g-1 \leq \deg(D) \leq 2g-2 = \deg(K)$ entonces obtenemos $0 \leq \deg(K-D) \leq g-1$, y cuando $\deg(K-D) \geq 0$, el lema 4.2.6 y lo anterior nos asegura que $h^0(K-D) \leq \deg(K-D)+1 \leq g$, y por Riemann-Roch se obtiene $h^0(D) = \deg(D)+1-g+h^0(K-D) \leq g$. □

Para demostrar el teorema de Riemann-Roch, definimos lo siguiente:

Para dos divisores $D = \sum_P a_P P$ y $E = \sum_P b_P P$, definimos $\mathrm{Inf}(D,E) := \sum_P \min(a_P, b_P)P$, y $\mathrm{Sup}(D,E) := \sum_P \max(a_P, b_P)P$.

Consideramos, para dos divisores $D \geq E$, la función $\varphi_{E,D} : H^1(E) \to H^1(D)$, y para $\alpha \in k(X)^*$ y $D \in \mathrm{Div}(X/k)$ el isomorfismo $\varphi_\alpha : H^1(D + \mathrm{div}(\alpha)) \to H^1(D)$, ambos vistos anteriormente. Sea $\lambda : H^1(D) \to k$ un elemento de $H^1(D)^\vee$. Si $D \geq E$ y $\alpha \in k(X)^*$ entonces λ define dos nuevos homomorfismos:

$\lambda \circ \varphi_{E,D} : H^1(E) \to k$ y

$\lambda \circ \varphi_\alpha : H^1(D + \mathrm{div}(\alpha)) \to k$

Así, podemos definir un $k(X)$-espacio vectorial J como sigue:

$$J := \Big(\bigsqcup_{D \in \mathrm{Div}(X/k)} H^1(D)^\vee \Big) / \sim$$

donde $\sim$ denota la siguiente relación de equivalencia: sean $\lambda_1 \in H^1(D_1)^\vee$ y $\lambda_2 \in H^1(D_2)^\vee$ entonces $\lambda_1 \sim \lambda_2$ si existe $C \in \mathrm{Div}(X/k)$ con $D_1 \geq C, D_2 \geq C$, y con $\lambda_1 \circ \varphi_{C,D_1} = \lambda_2 \circ \varphi_{C,D_2}$. Para probar que J tiene estructura de grupo, notamos lo siguiente. Dados dos elementos j_1, j_2 en J, existe un solo divisor D y dos homomorfismos $\lambda_1, \lambda_2 \in H^1(D)^\vee$ tales que j_1 y j_2 son las clases de equivalencia de λ_1 y λ_2, respectivamente. Para verlo, tomamos $\lambda_1' \in H^1(D_1)^\vee$ y $\lambda_2' \in H^1(D_2)$ representantes de j_1 y j_2. Sea $D := \mathrm{Inf}(D_1, D_2)$ (entonces $D \leq D_1$ y $D \leq D_2$). De aquí, tomando $\lambda_1 := \lambda_1' \circ \varphi_{D,D_1}$ y $\lambda_2 := \lambda_2' \circ \varphi_{D,D_2}$ se obtiene que tambin son representantes de j_1 y j_2.

Así, podemos definir una suma $+ : J \times J \to J$ como sigue: dados $j_1, j_2 \in J$, tomamos D un divisor, de manera que existan $\lambda_1, \lambda_2 \in H^1(D)^\vee$ representantes de las clases de equivalencias j_1 y j_2, respectivamente. Entonces, definimos la suma $j_1 + j_2$ como la clase de equivalencia de $\lambda_1 + \lambda_2 : H^1(D) \to k$, definimos 0_J como la clase del homomorfismo cero. Se puede verificar que J es entonces, un grupo.

Además, definimos una multiplicación por escalares $k(X) \times J \to J$. Definimos $0 \cdot j = 0_J$, $\forall\ j \in J$, y si $\alpha \in k(X)^*$ y $j \in J$, y $\lambda \in H^1(D)^\vee$ un representante de j entonces definimos a αj como la clase de equivalencia de $\lambda \circ \varphi_\alpha : H^1(D + \mathrm{div}(\alpha)) \to k$.

Se puede verificar que, con lo anterior, J es un $k(X)$-espacio vectorial.

Teorema 4.2.11. *J es un $k(X)$-espacio vectorial de dimensión 1.*

Demostración. Sean j y j' dos elementos, distintos de cero, en J. Sea $D \in \mathrm{Div}(X/k)$, y sean $\lambda, \lambda' \in H^1(D)^\vee$ representantes de j_1 y j_2, respectivamente. Sea E cualquier divisor efectivo de grado grande, con $h^0(E) \neq 0$. Sea $\alpha_1, \alpha_2, \ldots, \alpha_n$ una base para $H^0(E)$. Como $\mathrm{div}(\alpha_i) \geq -E$ (), se tiene

$$D + \mathrm{div}(\alpha_i) \geq D - E, \; \forall \; i = 1, 2, \ldots, n$$

y por tanto, se obtiene que los elementos $\alpha_i j$ y $\alpha_i j'$ tienen, para todo $i = 1, \ldots, n$, a las siguentes funciones lineales como representantes

$$\alpha_i \lambda := \lambda \circ \varphi_{\alpha_i} \circ \varphi_{D-E, D+\mathrm{div}(\alpha_i)} : H^1(D-E) \to k, \quad \text{y}$$

$$\alpha_i \lambda' := \lambda' \circ \varphi_{\alpha_i} \circ \varphi_{D-E, D+\mathrm{div}(\alpha_i)} : H^1(D-E) \to k$$

Supongamos que j y j' son linealmente independientes sobre $k(X)$ (se tendría entonces $h^1(D) \geq 2$). Entonces $S := \{\alpha_1\lambda, \alpha_2\lambda, \ldots, \alpha_n\lambda, \alpha_1\lambda', \alpha_2\lambda', \ldots, \alpha_n\lambda'\}$ es un conjunto de homomorfismos linealmente independiente sobre k. Para verlo, si hubiera $c_1, c_2, \ldots, c_n$ y $d_1, d_2, \ldots, d_n$ en k, con

$$\sum_{i=1}^{n} c_i \alpha_i \lambda + \sum_{i=1}^{n} d_i \alpha_i \lambda' = 0$$

entonces $(\sum_{i=1}^{n} c_i \alpha_i) j + (\sum_{i=1}^{n} d_i \alpha_i) j' = 0_J$. Como j y j' son linealmente independientes, se obtiene que $(\sum_{i=1}^{n} c_i \alpha_i) = (\sum_{i=1}^{n} d_i \alpha_i) = 0$ en $k(X)$, y como $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $H^0(E)$,$c_i = d_i = 0$, $\forall \; i = 1, 2, \ldots, n$. Así, los elementos de S son linealmente independientes, y $h^1(D-E) \geq 2h^0(E)$. Por el teorema de Riemann, sabemos que

$$\begin{aligned} h^0(D-E) - \deg(D) - 1 + g &= -\deg(E) + h^1(D-E) \\ &\geq -\deg(E) + 2h^0(E) \\ &= \deg(E) + 2 - 2g + 2h^1(E) \\ &\geq \deg(E) + 2 - 2g \\ \Rightarrow h^0(D-E) - \deg(D) - 1 + g &\geq \deg(E) + 2 - 2g \end{aligned} \tag{10}$$

Como $h^0(E) \neq 0$ para cualquier E de grado suficientemente grande, podemos elegir una cadena infinita $D \leq E_1 \leq E_2 \leq \ldots$ tal que $h^0(E_i) \neq 0$ y $\deg(E_i) < \deg(E_{i+1})$, $\forall i \geq 1$. Como, por hipótesis, tenemos que $D \leq E_i$, se obtiene $h^0(D - E_i) = 0$, y aplicando (10) a cada E_i, se tiene

$$-\deg(D) - 3 + 3g \geq \deg(E_i), \; \forall \; i \in \mathbb{N} \tag{11}$$

Pero (11) contradice el hecho de que la sucesión $\deg(E_i)$ tiende a ∞. Por tanto, j y j' son linealmente dependientes. □

Lema 4.2.12. *Sean $C, D, D' \in \mathrm{Div}(X/k)$ tales que $C \leq D, D'$. Sean $\lambda : H^1(D) \to \bar{k}$, $\lambda' : H^1(D') \to \bar{k}$ tales que $\lambda \circ \varphi_{C,D} = \lambda' \circ \varphi_{C,D'}$. Sea $I = \mathrm{Inf}(D, D')$. Entonces $\lambda \circ \varphi_{I,D} = \lambda' \circ \varphi_{I,D'}$.*

Demostración. De la definición de I se obtiene que $C \leq I$, y por tanto se tiene $\varphi_{C,D} = \varphi_{I,D} \circ \varphi_{C,I}$ y $\varphi_{C,D'} = \varphi_{I,D'} \circ \varphi_{C,I}$, y esto implica $\lambda' \circ \varphi_{I,D'} \circ \varphi_{C,I} = \lambda' \circ \varphi_{C,D'} = \lambda \circ \varphi_{C,D} = \lambda \circ \varphi_{I,D} \circ \varphi_{C,I}$, $\Longrightarrow \lambda' \circ \varphi_{I,D'} \circ \varphi_{C,I} = \lambda \circ \varphi_{I,D} \circ \varphi_{C,I}$, y como por definición se tiene que $\varphi_{C,I}$ es suprayectiva, se obtiene que $\lambda' \circ \varphi_{I,D'} = \lambda \circ \varphi_{I,D}$ □

Lema 4.2.13. *Sean $D, D' \in \mathrm{Div}(X/k)$, y sean $I = \mathrm{Inf}(D, D')$, $S = \mathrm{Sup}(D, D')$. Entonces, $\forall\ \lambda \in H^1(D)^\vee, \lambda' \in H^1(D')^\vee$ tales que $\lambda \circ \varphi_{I,D} = \lambda' \circ \varphi_{I,D'}$ entonces $\exists\ \lambda'_0 \in H^1(S)^\vee$ tal que $\lambda = \lambda'_0 \circ \varphi_{D,S}$ y $\lambda' = \lambda'_0 \circ \varphi_{D',S}$.*

Demostración. Sean λ,λ' que cumplan las hipótesis del lema. Sea $y \in H^1(S)$. Entonces y es de la forma $y = \frac{(\ldots, f_{iP}, \ldots)}{\mathrm{Im}(\varphi_S)}$, donde $f_{iP} = f'_{iP} + \zeta(S)_P$, $f'_{iP} \in k(X)$, y notamos que que el elemento $x = \frac{(\ldots, f'_{iP} + \zeta(I)_P, \ldots)}{\mathrm{Im}(\varphi_I)} \in H^1(I)$ cumple que $\varphi_{I,S}(x) = y$, y definimos $\lambda'_0(y) := (\lambda \circ \varphi_{I,D})(x) = (\lambda' \circ \varphi_{I,D'})(x)$. Podemos verificar que está bien definida y que por definición de λ'_0 y por ser $\lambda \circ \varphi_{I,D} \in H^1(I)^\vee$ (y $\lambda' \circ \varphi_{I,D'} \in H^1(I)^\vee$), se obtiene que $\lambda'_0 \in H^1(S)^\vee$. Además, si $s = \frac{(\ldots, s'_{iP} + \zeta(D)_P, \ldots)}{\mathrm{Im}(\varphi_D)} \in H^1(D)$ entonces el elemento $r = \frac{(\ldots, s'_{iP} + \zeta(I)_P, \ldots)}{\mathrm{Im}(\varphi_I)} \in H^1(I)$ cumple que $\varphi_{I,D}(r) = s$, y que $\varphi_{D,S}(s) = (\varphi_{D,S} \circ \varphi_{I,D})(r) = \varphi_{I,S}(r)$. Tenemos entonces que $(\lambda'_0 \circ \varphi_{D,S})(s) = \lambda'_0(\varphi_{D,S}(s)) := (\lambda \circ \varphi_{I,D})(r) = \lambda(s)$, y se obtiene que $\lambda'_0 \circ \varphi_{D,S} = \lambda$. Análogamente, se puede ver que $\lambda'_0 \circ \varphi_{D',S} = \lambda'$. □

Teorema 4.2.14. *Sea k un campo arbitrario. Sea X/k una curva completa no singular. Sea $j \in J$, $j \neq 0_J$. Entonces existe un divisor $K(j) \in \mathrm{Div}(X/k)$ tal que:*

i) j puede ser representado por un homomorfismo $\lambda : H^1(K(j)) \to k$, y

ii) $K(j)$ es maximal con esta propiedad: si $E \geq K(j)$ es cualquier divisor tal que j puede ser representado por $\lambda' : H^1(E) \to k$ entonces $E = K(j)$

Más aún, $\forall\ \alpha \in k(X)^*$, $K(\alpha j) = K(j) + \mathrm{div}(\alpha)$. En particular, la clase de $K(j)$ en $\mathrm{Pic}(X/k)$ es independiente de $j \in J \setminus \{0_J\}$.

Demostración. Sea $j \in J$,$j \neq 0_J$, y sea $\lambda : H^1(D) \to k$ un representante de j. Entonces $\deg(D) \leq 2g + 1$. Para verlo, notamos primero que del teorema de Riemann, tenemos $\deg(D) \leq H^0(D) + g - 1$. Queremos ver que $h^0(D) \leq g$. Si $h^0(D) \neq 0$, sea $\alpha_1, \alpha_2, \ldots . \alpha_n$ una base para $H^0(D)$ sobre k. Como $\mathrm{div}(\alpha_i) + D \geq$

O entonces el elemento $\alpha_i j$, en J, está representado por una función lineal $\alpha_i\lambda : H^1(O) \to k$ (con $\alpha_i\lambda := \varphi_{O,D+\mathrm{div}(\alpha_i)} \circ \varphi_{\alpha_i} \circ \lambda$). Asumiendo que existen $c_1, c_2, \ldots, c_n$ en k, tales que $\sum_{i=1}^{n} c_i\alpha_i\lambda = 0$, se obtiene que $\sum_{i=1}^{n}(c_i\alpha_i)\lambda = 0_J$ en J, y como J es un $k(X)$-espacio vectorial de dimensión 1, se obtiene que $\sum_{i=1}^{n}(c_i\alpha_i) = 0$, y como $\alpha_1, \ldots, \alpha_n$ son linealmente independientes sobre k por hipótesis, se tiene que $c_1 = \ldots = c_n = 0$, y por tanto $H^1(O)^\vee$ tiene dimensión, al menos, n, es decir, tiene dimensión al menos $h^0(D)$, y como la dimensión del dual de un espacio vectorial es igual a la dimensión del espacio vectorial (cuando tiene dimensión finita), se obtiene que $H^1(O)$ tiene dimensión, al menos, igual a $h^0(D)$, y por definición entonces $g \geq h^0(D)$. Ahora, sea D un divisor cuyo grado es maximal de entre todos los divisores E, tal que j puede ser representado por un homomorfismo $H^1(E) \to k$. Entonces $D \geq E$. Para verlo, sean $\lambda : H^1(D) \to k$ y $\lambda' : H^1(E) \to k$ dos representantes de j. Consideramos el siguiente diagrama

$$\begin{array}{ccc} H^1(\mathrm{Inf}(D,E)) & \xrightarrow{\psi'} & H^1(E) \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi'} \\ H^1(D) & \xrightarrow{\varphi} & H^1(\mathrm{Sup}(D,E)) \end{array}$$

Como λ y λ' representan a j, $\exists\ F \in \mathrm{Div}(X/k)$ tal que $F \leq D, E$, con $\lambda \circ \varphi_{F,D} = \lambda' \circ \varphi_{F,E}$. Por el lema 4.2.12 se tiene entonces que $\lambda \circ \psi = \lambda' \circ \psi'$, y por el lema 4.2.13 existe un único homomorfismo $\lambda'' : H^1(\mathrm{Sup}(D,E)) \to k$ tal que $\lambda = \lambda'' \circ \varphi$ y $\lambda = \lambda'' \circ \varphi'$. Como $\deg(D)$ es maximal por hipótesis, se obtiene que $\deg(\mathrm{Sup}(D,E)) \leq \deg(D)$, y de aquí, se obtiene que $E \leq \mathrm{Sup}(D,E) \leq D$.

Por último, hay que ver que, $\forall\ \alpha \in k(X)^*$, se tiene $K(\alpha j) = K(j) + \mathrm{div}(\alpha)$. De las definiciones, se obtiene que $K(j) + \mathrm{div}(\alpha)$ es tal que existe un elemento en $H^1(K(j) + \mathrm{div}(\alpha))^\vee$ que es representante de αj, y como $K(\alpha j)$ es maximal con esta propiedad, se obtiene que $K(j) + \mathrm{div}(\alpha) \leq K(\alpha j)$. Análogamente, de las definiciones se obtiene que $K(\alpha j) - \mathrm{div}(\alpha)$ es tal que existe un elemento en $H^1(K(\alpha j) - \mathrm{div}(\alpha))^\vee$ que es representante de j, y como $K(j)$ es maximal con esta propiedad, se tiene que $K(\alpha j) - \mathrm{div}(\alpha) \leq K(j)$, i.e., $K(\alpha j) \leq K(j) + \mathrm{div}(\alpha)$. Se tiene entonces la igualdad $K(\alpha j) = K(j) + \mathrm{div}(\alpha)$.

Y como J es de dimensión 1 sobre $k(X)$, del párrafo anterior se obtiene que, $\forall\ j, j' \in J \setminus \{0_J\}$, la clase de $K(j)$ y $K(j')$ son iguales en $\mathrm{Pic}(X/k)$. □

Ahora, podemos ver la prueba del teorema de Riemann-Roch.

Demostración. Sea $D \in \mathrm{Div}(X/k)$. Sea $j \in J \setminus \{0_J\}$, y sea $K := K(j)$. Veamos que la siguiente función es un isomorfismo

$$\delta : H^0(D) \to \mathrm{Hom}_k(H^1(K - D), H^1(K))$$

$$\alpha \mapsto \varphi_\alpha \circ \varphi_{K-D,K+\mathrm{div}(\alpha)}, \text{ si } \alpha \neq 0$$
$$0 \mapsto \text{el homomorfismo cero}$$

Notamos que, si $\alpha \neq 0$ entonces $\mathrm{div}(\alpha) \geq -D$, por lo que $K + \mathrm{div}(\alpha) \geq K - D$. Así, las funciones

$$H^1(K-D) \overset{\varphi_{K-D,K+\mathrm{div}(\alpha)}}{\longrightarrow} H^1(K+\mathrm{div}(\alpha)) \overset{\varphi_\alpha}{\longrightarrow} H^1(K)$$

están bien definidas.

Se puede verificar que δ es un homomorfismo de k-espacios vectoriales.

Sea $\lambda : H^1(K) \to k$ un representante de la clase j. Veamos que δ es inyectiva. Supongamos que $\delta(\alpha) = 0$, $\alpha \neq 0$. Entonces, debe ocurrir que $\lambda \circ \varphi_\alpha \circ \varphi_{K-D,K+\mathrm{div}(\alpha)} = 0$. Por lo tanto, la clase αj de $\lambda \circ \varphi_\alpha$ en J debe ser la clase 0_J, y entonces debe tenerse que $\alpha = 0$ (J es un $k(X)$-espacio vectorial), que es una contradicción. Así, δ es inyectiva. Para ver que es suprayectiva, sea $\psi \in \mathrm{Hom}_k(H^1(K-D), H^1(K))$. Entonces $\lambda \circ \psi \in H^1((K-D))^\vee$, y por tanto, la clase de $\lambda \circ \psi$ en J es igual a αj, para algún $\alpha \in k(X)^*$ (pues J es un espacio vectorial de dimensión 1 sobre k, y en particular la clase j de λ puede tomarse como base J). Como $K(\alpha j) = K + \mathrm{div}(\alpha)$ es un divisor maximal de entre los divisores E con la propiedad de que αj puede ser representado por un homomorfismo $H^1(E) \to k$, se debe tener $K - D \leq K + \mathrm{div}(\alpha)$, y de esto último se obtiene que $\alpha \in H^0(D)$, y

$$\lambda \circ \psi = \lambda \circ \varphi_\alpha \circ \varphi_{K-D,K+\mathrm{div}(\alpha)}$$

Luego, $\psi = \delta(\alpha)$ y δ es suprayectiva.

Lo anterior podemos aplicarlo al caso $D = O$. Tenemos entonces

$$H^1(O) \overset{\sim}{\longrightarrow} \mathrm{Hom}_k(H^1(K-O), H^1(K))$$

Como $h^0(O) = 1$, se concluye que $h^1(K) = 1$. Para ver esto, notamos que por ser $H^0(O)$ y $\mathrm{Hom}_k(H^1(K), H^1(K))$ isomorfos y como la dimensión de $H^0(O)$ es 1 entonces $\mathrm{Hom}_k(H^1(K), H^1(K))$ tiene dimensión 1, y podemos tomar a la identidad $\{\mathrm{Id}\}$ como base para $\mathrm{Hom}_k(H^1(K), H^1(K))$ sobre k. Sea $\{\lambda_1, \ldots, \lambda_n\}$ una base para $H^1(D)$. Entonces, para cualquier $g \in \mathrm{Hom}_k(H^1(K), H^1(K))$ se tiene, por un lado, que $g(\lambda_i) = \sum_i a_i \lambda_i$ para algunos $a_i \in k$, y por otro lado se tiene que $g(\lambda_i) = \alpha \mathrm{Id}(\lambda_i) = \alpha \lambda_i$ para alguna $\alpha \in k^*$, y en ambos casos para cada i. Se tiene por tanto $\alpha \lambda_i = \sum_i a_i \lambda_i$ y de la independencia lineal de los λ_i se obtiene $\alpha - a_i = 0$, y esto para cada a_i. Luego, se obtiene que $\lambda_i = \sum_i \lambda_i$ para cada i, y como cada elemento λ_i de la base es combinación lineal de la misma base y esto no puede ser posible si $n > 1$, se obtiene que $n = 1$, y por tanto $\mathrm{Hom}(H^1(K))$ tiene dimensión 1.

Usando la base correspondiente de $H^1(K)$, $\lambda : H^1(K) \to k$ (la dimensión de $H^1(K)^\vee$ es igual a la dimensión de $H^1(K)$), podemos identificar $\mathrm{Hom}_k(H^1(K-D), H^1(K))$ con $H^1(K-D)^\vee$ (pues notamos que $\mathrm{Hom}_k(H^1(K-D), H^1(K))$ tendría dimensión 1 también, por lo que $\mathrm{Hom}_k(H^1(K-D), H^1(K)) = \{\alpha\psi_0 | \alpha \in k\}$, para algún $\psi_0 \in \mathrm{Hom}_k(H^1(K-D), H^1(K))$, y además tenemos $H^1(K)^\vee = \{\alpha\lambda | \alpha \in k\}$, y utilizando estos dos hechos, junto con la linealidad de ψ_0 y de λ,

se obtiene la identificación mencionada). Sustituyendo $D = K - E$, encontramos que $H^1(E)^\vee$ es isomorfo a $H^0(K - E)$, y esto para cada $E \in \mathrm{Div}(X/k)$. Así, se obtiene el resultado. $\square$

5. Capítulo V - Extensiones inseparables y resultados extras necesarios

En este capítulo revisamos algunos resultados que se utilizan principalmente en el capítulo 2 aunque también se usan en los capítulos 3 y 4.

5.1. Extensiones inseparables

En esta sección se revisan algunos resultados que son útiles en los capítulos anteriores. En particular, la proposición 5.1.4 y el corolario 5.1.7 se utilizan con frecuencia durante todo el trabajo, mientras que el resto de los resultados de esta sección se enuncian para complementar los dos resultados mencionados. Las demostraciones se omiten, pero se pueden encontrar en [9] (capítulo 10, sección 1).

Sea R cualquier anillo de característica $p > 0$. La función $\text{Frob}_R : R \to R$, que manda r a r^p, es un homomorfismo de anillos llamado el morfismo de Frobenius absoluto de R (notamos que si $r, s \in R$ entonces $(r+s)^p = r^p + s^p$ en característica p).

Sea k cualquier campo de característica p. El homomorfismo $\text{Frob}_k : k \to k$ es la función identidad si y sólo si $k = \mathbb{F}_p$. Para verlo, notamos que si $\text{Frob}_k = \text{Id}_k$ entonces $\alpha^p - \alpha = 0 \ \forall \ \alpha \in k$. Como el polinomio $y^p - y \in k[y]$ tiene p raíces distintas en $\overline{k}$, se obtiene que $2 \leq |k| \leq p$. Como $\text{char}(k) = p > 0$ entonces $|k| \geq p$, y por tanto $|k| = p$. Supongamos ahora que k está contenido en un anillo R. Consideramos a R como una k-álgebra. Entonces el homomorfismo de anillos Frob_R no es un morfismo de k-álgebras si $k \neq \mathbb{F}_p$. Sea R^p la imagen de Frob_R en R. En general, sea

$$R^{p^n} := \text{imagen de } (\text{Frob}_R)^n \text{ en } R = (R^{p^{n-1}})^p$$

El conjunto R^p es un subanillo de R, pero no es, en general, una k-subálgebra de R (es decir, puede existir $\alpha \in k$ y $r \in R^p$ tal que $\alpha r \notin R^p$). Recordamos que un campo k es perfecto si Frob_k es suprayectivo (y por tanto, un isomorfismo de campos.) Se puede verificar que R^p es una k-álgebra cuando k es perfecto.

Sea K cualquier campo de característica $p > 0$. Si $\alpha \in \overline{K}$, denotamos por $\alpha^{1/p}$ a la única raíz del polinomio $y^p - \alpha$ en $\overline{K}$, o equivalentemente, $\alpha^{1/p} = \text{Frob}_{\overline{K}}^{-1}(\alpha)$. Definimos inductivamente $\alpha^{1/p^n} := (\alpha^{1/p^{n-1}})^{1/p}$.

Proposición 5.1.1. *Sea k un campo perfecto. Sea $L/k(x)$ una extensión finita. Sea L/K una extensión finita puramente inseparable de grado p^n. Entonces $K = L^{p^n}$. En particular, $L = K^{1/p^n} := \{\alpha^{1/p^n} \mid \alpha \in K\}$*

Observación 5.1.2. *Sea $L = k(x, y)$ el campo de funciones racionales en dos variables. Sea $K = k(x, y^p)$. La extensión L/K es algebraica, con $[L : K] = p$.*

Se puede verificar que $x^{1/p} \notin L$ *y que* $L^p = k(x^p, y^p) \subset K \subset L$*, donde las contenciones son propias. De este ejemplo observamos que la hipótesis de que* $K/k(x)$ *es una extensión finita no puede ser omitida en la proposición anterior.*

Proposición 5.1.3. *Sea* k *un campo perfecto. Sea* $K/k(x)$ *una extensión finita. Sea* L/K *una extensión puramente inseparable de grado* p^n*. Sea* A *un dominio de Dedekind que contenga a* k *y que tenga a* K *como su campo de fracciones. Sea* B *la cerradura entera de* K *en* L*. Entonces*

- *(i)* B *es un dominio de Dedekind y* $A = B^{p^n}$*.*
- *(ii) La función inducida* $\pi : \mathrm{Max}(B) \to \mathrm{Max}(A)$*, con* $M \mapsto M \cap A$*, es una biyección.*
- *(iii) Los grupos* $\mathrm{Cl}(A)$ *y* $\mathrm{Cl}(B)$ *son isomorfos.*

La proposición 5.1.3 nos dice que B es un anillo noetheriano, pero no nos dice que sea un A-módulo finitamente generado. Cuando L/K es separable, el teorema 1.4.6, nos dice que la cerradura entera A en L es un A-módulo finitamente generado. Sin embargo, cuando $A = k[x]$ y se tiene una extensión finita $L/k(x)$ entonces no se necesita que sea separable.

Proposición 5.1.4. *Sea* k *cualquier campo. Sea* $L/k(x)$ *una extensión finita. Sea* B *la cerradura entera de* $k[x]$ *en* L*. Entonces* B *es un* $k[x]$*-módulo finitamente generado.*

Se puede generalizar lo anterior. Sea k cualquier campo. Sea A una k-álgebra finitamente generada con campo de fracciones K. Sea L/K una extensión finita. Entonces la cerradura entera de A en L es un A-módulo finitamente generado.

Corolario 5.1.5. *Sea* k *un campo perfecto de característica* $p > 0$*. Sea* $K/k(x)$ *una extensión finita. Sea* L/K *una extensión puramente inseparable de grado* p^n*. Sean* A *y* B *las cerraduras enteras de* $k[x]$ *en* K *y* L*, respectivamente. Sea* $P \in \mathrm{Max}(A)$*. Entonces* $PB = M^{p^n}$*, para algún* $M \in \mathrm{Max}(B)$*. Más aún, la función norma* $N_{B/A} : I_B \to I_A$ *está definida y* $\forall\ \alpha \in B$*,* $N_{B/A}(\alpha B) = N_{L/K}(\alpha)A$*.*

Proposición 5.1.6. *Sea* k *un campo perfecto. Sea* $L/k(x)$ *una extensión finita. Entonces existe* $y \in L$ *tal que* $L = k(x)(y)$*.*

Corolario 5.1.7. *Sea* k *un campo perfecto. Sea* $L/k(x)$ *una extensión finita que no es separable. Entonces existe* $y \in L$ *tal que*

- *(i) El campo* $k(y)$ *generado por* k *y* y *en* L *es isomorfo al campo de funciones racionales en una variable, y*
- *(ii)* $L = k(x)(y)$ *y la extensión* $L/k(y)$ *es separable.*

5.2. Resultados extras necesarios

En esta sección recordamos algunos resultados utilizados a lo largo de este trabajo. Algunos de los resultados aquí enunciados se escriben debido a que se utilizaron en algunos momentos de esta tesis pero que durante el proceso de escribir este trabajo no se tenían contemplados. También, algunos sirven solamente como observaciones importantes con respecto a algunos detalles del trabajo en cuestión. Por ejemplo, damos dos definiciones del concepto de anillo de valoraciones discreto (un concepto que no se menciona explícitamente por ejemplo durante la sección 2.2 del capítulo II donde se trata el concepto de valoración) y vemos que son equivalentes ambos.

Recordamos algunos resultados referentes a la relación que existe entre álgebras finitamente generadas y módulos finitamente generados.

Proposición 5.2.1. *Sea k cualquier campo. Sea A un dominio entero con campo de fracciones K. Supongamos que A es una k-álgebra finitamente generada. Sea L/K una extensión finita. Entonces la cerradura entera B de A en L es un A-módulo finitamente generado, y es también una k-álgebra finitamente generada.*

(para esta proposición, ver [7], teorema 3.9A, página 20)

Consideramos el siguiente lema que nos servirá para probar la proposición 5.2.3 (ver [8], sección 2 del capítulo 1).

Lema 5.2.2. *Sea A un anillo con campo de fracciones K, y x un elemento algebraico sobre K. Entonces existe un elemento $c \neq 0$ de A tal que cx es entero sobre A.*

Demostración. Como x es algebraico sobre K y K es el campo de fracciones de A entonces podemos encontrar una ecuación $a_x x^n + \cdots + a_0 = 0$, donde $a_n \neq 0$ y $a_i \in A$ para todo i. Multiplicamos esta ecuación por a_n^{n-1} para obtener $(a_n x)^n \cdots + a_0 a_n^{n-1} = 0$, y por tanto se obtiene que $a_n x$ es entero sobre A. □

Proposición 5.2.3. *Si B es una extensión entera sobre A y además es una A-álgebra finitamente generada entonces B es un A-módulo finitamente generado.*

Demostración. Notamos que, como B es una A-álgebra finitamente generada entonces $B = A[x_1, \ldots, x_r]$ con $x_i \in B$ (y con $A[x_1, \ldots, x_r]$ isomorfo como A-álgebra al anillo de polinomios en r variables con coeficientes en A), y podemos usar inducción en el número r. Así, basta probar el caso $r = 1$ y suponer que $B = A[x]$, con $x \in B$. Como B es extensión entera sobre A entonces existe un polinomio mónico $g(y) \in A[y]$ (donde y es una variable) tal que $g(x) = 0$, y donde $g(y)$ es de grado digamos n. Notamos que cualquier elemento en $A[x]$ es de

la forma $f(x)$ para algún $f(y) \in A[y]$. Como $A[x]$ es isomorfo como A-álgebra al anillo de polinomios $A[y]$ en una variable con coeficientes en A, podemos utilizar el algoritmo de la división para obtener $f(y) = g(y)h(y) + r(y)$, donde el grado de $r(y)$ es menor estricto a n. De la última igualdad se obtiene $f(x) = r(x)$, y por lo tanto cualquier elemento en $A[x]$ es una combinación lineal de los elementos $1, x, \ldots, x^{n-1}$ con coeficientes en A, y obtenemos lo buscado. □

Existen varias definiciones de anillo de valoraciones discreto. A continuación veremos dos de esas definiciones, y veremos que son equivalentes. La primera definición es la siguiente.

Definición 5.2.4. *Un anillo A es un anillo de valoraciones discreto si A es un dominio de ideales principales local que no sea campo.*

Recordamos que si A es un anillo local con ideal maximal P entonces el A-módulo P/P^2 es un espacio vectorial sobre A/P (la multiplicación por P manda P a P^2.)

Proposición 5.2.5. *Para un dominio local A con ideal maximal P son equivalentes:*

- *(i) A es un anillo de valoraciones discreto.*
- *(ii) A es noetheriano con dimensión de Krull 1, y además P/P^2 es de dimensión 1 sobre A/P.*
- *(iii) A es noetheriano y P es principal.*

Para probar lo anterior, usaremos dos corolarios de la siguiente versión del lema de Nakayama:

Lema 5.2.6. *Sea A un anillo local con ideal maximal P y sea M un A-módulo finitamente generado. Si $PM = M$ entonces $M = 0$.*

Corolario 5.2.7. *Sea A un anillo local noetheriano con ideal maximal P. Entonces $\cap_i P^i = (0)$. Además, si $P^i \neq (0)$ entonces $P^i \neq Pi + 1$.*

Demostración. Sea Q la intersección de los P^i. Como A es noetheriano entonces P es finitamente generado. Notamos que $PQ = Q$ (pues $Q \subseteq P$ y PQ es el menor subanillo de A que contiene a P y a Q), y aplicando el lema de Nakayama se obtiene la primera parte. Luego, como $P^i \subseteq P$ entonces se obtiene que P^i es un A-módulo finitamente generado, y aplicando de nuevo el lema 5.2.6, se obtiene la segunda parte. □

Corolario 5.2.8. *Sea A un anillo local con ideal maximal P. Sea M un A-módulo finitamente generado. Supongamos que existen elementos $t_1, \ldots, t_m \in M$ tales que sus imágenes forman un conjunto generador del espacio vectorial M/PM sobre A/P. Entonces $t_1, \ldots, t_m$ generan a M sobre A.*

Demostración. Sea T el A-submódulo generado por los t_i. Notamos entonces que se cumple que $M = T + PM$. Esto implica, a su vez, que $M/T = P(M/T)$. Aplicando el lema 5.2.7 se obtiene que $M = T$. □

Procedemos ahora a probar la proposición 5.2.5:

Demostración. (i) ⇒ (ii). Supongamos que A es un anillo de valoraciones discreto, y sea t un generador de P. Por el corolario 5.2.7, se obtiene que cualquier ideal primo distinto de cero $Q \subseteq P$ debe contener una potencia de t. (de lo contrario, se tendría para todo i que $P^i \not\subseteq Q$ y $P^i \cap Q \neq \emptyset$, por lo que la intersección de los P^i sería un subconjunto no vació de Q, contradiciendo el corolario 5.2.7). Como Q es primo entonces contiene a t mismo, y se obtiene que $Q = P$ y que A tiene dimensión de Krull 1. Además, la imagen de t en P/P^2 genera al A/P-espacio vectorial P/P^2.

(ii) ⇒ (iii). Basta aplicar el corolario 5.2.8 al caso $M = P$.

(iii) ⇒ (i). Supongamos que el ideal maximal P de A está generado por t. Veamos que cualquier elemento $a \in A$ se puede escribir de manera única como un producto de la forma $a = ut^n$, con u unidad en A, ya que del corolario 5.2.7 se obtiene que existe un único entero $n \geq 0$ tal que $a \in P^n \setminus P^{n+1}$, y por tanto a se puede escribir en la forma deseada. Además, si tenemos $a = ut^n = vt^n$ entonces $u = v$ pues A es dominio. Tomamos un ideal I de A. Como A es noetheriano entonces I está generado por un número finito de elementos $a_1 \ldots, a_k \in I$. Escribimos $a_i = u_i t^i$, $i = 1, \ldots, k$, y sea n_j el menor valor entre los n_i. Se obtiene que a_i es un múltiplo de t_{n_j} $\forall\, i$, y por tanto $I = (t^{n_j})$ es principal. □

Consideramos ahora la segunda definición de anillos de valoraciones discreto.

Definición 5.2.9. *Un dominio entero R es un anillo de valoraciones discreto si existe una valoración $v : F^* \to \mathbb{Z}$, con F el campo de fracciones de R, tal que $R = \{a \in F^* \mid v(a) \geq 0\} \cup \{0\}$.*

Proposición 5.2.10. *Sea R un dominio entero que sea local, noetheriano y de dimensión 1. Sea M es el único ideal maximal de R, y sea $k = R/M$ entonces son equivalentes:*

1. *(i) R es un anillo de valoraciones discreto.*
2. *(ii) R es enteramente cerrado.*
3. *(iii) El ideal maximal M de R es principal.*

4. *(iv) La dimensión M/M^2 sobre k (es decir, como espacio vectorial sobre k) es igual a 1.*

5. *(v) Todo ideal propio distinto de cero de R es una potencia de M.*

Demostración. Notamos primero que $M^{n+1} = M^n$ ya que si se tuviera $M^{n+1} = M^n$ entonces el R-módulo finitamente generado $M' = M^n$ cumpliría que $MM' = M'$ (recordamos que por ser R noetheriano, cualquier ideal es finitamente generado, y en particular M' es finitamente generado sobre R) y por Nakayama se tiene $M' = 0$, lo cual es falso. Notamos también que si I es cualquier ideal no cero de R entonces $\sqrt{I} = M$ entonces $\sqrt{I}$ es la intersección de todos los ideales primos que contienen a I, y como R es local y de dimensión 1, el único ideal primo de R es M. Esto implica que $M^n \subseteq I$ para algún n, y para verlo, escribimos $(x_1, \ldots, x_r)$. Como $\sqrt{I} = M$, existen enteros n_i con $x_i^{n_i} \in I$. Si ponemos $n = \sum n_i$ entonces M^n está generado por los elementos $x_1^{s_1}, \ldots, x_r^{s_r}$ con $\sum s_i = n$. Para cada uno de estos generadores se tiene algún con $s_i \geq n_i$, por lo que $x_i^{s_i} \in I$, y así el producto $x_1^{s_1} \cdots x_r^{s_r} \in I$. Por tanto, $M^n \subseteq I$. Con todo esto, se pueden probar las implicaciones:

i) $\Rightarrow$ ii). Sea F el campo de fracciones de R. Supongamos que $\alpha \in R$ es entero sobre R. Entonces $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ para algunos $a_i \in R$. Si $R = \mathcal{O}_v$ para alguna valoración v entonces $v(a_i) \geq 0$ para cada i. Supongamos que $\alpha \notin R$. Entonces $v(\alpha) < 0$. Multiplicando la igualdad por $1/\alpha^{n-1}$, se obtiene que $\alpha = -(a_{n-1} + a_{n-2}\alpha^{-1} + \cdots + a_0\alpha^{-n+1})$. El lado derecho pertenece a R (pues $v(\alpha^{-1}) > 0$ que por definición implica que $\alpha^{-1} \in R$). Por tanto, el lado izquierdo está en R, es decir, $\alpha \in R$, lo cual es una contradicción. Se obtiene que R es enteramente cerrado.

ii) $\Rightarrow$ iii). Sea $a \in M$ con $a \neq 0$. Sabemos entonces que $M^n \subseteq (a)$ para algún n. Sea n mínimo tal que $M^{n-1} \nsubseteq (a)$. Tomamos $b \in M^(n-1) \setminus (a)$, y sea $x = a/b$. Entonces $x^{-1} \notin R$ ya que $b \notin (a)$ (de lo contrario, tendríamos que $x^{-1}a \in (a)$, es decir, $b = \frac{b}{a}a \in (a)$, lo cual es contradicción) y entonces x^{-1} no es entero sobre R. Además tenemos que las condiciones $M^n \subseteq (a)$ y $b \in M^{n-1}$ implican que $x^{-1}M \subseteq R$ (eligiendo $m \in M$ se tiene $x^{-1}m = bm/a$, y $bm \in M^n \subseteq (a)$ y entonces $\exists\, c \in R$ tal que $bm = ac$ y entonces $bm/a = c \in R$). Ahora, si ocurre que $x^{-1}M = R$ entonces $M = (x)$ (se toma cualquier $m \in M$ y por tanto $\exists\, r \in R$ tal que $x^{-1}m = r$, es decir, $m = xr$), y por tanto M es principal. Si ocurriera $x^{-1}M \subset R$ entonces por ser $x^{-1}M$ ideal de R tendríamos $x^{-1}M \subseteq M$. Elegimos $u_1, \ldots, u_r$ generadores de M (R es noetheriano). Tenemos entonces que $x^{-1}u_i = \sum_{j=1}^{r} r_{ij}u_j$, para algunos $r_{ij} \in R$, y esto para cada i. Si escribimos $\delta_{ij} = 1$ si $i = j$ y $\delta_{ij} = 0$ si $i \neq j$ $(1 \leq i, j \leq r)$, se obtiene $\sum_{j=1}^{r}(r_{ij} - \delta_{ij}x^{-1})u_i = 0$ para cada i, y de esto se obtiene que la matriz A cuya entrada (i, j) es $r_{ij} - \delta_{ij}x^{-1}$ (con $1 \leq i, j \leq r$) es tal que su determinante al multiplicarse por cada u_j es igual a 0, es decir, $(\det(r_{ij} - \delta_{ij}x^{-1})_{1\leq i,j\leq r})u_j = 0$ para cada u_j. Como estamos en un dominio entero, se debe tener $\det(r_{ij} - \delta_{ij}x^{-1})_{1\leq i,j\leq r} = 0$. Desarrollando este determinante, se obtiene una expresión en términos de x^{-1} con coeficientes en R que es igual a 0, es decir, obtenemos que x^{-1} es entero sobre R, lo cual es una contradicción pues R es enteramente cerrado y $x^{-1} \notin R$.

Por tanto, no puede ocurrir $x^{-1}M \subseteq M$ y se cumple que $M = (x)$.

iii) $\Rightarrow$ iv) Supongamos que $M = (x)$. Entonces M está generado por x como R-módulo y por tanto M/M^2 está generado por $x + M^2$. Pero entonces M/M^2 está generado como R/M-módulo por $x + M^2$, y por tanto la dimensión de M/M^2 sobre k es menor o igual a 1, y como sabemos que $M/M^2 \neq 0$ entonces la dimensión es igual a 1.

iv) $\Rightarrow$ v). Sea $x + M^2$ un generador del espacio vectorial M/M^2 sobre R/M. Entonces $M = Rx + M^2 = Rx + M \cdot M$. Por tanto, por el lema de Nakayama se obtiene que $M = (x)$. Sea I cualquier ideal propio distinto de cero de R. Entonces $I \subseteq M$ pues M es el único ideal maximal de R. Sea r tal que $I \subseteq M^r$ y $I \nsubseteq M^{r+1}$ (notamos que tal r existe, pues de lo contrario tendríamos $I \subseteq M^r$ para toda r, y sabemos entonces que $M^n \subseteq I$ para algún n, por lo que $M^n = M^{n+s}$ para cada $s \geq 0$, lo cual es falso por lo mencionado al principio). Tomamos $y \in I \setminus M^{r+1}$. Entonces podemos escribir $y = ax^r$ para algún $a \in R$ pues $M = (x)$, y como $y \notin M^{r+1}$ entonces $a \notin M$, y por tanto a es una unidad en R. Por tanto, $(y) = (x^r) = M^r$, lo cual implica que $I = M^r$.

v) $\Rightarrow$ i). Sea F el campo de fracciones de R, y supongamos que cada ideal de R es una potencia de M. Para definir una valoración sobre F, tomamos $a \in R \setminus \{0\}$ y definimos $v(a) = n$ si $(a) = M^n$ (donde ponemos $M^0 = R$ para que v esté definida sobre todo elemento de R). Se obtiene entonces que $v(ab) = v(a) + v(b)$ y $v(a+b) \geq \min(v(a), v(b))$ $\forall\, a, b \in R$ (ya que $(a)(b) = (ab)$, y $(a + b) \subseteq (a) + (b)$). Para extender v a F^*, se define $v(a/b) = v(a) - v(b)$ ($b \in R \setminus \{0\}$). Notamos que está bien definida pues si $a/b = c/d$ entonces $ad = bc$, y por tanto $v(a)+v(d) = v(b)+v(c)$, y entonces $v(a)-v(b) = v(c)-v(d)$. Se puede verificar que v cumple las propiedades de una valoración. Además, de la definición de v se obtiene que $R \subseteq \mathcal{O}_v$ y $M \subseteq M_v$. Sea $a/b \in F$ con $a, b \in R$. Entonces $0 \leq v(a/b) = v(a) - v(b)$, y entonces $v(a) \geq v(b)$. Queremos ver que $a = bx$ para algún $x \in R$ (lo cual implicaría $a/b \in R$ y por tanto se tendría $R \subseteq \mathcal{O}_v$ y así al igualdad $R = \mathcal{O}_v$). Sea $\pi \in M \setminus M^2$. Entonces $(\pi) = M$ pues todos los ideales de R son potencias de R y $(\pi) \nsubseteq M^2$. Por tanto, M es principal, y por consecuencia todas las potencias de M son principales, y así todos los ideales de R son principales. Si $(a) = M^n = (\pi^n)$ y $(b) = M^m = (\pi^m)$ entonces $n \geq m$ y escribimos $a = \pi^n x$ y $b = \pi^m y$ con x, y unidades de R. Entonces $a/b = \pi^{n-m} x/y \in R$ pues $n - m \geq 0$ y x, y son unidades en R y por tanto $x/y \in R$. Se obtiene que $\mathcal{O}_v = R$, y como $\mathcal{M}_v$ es un ideal de R que contiene a M, se obtiene que $\mathcal{M}_v = M$. $\square$

Notamos entonces que las proposiciones 5.2.3 y 5.2.5 implican que las definiciones 5.2.4 y 5.2.9 son equivalentes y podemos usarlas indistintamente.

Recordamos ahora algunos teoremas importantes que se usan a lo largo de todo el trabajo. Algunos de los resultados que siguen a continuación ya aparecieron antes pero se vuelven a mencionar para recalcar algunas observaciones que son importantes durante el proceso del trabajo. El resto de los resultados a continuación se desprenden del mismo trabajo y por tanto se escribe la

demostración correspondiente.

Recalcamos de nuevo las condiciones necesarias para que, dado un dominio de Dedekind A con campo de fracciones K y una extensión finita L/K, la cerradura entera B de A en L también sea dominio de Dedekind.

Teorema 5.2.11. *Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita, y sea B la cerradura entera de A en L. Supongamos que B es un A-módulo finitamente generado. Entonces B también es un dominio de Dedekind.*

Demostración. Como A es noetheriano y B es un A-módulo finitamente generado entonces del corolario 1.4.5, se obtiene que B es noetheriano. Como A tiene dimensión 1 y L/K es finita entonces del corolario 1.5.8, se obtiene que B también tiene dimensión 1. Finalmente, por la proposición 1.2.15, inciso ii), se obtiene que B es eneteramente cerrado. Por tanto, B es de Dedekind. □

Observación 5.2.12. *En el teorema 5.2.11, si la extensión L/K es separable entonces puede omitirse la condición de que B sea un A-módulo finitamente generado, gracias al teorema 1.4.6.*

Recalcamos a continuación algunos detalles de la relación que hay entre un dominio de Dedekind A con campo de fracciones K y el dominio de ideales principales local $\mathcal{O}_v$ dado por una valoración $v : K \to \mathbb{Z}$.

Lema 5.2.13. *Sea A un dominio de Dedekind con campo de fracciones K. Sea $v : K^* \to \mathbb{Z}$ una valoración suprayectiva tal que $v(A) \geq 0$. Entonces existen un ideal maximal M de A tal que $A_M = \mathcal{O}_v$. En particular, se tiene $v = v_M$, donde $v_M : K \to \mathbb{Z}$ es la valoración M-ádica con $M := M_v \cap A$.*

Demostración. Sea $M := \mathcal{M}_v \cap A$. Tenemos que $v(A) \geq 0$, y por tanto $A \subseteq \mathcal{O}_v$, y sea i la inclusión inducida. Como A es dominio, la función $j : A \to A_M$ (con $a \mapsto \frac{a}{1}$) es inyectiva. Además, cada elemento perteneciente a la imagen bajo i del conjunto multiplicativo $A \setminus M$ es invertible en $\mathcal{O}_v$ (pues M es maximal en A, y su complemento en A consiste de los elementos invertibles en A, los cuales a su vez lo siguen siendo en $\mathcal{O}_v$). Por tanto, aplicando la propiedad universal de anillos de fracciones, se obtiene que existe una función (inyectiva) $f : A_M \to \mathcal{O}_v$ tal que $i = f \circ j$. Por tanto, $A_M \subseteq \mathcal{O}_v$.

Notemos ahora que $MA_M \subseteq \mathcal{M}_v$. Si $m/s \in MA_M$ (con $m \in M$, $s \in A \setminus M$) entonces $f(m/s) = i(m)(i(s))^{-1} = ms^{-1}$. Luego, $v(ms^{-1}) = v(m) + v(s) = v(m) > 0$ (pues $m \in M = \mathcal{M}_v \cap A$ y s es invertible en $\mathcal{O}_v$). Por tanto, $m/s \in \mathcal{M}_v$. Aplicando entonces el lema 1.14.6, se obtiene que $A_M = \mathcal{O}_v$.

Aplicando el lema 5.2.14 abajo, obtenemos que $\mathcal{O}_{v_M} = \mathcal{O}_v$ (y notamos además que ambos son dominios de ideales principales locales con campo de fracciones K, y $v_M, v : K^* \to Z$ suprayectivas), y entonces del teorema 2.2.8 se obtiene $v_M = v$. □

Lema 5.2.14. *Sea A un dominio de Dedekind con campo de fracciones K. Sea $v_M : K^* \to \mathbb{Z}$ la valoración M-ádica asociada a un ideal maximal M de A. Entonces $\mathcal{O}_{v_M} = A_M$.*

Demostración. Como v_M es la valoración M-ádica entonces $v_M(A) \geq 0$, y $A \subseteq \mathcal{O}_{v_M}$. Además, como M es maximal en A entonces el subconjunto multiplicativo $S := A \setminus M$ es un conjunto de elementos invertibles en A, y por tanto son invertibles en $\mathcal{O}_{v_M}$. Consideramos la inclusión $i : A \hookrightarrow \mathcal{O}_{v_M}$. Aplicando la propiedad universal de anillos de fracciones, obtenemos una función única $g' : A_M \to \mathcal{O}_{v_M}$ tal que $i = g' \circ j$ (con $j : A \to A_M$, $a \mapsto a/1$, que es inyectiva por ser A dominio), y por tanto g' es inyectiva, y obtenemos $A_M \subseteq \mathcal{O}_{v_M}$. Por otro lado, de la demostración de la propiedad universal de anillos de fracciones, se puede obtener que la imagen bajo g' de un elemento $m/s \in MA_M$, con $m \in M$ y $s \in A \setminus M$, es igual a $i(m)i(s)^{-1} = ms^{-1}$. Luego, por ser s^{-1} invertible en $\mathcal{O}_{v_M}$, se tiene $v_M(s^{-1}) = 0$, y como $m \in M$ entonces $(m) \subseteq M$, y de la definición de v_M se obtiene que $v_M(m) > 0$. Por tanto, $v_M(ms^{-1}) > 0$, y $ms^{-1} \in \mathcal{M}_{v_M}$, es decir, $MA_M \subseteq \mathcal{M}_{v_M}$. Además, como $A \subseteq A_M \subseteq K$ entonces el campo de fracciones de A_M es K. Entonces, aplicando el lema 1.14.6, se obtiene que $A_M = \mathcal{O}_{v_M}$. □

Lema 5.2.15. *Sea A un anillo de valoraciones discreto con campo de fracciones K inducido por una valoración discreta $v : K^* \to \mathbb{Z}$. Sea B cualquier subanillo de K que contenga a A. Entonces $B = K$ o $B = A$.*

Demostración. Supongamos que $B \neq A$. Entonces existe un elemento $a \in B$ que no está en A. Como $A = \{x \in K \mid v(x) \geq 0\}$, tenemos que $v(a) < 0$. Sea $x \in K$. Para una n suficientemente grande, se obtiene que $v(xa^{-n}) = v(x) - nv(a) > 0$, por lo que $xa^{-n} \in A \subseteq B$. Por tanto, $x = xa^{-n} \cdot a^n \in B$. □

Lema 5.2.16. *Sea A un dominio de Dedekind con campo de fracciones K. Sea L/K una extensión finita, y sea B la cerradura entera de A en L. Supongamos que B es un A-módulo finitamente generado. Sea $P \in \mathrm{Max}(A)$, junto con $v_P : K^* \to \mathbb{Z}$ su valoración P-ádica asociada, y factorizamos al ideal PB en un producto de ideales maximales de B, $PB = \prod_i \mathcal{B}_i^{e_i}$, y fijamos una $\mathcal{B}_i$, junto con $v_{\mathcal{B}_i} : L^* \to \mathbb{Z}$ su valoración $\mathcal{B}_i$-ádica. Entonces $v_{\mathcal{B}_i}(x) = e_i v_P(x)$.*

Demostración. Tenemos que la restricción $v_{\mathcal{B}_i}|_K : K \to \mathbb{Z}$ es una valoración discreta pero no necesariamente suprayectiva. Sea e el entero positivo tal que $\frac{1}{e} v_{\mathcal{B}_i}$ es suprayectiva. Del lema 5.2.14 tenemos que $\mathcal{O}_{v_{\mathcal{B}_i}} = B_{\mathcal{B}_i}$, y por tanto $\{x \in K \mid v_{\mathcal{B}_i}(x) \geq 0\} = B_{\mathcal{B}_i} \cap K$. Además, notamos que $A \subseteq A_P \subseteq K$, y además que por tener $A \subseteq B$ y $P \subseteq \mathcal{B}_i$ (pues $\mathcal{B}_i$ aparece en la factorización de PB), se tiene $A_P \subseteq B_{\mathcal{B}_i}$. Por tanto, se obtiene que $A_P \subseteq B_{\mathcal{B}_i} \cap K$. Por otro lado, observamos que $B_{\mathcal{B}_i} \cap K \neq K$, ya que si $p \in P$ entonces $1/p \in K$ no puede ser un elemento de $B_{\mathcal{B}_i}$, ya que de lo contrario tendríamos $1/p = b/s$, con $b \in B$ y $s \in B \setminus \mathcal{B}_i$, y entonces $s = pb \in PB$, lo cual no es posible pues $PB \subseteq \mathcal{B}_i$. Así,

aplicando el lema 5.2.15 obtenemos $A_P = B_{\mathcal{B}_i} \cap K$, y se obtiene entonces que $v_P = \frac{1}{e} v_{\mathcal{B}_i}$.

Ahora, veamos que $e = e_i$. Sea $u \in A_P$ tal que $v_P(u) = 1$. Como v_P es una valoración suprayectiva, y el elemento en $\mathcal{O}_{v_P}$ que genera al ideal maximal $\mathcal{M}_{v_P}$ toma el menor valor positivo entonces se obtiene que $uA_P = PA_P$, y además, que $uB_{\mathcal{B}_i} = uA_P B_{\mathcal{B}_i} = PA_P B_{\mathcal{B}_i} = (\mathcal{B}_i B_{\mathcal{B}_i})^{e_i}$, donde la última igualdad se obtiene del lema 1.17.2. De la definición de $v_{\mathcal{B}_i}$ y del mismo lema 1.17.2, se obtiene que $v_{\mathcal{B}_i}(u) = e_i$, y como $v_P = \frac{1}{e} v_{\mathcal{B}_i}$ entonces $1 = v_P(u) = \frac{1}{e} v_{\mathcal{B}_i}(u) = e_i/e$, y por tanto $e = e_i$, y se obtiene el resultado. □

Observación 5.2.17. *Podemos sustituir en el lema 5.2.16 la condición de que B sea un A-módulo finitamente generado por la condición de que L/K sea separable, gracias a la observación 5.2.12.*

Observación 5.2.18. *Sea L cualquier campo. Sea $w : L^* \to \mathbb{Z}$ una valoración suprayectiva de L. Entonces L es el campo de fracciones del dominio de ideales principales local $\mathcal{O}_w$. Para verlo, sea a/b un elemento en el campo de fracciones de $\mathcal{O}_w$. Entonces $a, b \in \mathcal{O}_w$, y $w(a/b) \in \mathbb{Z}$. Como w es suprayectiva entonces existe un elemento $m \in L$ tal que $w(m) = w(a/b)$, lo cual implica que $w(\frac{a}{b} \cdot m^{-1}) = 0$, y por tanto, el elemento $\frac{a}{b} \cdot m^{-1}$ pertenece a $\mathcal{O}_w \setminus \mathcal{M}_w$, es decir, es igual a una unidad u en $\mathcal{O}_w \subseteq L$, y se obtiene que $a/b = mu \in L$. Recíprocamente, si $m \in L$ entonces $w(m) \in \mathbb{Z}$. Sean $r, s \geq 0$ tales que $w(m) = r - s$. Por ser w suprayectiva, existen $a, b \in L$ tales que $w(a) = r$ y $w(b) = s$. Notamos entonces que $a, b \in \mathcal{O}_w$. Tenemos que $w(a/b) = w(m)$, y se obtiene nuevamente que existe una unidad u en $\mathcal{O}_w$ tal que $\frac{a}{b} m^{-1} = u$, es decir, $m = u^{-1} \frac{a}{b}$, el cual pertenece al campo de fracciones de $\mathcal{O}_w$. Por tanto, se obtiene el resultado deseado.*

Se menciona a continuación una observación referente a la factorización de un ideal en un dominio de Dedekind.

Observación 5.2.19. *Sea A un dominio de Dedekind, y $x \in A$. Consideramos la factorización única $(x) = \prod_i P_i^{n_i}$ del ideal (x) en ideales maximales P_i de A. Sabemos que x pertenece a un ideal maximal si y sólo si dicho ideal maximal aparece en la factorización única del ideal (x). Además, se cumple que $x \in P_i^{n_i}$ pero $x \notin P_i^{n_i+1}$. Para verlo esto último, notamos que si tenemos cualesquiera $P, Q \in \mathrm{Max}(A)$ entonces P^n y Q^m son primos relativos, con $m, n \in \mathbb{N}$ (pues cualesquiera dos ideales maximales son primos relativos, y la igualdad $A = P + Q$ implica $A = A^{n+m-1} = (P + Q)^{n+m-1} \subseteq P^n + Q^m$, por lo que $A = P^n + Q^m$). Usando el lema 1.17.6 inciso ii), se obtiene entonces que $(x) = \prod_i P_i^{n_i} = \cap_i P_i^{n_i}$, y por tanto, $x \in P_i^{n_i}$. Si ocurriera que $x \in P_j^{n_j+1}$ para algún j entonces la contención $P_j^{n_j+1} \subset P_j^{n_j}$ (la cual es contención propia por ser A de Dedekind, es decir, por tener la propiedad de factorización única en ideales maximales)*

implicaría que $(x) = \cap_i P_i^{n_i'}$, *donde* $n_i' = n_i$ *si* $i \neq j$, *y* $n_i' = n_i + 1$ *si* $i = j$, *y de nuevo por el lema 1.17.6, inciso ii), se tendría* $(x) = \prod_i P_i^{n_i'}$, *donde* $n_i' = n_i$ *si* $i \neq j$, *y* $n_i' = n_i + 1$ *si* $i = j$, *lo cual contradice la propiedad de factorización única en ideales maximales de A. Se obtiene así el resultado.*

Notamos también que del procedimiento anterior se obtiene que si x pertenece a un ideal maximal P, y si pertenece a P^n *pero no a* P^{n+1} *entonces en la factorización del ideal* (x) *aparecerá el factor* P^n *(es decir, P únicamente aparecerá elevado a la potencia n en la factorización de* (x)*).*

Tenemos también un lema sobre dominios de Dedekind y dominios de ideales principales.

Lema 5.2.20. *Sea A un dominio de Dedekind, y M un ideal maximal de A. Entonces* A_M *es un dominio de ideales principales local.*

Demostración. Como A es de Dedekind entonces A_M también lo es. Además, A_M es local por propiedades de localización, por lo que tiene un número finito de ideales maximales. De estos dos hechos, se obtiene que A_M es de ideales principales (un dominio de Dedekind con un número finito de ideales maximales es es un dominio de ideales principales). □

Finalmente, se concluye con una observación sobre el valor de $\deg(P)$ cuando P pertenece a $\mathbb{P}^1/k$, donde k es cualquier campo.

Observación 5.2.21. *Sea* $\mathbb{P}^1/k$ *curva completa no singular asociada a un campo de funciones* $k(x)/k$. *Sea* $v \in \mathcal{V}(k(x)/k)$. *Por el teorema 2.2.10, sabemos que* $v = v_{g(x)}$ *con* $g(x) \in k[x]$ *mónico e irreducible, o* $v = v_\infty$. *En el primer caso, se tiene* $[\mathcal{O}_v/\mathcal{M}_v : k] = n =$ *grado de* $g(x)$, *ya que por el teorema 2.2.10 se tiene que* $\mathcal{O}_v/\mathcal{M}_v \cong k[x]/(g)$, *y una base para este cociente es* $1, x, \ldots, x^{n-1}$. *En el segundo caso, se tiene que* $[\mathcal{O}_\infty/\mathcal{M}_\infty : k] = 1$, *ya que nuevamente se tiene* $\mathcal{O}_\infty/\mathcal{M}_\infty \cong k[1/x]/(1/x) \cong k$, *y se obtiene el resultado.*

Referencias

[1] Atiyah M. y McDonald, I. *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] Bombieri, E. *Counting points on curves over finite fields*, Seminaire Bourbaki 430, 1972/73.

[3] Bump, D. *Algebraic Geometry*, World Scientific, 1998.

[4] Deligne, P. *La conjecture de Weil I*, Publ. Math. IHES 43, 1974, 273-307.

[5] Dwork, B. *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math., **82**(1960), 631-648

[6] Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry*, Springer Verlag, 1995.

[7] Hartshorne, R. *Algebraic Geometry*, Springer-Verlag, 1977.

[8] Lang, S. *Algebraic Number Theory*, Springer-Verlag, 1994.

[9] Lorenzini, D. *An Invitation to Arithmetic Geometry*, Graduate Studies in Mathematics. American Mathematical Society, 1996.

[10] Moreno, C. *Algebraic Curves Over Finite Fields*, Cambridge Press University, 1991.

[11] Niven, I. *Formal Power Series*, Am. Monthly **76**, Mathematical Asociation of America, Octubre 1969, 871-894.

[12] Zariski, O. y Samuel, P. *Commutative Algebra Volume I*, Springer, 1958.