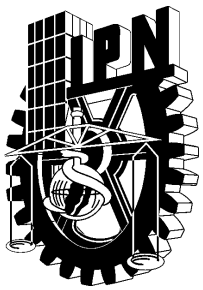

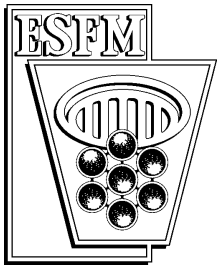

INSTITUTO POLITECNICO NACIONAL

Escuela Superior de Física y Matemáticas

Introducción a los Puntos de Weierstrass en Característica Positiva

TESIS

QUE PARA OBTENER EL TITULO DE

Maestro en Ciencias

PRESENTA

CAIN ALVAREZ GARCIA

Director de Tesis

Dr. Gabriel Villa Salvador

México, D. F. Diciembre de 2005

CGPI-14

INSTITUTO POLITECNICO NACIONAL

SECRETARIA DE INVESTIGACION Y POSGRADO

ACTA DE REVISION DE TESIS

En la Ciudad de México, D. F., siendo las 12:00 horas del día 31 del mes de Octubre del 2005 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de la ESFM para examinar la tesis de grado titulada:

"Introducción a los Puntos de Weierstrass en Característica Positiva "

Presentada por el alumno:

Álvarez	García	Caín
Apellido paterno	materno	nombre(s)

Con registro: A 0 3 0 2 7 2

aspirante al grado de:

Maestro en Ciencias con especialidad en Matemáticas

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACION DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISION REVISORA

Director de tesis

Dr. Gabriel Villa Salvador

Dr. Valeri Kucherenko

Dr. José María Rocha Martínez
(Co-director)

Dr. Edmundo del Valle Gallegos

Dr. Pablo Lam Estrada

ESCUELA SUPERIOR DE FISICA Y MATEMATICAS I. P. N.

EL PRESIDENTE DEL COLEGIO

M. en C. Carlos Antonio Díaz Pico

INSTITUTO POLITECNICO NACIONAL

COORDINACION GENERAL DE POSGRADO E INVESTIGACION

CARTA CESION DE DERECHOS

En la Ciudad de México el día 14 del mes de noviembre del año 2005 el que suscribe Cain Alvarez Garcia alumno del Programa de Estudios de Posgrado en la E.S.F.M del I.P.N con número de registro A030272 adscrito a la Especialidad en Matemáticas, manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección del Dr. Gabriel Villa Salvador y cede los derechos del trabajo titulado Introducción a los Puntos de Weierstrass en Característica Positiva al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección cainalvarez@hotmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Cain Alvarez Garcia

Cain Alvarez Garcia.

Nombre y Firma

Resumen

Introduccion a los Puntos de Weierstrass en Caracteristica Positiva

En ciertas extensiones cíclicas de un campo de funciones racionales K(x) existen condiciones necesarias bajo las cuales un divisor primo de la extensión sea un punto de Weierstrass. Supongamos que F/K es un campo de funciones algebraicas cuyo campo de constantes es algebraicamente cerrado de característica $p > 0$.
Entonces para cualquier extensión cíclica F/K(x) de grado p^n, $n > 1$, los lugares de F totalmente ramificados en F/K(x) son puntos de Weierstrass.
Cuando p no divide al grado m de la extensión cíclica F/K(x) es necesario que existan al menos $m + 3$ divisores primos totalmente ramificados para que todo divisor primo que se ramifique totalmente en dicha extensión sea un punto de Weierstrass.
El hecho de suponer que la sucesión laguna del campo de funciones F es la clásica nos permite abandonar la hipótesis sobre el género de E en una extensión cíclica F/E de campos de funciones. Así, cualquier lugar totalmente ramificado en F/E es un punto de Weierstrass si existen al menos cinco de estos lugares.

Abstract

Introduction to Weierstrass Points in Positive Characteristic

In certain cyclic extensions of rationals functions fields K(x) exist necessary conditions which a prime divisor of the extension is a Weierstrass point. Assume F/K is an algebraic functions field of which constants field is algebraically closed of characteristic $p > 0$.
For any cyclic extension F/K(x) of grade p^n, $n > 1$, the places of F totally ramified are Weierstrass points. When p doesn't divide to the grade m of the cyclic extension it is necessary the existence of at least $m + 3$ prime divisors totally ramified so for all prime divisor is a Wierstrass point if it is totally ramified over the mentioned extension.
The fact of assuming the functions field F sequence is the classical, allow us to leave the E genus over a fields cyclic extension F/E hypothesis. Thus, for any place totally ramified in F/E is a Weierstrass point if exists at least five of these places.

Introducción

Superficies de Riemann

La teoría de las superficies de Riemann se encuentra en la intersección de muchas áreas de las matemáticas y es fuente de inspiración, intuición y ejemplos en ramas como variedades complejas, grupos de Lie, teoría algebraica de números, análisis armónico, variedades abelianas y topología algebraica entre otras.
Una *superficie de Riemann* es una variedad analítica compleja conexa uno-complejo-dimensional; esto es, una variedad conexa M dos-real-dimensional con un conjunto maximal de cartas $\{\mathrm{U}_\alpha, z_\alpha\}_{\alpha\in\mathrm{A}}$ sobre M (es decir, $\{\mathrm{U}_\alpha\}_{\alpha\in\mathrm{A}}$ es una cubierta abierta de M y $z_\alpha : \mathrm{U}_\alpha \to \mathbb{C}$ es un homeomorfismo sobre un subconjunto abierto del plano complejo $\mathbb{C}$) tal que las *funciones de transición*

$$f_{\alpha\beta} = z_\alpha \circ z_\beta^{-1} : z_\beta(\mathrm{U}_\alpha \cap \mathrm{U}_\beta) \to z_\alpha(\mathrm{U}_\alpha \cap \mathrm{U}_\beta)$$

son holomorfas siempre que $\mathrm{U}_\alpha \cap \mathrm{U}_\beta \neq \emptyset$.
Una función continua $f : \mathrm{M} \to \mathrm{N}$ entre dos superficies de Riemann es llamada *holomorfa* o *analítica* si para toda carta $\{\mathrm{U}, z\}$ sobre M y toda carta $\{\mathrm{V}, \zeta\}$ en N con $\mathrm{U} \cap f^{-1}(\mathrm{V}) \neq \emptyset$, la función

$$\zeta \circ f \circ z^{-1} : z(\mathrm{U} \cap f^{-1}(\mathrm{V})) \to \zeta(\mathrm{V})$$

es holomorfa (como una función de $\mathbb{C}$ a $\mathbb{C}$). La función f es llamada *conforme* si es uno a uno y sobre. Dos superficies de Riemann M, N son *conformemente equivalentes* (isomorfas como superficies de Riemann) si existe una función holomorfa $f : \mathrm{M} \to \mathrm{N}$ biyectiva con inversa holomorfa.
El conjunto de todas la funciones holomorfas de una superficie de Riemann M a $\mathbb{C}$ forma un anillo H(M), en el cual la suma y multiplicación de funciones se define

puntualmente. Una *función meromorfa* es una función holomorfa de M en $\mathbb{C} \cup \{\infty\}$. El conjunto de todas las funciones meromorfas forma un campo K(M).
La definición de superficie de Riemann mezcla conceptos topológicos y analíticos. Dicha interacción da por resultado una caracterización analítica y otra topológica cuando se consideran superficies de Riemann compactas. Más precisamente se tienen los siguientes resultados (ver [2], [4] y [12]).

TEOREMA 1 *Toda superficie de Riemann compacta* M *es homeomorfa a la esfera de Riemann con* g *asas, donde* $g \in \mathbb{Z}$, $g \geq 0$, g *es llamado el género de* M, *y por lo tanto dos superficies de Riemann son topológicamente equivalentes si y sólo si tienen el mismo género.*

TEOREMA 2 *Toda superficie de Riemann compacta de género* g *es conformemente equivalente a una cubierta de* $(g+1)$ *hojas de la esfera de Riemann.*

El género caracteriza topológicamente a las superficies de Riemann compactas pero no analíticamente; por ejemplo, existe una cantidad infinita de superficies de Riemann de género uno conformemente inequivalentes a pares.

TEOREMA 3 *Sea* M *una superficie de Riemann. Entonces* K(M) *es un campo finitamente generado sobre* $\mathbb{C}$ *con grado de trascendencia 1, esto es,* $\mathrm{K(M)} \cong \mathbb{C}(x, y)$ *con* x, y *dos indeterminadas sobre* $\mathbb{C}$ *sujetas a una relación* $F(x, y) = 0$, *con* F *un polinomio en dos variables no cero.*

El Teorema 3 nos dice que el campo K(M) es un *campo de funciones de una variable* y su importancia queda determinada por el siguiente

TEOREMA 4 *Sean* M, N *dos superficies de Riemann compactas. Entonces* M *y* N *son conformemente equivalentes si y sólo si* K(M) *y* K(N) *son* $\mathbb{C}$*-isomorfas como campos (esto es, existe* $\varphi : \mathrm{K(M)} \to \mathrm{K(N)}$ *isomorfismo de campos tal que* $\varphi(\alpha) = \alpha$ *para toda* $\alpha \in \mathbb{C}$).

Por lo tanto, el campo de funciones meromorfas de una superficie de Riemann M refleja en el espacio de los *campos funciones* sobre $\mathbb{C}$ propiedades que determinan su clase de equivalencia conforme, es decir, el conjunto de todas las superficies de Riemann que son conformemente equivalentes con M. Este hecho nos permite pensar en los campos de funciones como superficies de Riemann sobre un campo arbitrario.

Puntos de Weierstrass en el caso clásico

Sea M una superficie de Riemann de género g mayor o igual que 2. Para cada punto $\mathrm{P} \in \mathrm{M}$, construimos una sucesión de enteros positivos

$$\nu_1 < \cdots < \nu_k < \cdots ,$$

como sigue: ν_k está en la lista si y sólo si existe una función meromorfa sobre M que sea holomorfa en $\mathrm{M} \setminus \{\mathrm{P}\}$ con un polo de orden ν_k en P ¿Cuántas sucesiones de este tipo existen? *Para casi todos* (es decir, para todos salvo posiblemente un número finito) los puntos de la sucesión son

$$g+1, g+2, g+3, \ldots$$

Los puntos que en número finito son las excepciones son los llamados *puntos de Weierstrass*.

Teorema 5 *Sea* M *una superficie de Riemann de género positivo* g *y* $\mathrm{P} \in \mathrm{M}$ *un punto arbitrario. Entonces existen solamente* g *enteros*

$$1 = n_1 < n_2 < \cdots < n_g < 2g$$

tales que no existe una función $f \in \mathrm{K(M)}$ *holomorfa en* $\mathrm{M} \setminus \{\mathrm{P}\}$ *con un polo de orden* n_j *en* P.

A los g números enteros del Teorema 5 les llamaremos *números laguna* en P. Sea

$$\mu_1 < \cdots < \mu_k < \cdots ,$$

la única sucesión determinada por el complemento de $\{\nu_k\}$ en $\mathbb{Z}^+$. La sucesión $\{\mu_k\}$ tiene dos ventajas, por el Teorema 5 $\{\mu_k\}$ tiene g elementos y para casi todos los puntos es igual a

$$1, 2, \ldots, g.$$

Esto nos da una definición equivalente de lo que es un punto de Weierstrass: Un punto P de M es un punto de Weierstrass si y sólo si existe una función meromorfa sobre M que sea holomorfa en $\mathrm{M} \setminus \{\mathrm{P}\}$ con un polo de orden ν, $\nu < g$, en P.
Es de interés encontrar una manera de trasladar el concepto de punto de Weierstrass al campo de funciones meromorfas $\mathrm{K(M)} = \mathrm{F}$. A cada punto P de M se le identifica

con el *divisor primo* de F determinado por el anillo de valuación que consiste de todas las funciones holomorfas en P. Entonces el divisor primo P es un punto de Weierstrass de F si el punto P lo es para M.
La existencia de puntos de Weierstrass queda determinada por el teorema de Riemann-Roch (Teorema 1.46). F no tiene puntos de Weierstrass cuando su *género* es menor que 2. Un campo de género cero es un campo de funciones racionales, mientras que un campo de género uno es un campo de funciones elípticas. Campos de género mayor o igual a dos tienen al menos $2g + 2$ puntos de Weierstrass y a lo más $g^3 - g$. Todo automorfismo σ de F que sea la identidad sobre su *campo de constantes* mapea de manera natural al conjunto de los puntos de Weierstrass en si mismo. Este hecho se utiliza para demostrar que el grupo de automorfismos de F que son la identidad en su campo de constantes es de orden finito. Lewittes [9] demostró que si σ deja fijos al menos a cinco divisores primos, entonces cada divisor primo fijado es un punto de Weierstrass. Accola [1] dio una demostración simple para la afirmación anterior. Hasta aquí se ha resumido brevemente el caso clásico.

Puntos de Weierstrass en característica positiva

Consideremos un *campo de funciones algebraicas* F *de una variable* de género g en el cual su campo de constantes K es algebraicamente cerrado de característica positiva p. Schmidt [11] generaliza la definición de punto de Weierstrass para este caso. Dado un divisor primo P de F/K existen g enteros positivos λ menores que $2g - 1$, tales que no existe una función f en F que tenga a P como único polo de multiplicidad λ. Los números λ son llamados números *laguna* de P. Al igual que en el caso clásico casi todos los divisores primos tiene los mismos números laguna y el conjunto finito de excepciones son los puntos de Weierstrass de F. Nuevamente, con la ayuda del teorema de Riemann-Roch se concluye la existencia de puntos de Weierstrass cuando el género es mayor que uno. Aquí encontramos una diferencia con el caso clásico, campos de género arbitrariamente grande pueden tener sólo un punto de Weierstrass. En [10] Schmid establece que si F es una extensión cíclica del campo de funciones racionales K(x) cuyo grado es una potencia de p, entonces todo divisor primo *totalmente ramificado* es un punto de Weierstrass, siempre que F no pertenezca a una clase singular. En su demostración supuso que el complemento de los puntos de Weierstrass tiene los mismos números laguna que en el caso clásico, cosa que en

general no ocurre. En [3] (ver también [5]) Boseck demostró el resultado de Schmid cuando el grado de F sobre K(x) es p.

El presente trabajo está basado en el artículo *Weierstrass Points in Characteristic p* escrito por Robert C. Valentini y Manohar L. Madan [14]. Por lo cual los objetivos que presentaremos están determinados por aquellos del artículo mencionado, sin embargo se incluirán algunos que son propios. El objetivo principal es dar una demostración del teorema de Schmid [10]. Esto está desarrollado en la Sección 2.2. Después, en la Sección 2.3, tratamos con extensiones cíclicas de un campo de funciones racionales K(x) cuyo grado m es primo relativo con la característica de K. Aquí se logra probar la siguiente generalización de un resultado de Boseck: si al menos $m+3$ primos son totalmente ramificados, entonces todo primo totalmente ramificado es un punto de Weierstrass. Cuando en la Sección 2.4 suponemos que para el campo de funciones en consideración su *sucesión laguna* es la clásica, evitamos tratar solamente con extensiones cíclicas de un campo de funciones racionales y se generaliza una afirmación de Lewittes demostrada por él en [9]. Finalmente nuestro trabajo estuvo dirigido a desarrollar y completar las demostraciones contenidas en el artículo de Valentini y Madan, además de dar algunas observaciones particulares (subsección 2.2.1) a los resultados mencionados en dicho artículo.

Los resultados presentados en el Capítulo 1 no están acompañados de una demostración y a menos que se diga lo contrario éstas se encuentran en [13].

Índice general

Capítulo 1

Campos de Funciones Algebraicas

En este capítulo presentamos resultados generales de campos de funciones algebraicas de una variable que son la base para el desarrollo de este trabajo. Sus demostraciones se pueden encontrar en [13].

1.1. Campos de Funciones

DEFINICIÓN 1.1 *Sea* K *un campo. Un campo de funciones algebraicas* F *sobre* K *es una extensión de campos de* K*, finitamente generada, con grado de transcendencia* $r \geq 1$*. El campo* F *recibe el nombre de campo de funciones de* r *variables.*

En adelante nos concentraremos en el caso $r = 1$, esto es, F será un campo de funciones de una variable y para abreviar sólo lo llamaremos *campo de funciones* y se escribirá F/K para denotarlo.

DEFINICIÓN 1.2 *Sea* F/K *un campo de funciones. A la cerradura algebraica de* K *en* F*, esto es, el campo* $\mathrm{K}' = \{\alpha \in \mathrm{F} \mid \alpha \text{ es algebraico sobre } \mathrm{K}\}$*, se le llama el campo de constantes de* F *.*

Notemos que F/K′ también es un campo de funciones, con la propiedad adicional de que cualquier elemento $x \in \mathrm{F} \setminus \mathrm{K}$ es trascendente y $[\mathrm{K}' : \mathrm{K}]$ es finito. En adelante, a menos que se diga lo contrario, se supondrá siempre que $\mathrm{K} = \mathrm{K}'$, es decir, cuando digamos un campo de funciones F/K, supondremos que el campo de constantes de F es K.

DEFINICIÓN 1.3 *Un anillo de valuación del campo de funciones* F/K *es un anillo* $\mathcal{O} \subseteq \mathrm{F}$ *con las siguientes propiedades:*
(*a*) $\mathrm{K} \subsetneq \mathcal{O} \subsetneq \mathrm{F}$, *y*
(*b*) *para todo* $x \in \mathrm{F}$, $x \in \mathcal{O}$ *o* $x^{-1} \in \mathcal{O}$.

PROPOSICIÓN 1.4 *Sea* $\mathcal{O}$ *un anillo de valuación del campo de funciones* F/K. *Entonces* $\mathcal{O}$ *es un anillo local, es decir,* $\mathcal{O}$ *tiene un único ideal maximal* $\mathrm{P} = \mathcal{O} \setminus \mathcal{O}^*$, *donde* $\mathcal{O}^* = \{x \in \mathcal{O} \mid \text{existe un } y \in \mathcal{O} \text{ con } xy = 1\}$ *es el grupo de unidades de* $\mathcal{O}$.

TEOREMA 1.5 *Sea* $\mathcal{O}$ *un anillo de valuación del campo de funciones* F/K *y* P *su único ideal maximal. Entonces*
(*a*) P *es principal.*
(*b*) *Si* $\mathrm{P} = t\mathcal{O}$ *entonces cualquier* $x \in \mathrm{F}$, $x \neq 0$, *tiene una única representación de la forma* $x = t^n u$ *para algún* $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$.
(*c*) $\mathcal{O}$ *es un dominio de ideales principales. Más precisamente, si* $\mathrm{P} = t\mathcal{O}$ *y* $\{0\} \neq \mathrm{I} \subsetneq \mathcal{O}$ *es un ideal, entonces* $\mathrm{I} = t^n\mathcal{O}$ *para algún* $n \in \mathbb{N}$.

Un anillo con las propiedades del teorema anterior es llamado *anillo de valuación discreta.*

DEFINICIÓN 1.6 *Un lugar* P *del campo de funciones* F/K *es el ideal maximal de algún anillo de valuación* $\mathcal{O}$ *de* F/K. *Cualquier elemento* $t \in \mathrm{P}$ *tal que* $\mathrm{P} = t\mathcal{O}$ *es llamado un elemento primo.*

Para una campo de funciones F/K, sea $\mathbb{P}_\mathrm{F}$ o simplemente $\mathbb{P}$ en caso de no haber confusión posible, el conjunto de todos los lugares de F, esto es,

$$\mathbb{P}_\mathrm{F} = \{\mathrm{P} \mid \mathrm{P} \text{ es un lugar de F}\}.$$

Si $\mathcal{O}$ es un anillo de valución de F/K y P es su ideal maximal, entonces $\mathcal{O}$ está unívocamente determinado por P, a saber $\mathcal{O} = \{x \in \mathrm{F} \mid x^{-1} \notin \mathrm{P}\}$. Entonces $\mathcal{O}_\mathrm{P} = \mathcal{O}$ es llamado el *anillo de valuación del lugar* P.

DEFINICIÓN 1.7 *Una valuación discreta de* F/K *es una función* $v : \mathrm{F} \to \mathbb{Z} \cup \{\infty\}$ *con las siguientes propiedades:*
(*a*) $v(x) = \infty$ *si y sólo si* $x = 0$.
(*b*) $v(xy) = v(x) + v(y)$ *para cualquier* $x, y \in \mathrm{F}$.

(*c*) $v(x+y) \geq \min\{v(x), v(y)\}$ *para cualquier* $x, y \in \mathrm{F}$.
(*d*) *Existe un elemento* $x \in \mathrm{F}$ *con* $v(x) = 1$.
(*e*) $v(a) = 0$ *para cualquier* $a \in \mathrm{K}$, $a \neq 0$.

En este contexto, el símbolo ∞ representa a un elemento que no está en $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = n + \infty = \infty$ y $\infty > m$ para $n, m \in \mathbb{Z}$.
Cada lugar $\mathrm{P} \in \mathbb{P}_\mathrm{F}$ define una función $v_\mathrm{P} : \mathrm{P} \to \mathbb{Z} \cup \{\infty\}$ de la siguiente manera: Primero escojamos un elemento primo t para P. Entonces todo $x \in \mathrm{F}$, $x \neq 0$, se representa de manera única como $x = t^n u$ con $u \in \mathcal{O}_\mathrm{P}^*$ y $n \in \mathbb{Z}$. Definimos $v_\mathrm{P}(x) = n$ y $v_\mathrm{P}(0) = \infty$. Esta definición no depende de la elección de t.

Teorema 1.8 *Sea* F/K *un campo de funciones.*
(*a*) *Para cualquier lugar* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$*, la función* v_P *es una valuación discreta de* F/K*. Más aún, tenemos que* $\mathcal{O}_\mathrm{P} = \{x \in \mathrm{F} \,|\, v_\mathrm{P}(x) \geq 0\}$, $\mathcal{O}_\mathrm{P}^* = \{x \in \mathrm{F} \,|\, v_\mathrm{P}(x) = 0\}$ *y* $\mathrm{P} = \{x \in \mathrm{F} \,|\, v_\mathrm{P}(x) > 0\}$.
(*b*) *Inversamente, supongamos que* v *es una valuación discreta de* F/K*. Entonces el conjunto* $\mathrm{P} = \{x \in \mathrm{F} \,|\, v(x) > 0\}$ *es un lugar de* F/K*, y* $\mathcal{O}_\mathrm{P} = \{x \in \mathrm{F} \,|\, v(x) \geq 0\}$ *es su anillo de valuación correspondiente.*
(*c*) *Cualquier anillo de valuación* $\mathcal{O}$ *de* F/K *es un subanillo maximal propio de* F.

De acuerdo al teorema anterior los lugares, anillos de valuación y valuaciones discretas de un campo de funciones representan esencialmente un mismo objeto.

Sea P un lugar de F/K y $\mathcal{O}_\mathrm{P}$ su anillo de valuación. Ya que P es un ideal maximal el anillo cociente $\mathrm{F}_\mathrm{P} = \mathcal{O}_\mathrm{P}/\mathrm{P}$ es un campo al cual le llamaremos *campo residual*. El mapeo de clases residuales $\mathcal{O}_\mathrm{P} \to \mathcal{O}_\mathrm{P}/\mathrm{P}$ induce una inyección canónica de K en F_P. Por lo cual nosotros trataremos a K como un subcampo de F_P y entonces podemos definir el *grado* de P como $\deg(\mathrm{P}) = [\mathrm{F}_\mathrm{P} : \mathrm{K}]$. El grado de un lugar siempre es finito.

Proposición 1.9 *Si* P *es un lugar de* F/K *y* $0 \neq x \in \mathrm{P}$*, entonces* $\deg(\mathrm{P}) \leq [\mathrm{F} : \mathrm{K}(x)] < \infty$.

Teorema 1.10 *Sea* F/K *un campo de funciones y* R *un subanillo de* F *con* $\mathrm{K} \subseteq \mathrm{R} \subseteq \mathrm{F}$*. Supongamos que* $\{0\} \neq \mathrm{I} \subset \mathrm{R}$ *es un ideal propio de* R*. Entonces existe un lugar* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$ *tal que* $\mathrm{I} \subseteq \mathrm{P}$ *y* $\mathrm{R} \subseteq \mathcal{O}_\mathrm{P}$.

COROLARIO 1.11 *Sea* $\mathrm{F/K}$ *un campo de funciones y* $x \in \mathrm{F}$ *transcendente sobre* K. *Entonces existe al menos un lugar* P *de* F *tal que* $v_{\mathrm{P}}(x) > 0$. *En particular* $\mathbb{P}_{\mathrm{F}} \neq \emptyset$.

DEFINICIÓN 1.12 *Dado un campo de funciones* $\mathrm{F/K}$, *al grupo abeliano libre generado por los elementos de* $\mathbb{P}_{\mathrm{F}}$ *se le llama el grupo de divisores de* F *y será denotado por* D_{F}. *Los lugares reciben también el nombre de divisores primos. El grupo de divisores será escrito multiplicativamente.*

Así, un divisor arbitrario U se escribe de manera única como $\prod_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}}} \mathrm{P}^{v_{\mathrm{P}}(\mathrm{U})}$, donde $v_{\mathrm{P}}(\mathrm{U}) \in \mathbb{Z}$ y $v_{\mathrm{P}}(\mathrm{U}) = 0$ para casi todo P. El divisor unidad, esto es, el divisor $\prod_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}}} \mathrm{P}^0$, se denota por N.

DEFINICIÓN 1.13 *Un divisor* U *se llama entero si* $v_{\mathrm{P}}(\mathrm{U}) \geq 0$ *para todo lugar* P. *Se dice que un divisor* U *divide a otro divisor* B *si existe un divisor entero* C *tal que* $\mathrm{B} = \mathrm{UC}$, *lo cual es equivalente a pedir que* $v_{\mathrm{P}}(\mathrm{B}) \geq v_{\mathrm{P}}(\mathrm{U})$ *para toda* P. *Cuando* U *divide a* B, *denotamos esto por* $\mathrm{U|B}$.

DEFINICIÓN 1.14 *Dos divisores* U, B *se llaman primos relativos o coprimos si* $v_{\mathrm{P}}(\mathrm{U}) \neq 0$ *implica que* $v_{\mathrm{P}}(\mathrm{B}) = 0$.

DEFINICIÓN 1.15 *Sea* U *un divisor. Definimos el grado de* U, *el cual será denotado por* $\deg_{\mathrm{F}}(\mathrm{U})$ *o* $\deg(\mathrm{U})$ *en caso de no haber confusión, por* $\deg_{\mathrm{F}}(\mathrm{U}) = \sum_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}}} f_{\mathrm{P}} v_{\mathrm{P}}(\mathrm{U})$, *donde* $\mathrm{U} = \prod_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}}} \mathrm{P}^{v_{\mathrm{P}}(\mathrm{U})}$ *y* $f_{\mathrm{P}} = \deg(\mathrm{P})$.

DEFINICIÓN 1.16 *Sea* U *un divisor de* $\mathrm{F/K}$. *Denotemos por* $L_{\mathrm{F}}(\mathrm{U})$ *o* $L(\mathrm{U})$ *al conjunto* $L_{\mathrm{F}}(\mathrm{U}) = \{x \in \mathrm{F} \mid v_{\mathrm{P}}(x) \geq v_{\mathrm{P}}(\mathrm{U})$ *para toda* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}\}$.

Se tiene que $L(\mathrm{U})$ es un K-espacio vectorial y que si $\mathrm{U|B}$, $L(\mathrm{B}) \subseteq L(\mathrm{U})$. La dimensión de $L_{\mathrm{F}}(\mathrm{U})$ sobre K la denotaremos por $\dim(\mathrm{U}) = \ell(\mathrm{U})$.

LEMA 1.17 *En un campo de funciones algebraicas* $\mathrm{F/K}$ *se cumple lo siguiente:*
(*a*) $L(\mathrm{N}) = \mathrm{K}$.
(*b*) *Si* U *es entero y diferente de* N, *entonces* $L(\mathrm{U}) = 0$.

TEOREMA 1.18 *Sea* $x \in \mathrm{F}^*$, *entonces existe solamente un número finito de lugares* P *tales que* $v_{\mathrm{P}}(x) \neq 0$.

DEFINICIÓN 1.19 *Dado $x \in \mathrm{F}^*$, se define el divisor principal de x en* F *por* $(x)_{\mathrm{F}} = \prod_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}}} \mathrm{P}^{v_{\mathrm{P}}(x)}$. *Si no hay lugar a confusión, escribiremos* (x) *en lugar de* $(x)_{\mathrm{F}}$.

Un divisor U es *principal* si $\mathrm{U} = (x)_{\mathrm{F}}$ para algún $x \in \mathrm{F}^*$.

LEMA 1.20 (*a*) *Sean* U, U′ *divisores con* $\mathrm{U} = (x)_{\mathrm{F}}\mathrm{U}'$ *para algún* $x \in \mathrm{F}^*$. *Entonces se tiene que* $\dim(\mathrm{U}) = \dim(\mathrm{U}')$ *y* $\deg(\mathrm{U}) = \deg(\mathrm{U}')$.
(*b*) *Para un divisor* U *de grado cero, las siguientes condiciones son equivalentes:*
(1) U *es principal.*
(2) $\dim(\mathrm{U}) \geq 1$.
(3) $\dim(\mathrm{U}) = 1$.

Las demostraciones de los siguientes resultados, hasta el Corolario 1.49, se encuentran en el Capítulo 3 de [15].

DEFINICIÓN 1.21 *Dado $x \in \mathrm{F}^*$, se define el divisor de ceros* Z_x *de* x *como* $\mathrm{Z}_x = \prod_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}},\, v_{\mathrm{P}}(x)>0} \mathrm{P}^{v_{\mathrm{P}}(x)}$ *y el divisor de polos* N_x *como* $\mathrm{N}_x = \prod_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}},\, v_{\mathrm{P}}(x)<0} \mathrm{P}^{-v_{\mathrm{P}}(x)}$.

Notemos que los divisores Z_x, N_x son divisores enteros y que $(x)_{\mathrm{F}} = \mathrm{Z}_x\mathrm{N}_x^{-1}$.

PROPOSICIÓN 1.22 *El conjunto de divisores principales es un subgrupo de* D_{F}. *Este subgrupo se denota por* P_{F} *y se le llama el subgrupo de los divisores principales. Al cociente* $C_{\mathrm{F}} = D_{\mathrm{F}}/P_{\mathrm{F}}$ *se le llama el grupo completo de clases de divisores.*

Denotemos por $\sim$ a la relación de equivalencia canónica utilizada para definir el grupo cociente C_{F}.

TEOREMA 1.23 *Cualquier divisor principal tiene grado cero. Más precisamente: Sea* $x \in \mathrm{F} \setminus \mathrm{K}$ *y* Z_x (*resp.* N_x) *el divisor de ceros* (*resp. divisor de polos*) *de* x. *Entonces* $\deg \mathrm{N}_x = \deg \mathrm{Z}_x = [\mathrm{F} : \mathrm{K}(x)]$.

DEFINICIÓN 1.24 *Se define el grado de una clase* $C \in C_{\mathrm{F}}$ *por* $\deg(C) = \deg(\mathrm{U})$, *donde* U *es cualquier divisor que pertenece a* C.

Debido al Teorema 1.23 la definición anterior no depende del elemento $\mathrm{U} \in C$

PROPOSICIÓN 1.25 *Sea* $x \in \mathrm{F}$ *un elemento transcendente. Entonces existe un entero* $a \in \mathbb{Z}$ *que depende sólo de* x *tal que* $\ell(\mathrm{N}_x^{-m}) + \deg(\mathrm{N}_x^{-m}) \geq a$ *para toda* $m \in \mathbb{Z}$.

TEOREMA (RIEMANN) 1.26 *Sea x un elemento transcendente del campo de funciones* F/K *y sea* $1-g = \sup\{a \,|\, \ell(\mathrm{N}_x^{-m}) + \deg(\mathrm{N}_x^{-m}) \geq a \text{ para toda } m \in \mathbb{Z}\}$. *Entonces para cualquier divisor* $\mathrm{U} \in D_\mathrm{F}$, $\ell(\mathrm{U}) + \deg(\mathrm{U}) \geq 1-g$.

COROLARIO 1.27 *El número* $1-g$ *es la máxima cota inferior de* $\{\ell(\mathrm{U})+\deg(\mathrm{U}) \,|\, \mathrm{U} \in D_\mathrm{F}\}$ *y también de* $\{\ell(\mathrm{N}_z^{-m}) + \deg(\mathrm{N}_z^{-m}) \,|\, m \in \mathbb{Z}\}$ *para cualquier* $z \in \mathrm{F} \setminus \mathrm{K}$. *En particular,* $1-g$ *es independiente de* z.

DEFINICIÓN 1.28 *El número* $g = g_\mathrm{F}$ *recibe el nombre de género del campo* F.

PROPOSICIÓN 1.29 *Se tiene que* $g \geq 0$.

DEFINICIÓN 1.30 *Sea* $C \in C_\mathrm{F}$. *Se define la dimensión de la clase* C *por* $N(C) = \ell(\mathrm{U}^{-1})$, $\mathrm{U} \in C$ *cualquiera.*

DEFINICIÓN 1.31 *Una repartición es una función* $\varphi : \mathbb{P}_\mathrm{F} \to \mathrm{F}$ *tal que* $v_\mathrm{P}(\varphi(\mathrm{P})) \geq 0$ *para casi toda* P.

Equivalentemente, una repartición ξ es una sucesión $\xi = \{\xi_\mathrm{P}\}_{\mathrm{P}\in\mathbb{P}_\mathrm{F}} \in \prod_{\mathrm{P}\in\mathbb{P}_\mathrm{F}} \mathrm{F}$ tal que $\xi_\mathrm{P} \in \mathcal{O}_\mathrm{P}$ para casi toda P, donde $\mathcal{O}_\mathrm{P}$ denota el anillo de valuación de v_P. El conjunto de todas las reparticiones de F lo denotaremos por Λ_F o Λ en caso de ser claro el campo de referencia F.

PROPOSICIÓN 1.32 *El conjunto* Λ_F *es una* K*-álgebra, esto es,* Λ_F *es un* K*-espacio vectorial y a su vez un anillo con sus operaciones entrada por entrada, es decir, para* $a \in \mathrm{K}$, $\xi, \theta \in \Lambda_\mathrm{F}$ *se definen:* $(a\xi)_\mathrm{P} = a\xi_\mathrm{P}$; $(\xi+\theta)_\mathrm{P} = \xi_\mathrm{P} + \theta_\mathrm{P}$; $(\xi\theta)_\mathrm{P} = \xi_\mathrm{P}\theta_\mathrm{P}$.

La función $\phi : \mathrm{F} \to \Lambda$, dada por $\phi(x) = \xi_x$, donde $(\xi_x)_\mathrm{P} = x$ para toda P, es un monomorfismo, por lo que bajo esta inyección supondremos $\mathrm{F} \subseteq \Lambda$.

PROPOSICIÓN 1.33 *Para un lugar* P, *la valuación* v_P *se extiende a* Λ *de la siguiente forma:* $v_\mathrm{P}(\xi) = v_\mathrm{P}(\xi_\mathrm{P})$, $\xi \in \Lambda$. *Esta extensión satisface las mismas condiciones que sobre* F. *Para cualesquiera* $\xi, \theta \in \Lambda$*:* 1) $v_\mathrm{p}(\xi+\theta) \geq \mín\{v_\mathrm{P}(\xi), v_\mathrm{P}(\theta)\}$; 2) $v_\mathrm{P}(\xi\theta) = v_\mathrm{P}(\xi) + v_\mathrm{P}(\theta)$; 3) $v_\mathrm{P}(\xi_x) = v_\mathrm{P}(x)$ *para toda* $x \in \mathrm{F}$.

DEFINICIÓN 1.34 *Sea* $\mathrm{U} \in D_\mathrm{F}$, $\xi \in \Lambda_\mathrm{F}$. *Se dice que* U *divide a* ξ *o que* ξ *es divisible por* U *si* $v_\mathrm{P}(\xi) \geq v_\mathrm{P}(\mathrm{U})$ *para cualquier* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$, *y se denota* $\mathrm{U}|\xi$.

DEFINICIÓN 1.35 *Sea* $\mathrm{U} \in D_{\mathrm{F}}$*, se define* $\Lambda(\mathrm{U}) = \{\xi \in \Lambda \mid \mathrm{U}|\xi\}$.

Se tiene que $\Lambda(\mathrm{U})$ es un K-espacio vectorial.

DEFINICIÓN 1.36 *Sea* F/K *un campo de funciones. Una diferencial* (*o diferencial de Weil*) ω *en* F *es una función* K*-lineal,* $\omega : \Lambda_{\mathrm{F}} \to \mathrm{K}$ *tal que existe un divisor* $\mathrm{U} \in D_{\mathrm{F}}$ *con la propiedad de que* $\mathrm{F} + \Lambda(\mathrm{U}^{-1}) \subseteq \ker \omega$*. En este caso decimos que* U *divide a* ω *y ponemos* $\mathrm{U}|\omega$.

DEFINICIÓN 1.37 *Una diferencial* ω *en un campo de funciones* F/K *se llama de primer tipo o diferencial holomorfa si* $\mathrm{N}|\omega$.

PROPOSICIÓN 1.38 *Sean* U *y* B *divisores tales que* $\mathrm{B}|\mathrm{U}$*. Si* $\mathrm{U}|\omega$*, entonces se tiene* $\mathrm{B}|\omega$.

PROPOSICIÓN 1.39 *Sea* U *un divisor en* F *y definimos*

$$D(\mathrm{U}) = \{\omega \mid \omega \text{ es una diferencial tal que } \mathrm{U}|\omega\}.$$

Entonces $D(\mathrm{U})$ *es un* K*-espacio vectorial y* $\dim_{\mathrm{K}} D(\mathrm{U}) = \delta(\mathrm{U}) = \ell(\mathrm{U}^{-1}) + \deg(\mathrm{U}^{-1}) - 1 + g$.

COROLARIO 1.40 *La dimensión del* K*-espacio vectorial de las diferenciales holomorfas* $D(\mathrm{N})$ *es el género del campo* F.

PROPOSICIÓN 1.41 Dif_{F}*, el conjunto de las diferenciales sobre* F*, es un* F*-espacio vectorial con la operación:* $(x\omega)(\xi) = \omega(x\xi)$*,* $x \in \mathrm{F}$*,* $\omega \in Dif_{\mathrm{F}}$*,* $\xi \in \Lambda$*. Más aún, si* $\mathrm{U}|\omega$*, y* $x \neq 0$*, entonces* $(x)_{\mathrm{F}}\mathrm{U}|x\omega$.

TEOREMA 1.42 *Sea* $\omega_0 \in Dif_{\mathrm{F}}$*,* $\omega_0 \neq 0$*. Entonces toda diferencial* ω *puede escribirse de manera única como* $\omega = x\omega_0$ *para algún* $x \in \mathrm{F}$*. En particular* $\dim_{\mathrm{F}} Dif_{\mathrm{F}} = 1$.

A cada diferencial $\omega \neq 0$ se le asigna un divisor único:

TEOREMA 1.43 *Para cada diferencial* $\omega \neq 0$*, existe un único divisor, el cual denotaremos por* $(\omega)_{\mathrm{F}}$ *tal que* $\mathrm{U}|\omega$ *si y sólo si* $\mathrm{U}|(\omega)_{\mathrm{F}}$.

El divisor $(\omega)_{\mathrm{F}}$ es el *divisor asociado* a la diferencial ω .

COROLARIO 1.44 *Si* $x \in \mathrm{F}^*$, $\omega \in Dif_{\mathrm{F}}$, $\omega \neq 0$, *entonces* $(x\omega)_{\mathrm{F}} = (x)_{\mathrm{F}}(\omega)_{\mathrm{F}}$.

El Corolario 1.44 tiene como consecuencia importante que el conjunto de divisores de las diferenciales no cero forman una clase en C_{F}.

DEFINICIÓN 1.45 *A la clase* C *que consiste de los divisores de las diferenciales no cero de un campo de funciones se le llama la clase canónica y se denota por* $\mathrm{W} = \mathrm{W}_{\mathrm{F}}$.

TEOREMA (RIEMANN-ROCH) 1.46 *Sea* F/K *un campo de funciones y sea* $C \in C_{\mathrm{F}}$ *una clase cualquiera. Sea* W *la clase canónica y* g *el género de* F. *Entonces*

$$N(C) = \deg(C) - g + 1 + N(\mathrm{W}C^{-1}).$$

Equivalentemente, si U *es cualquier divisor y* ω *es cualquier diferencial diferente de cero, se tiene*

$$\ell(\mathrm{U}^{-1}) = \deg(\mathrm{U}) - g + 1 + \ell((\omega)_{\mathrm{F}}^{-1}\mathrm{U}).$$

En otras palabras se tiene que

$$\delta(\mathrm{U}) = \ell(\mathrm{U}^{-1}) + \deg(\mathrm{U}^{-1}) + g - 1 = \ell((\omega)_{\mathrm{F}}^{-1}\mathrm{U}) = N(\mathrm{W}C^{-1})$$

para $\mathrm{U} \in C$.

COROLARIO 1.47 *Sea* W *la clase canónica. Entonces* $N(\mathrm{W}) = g$, $\deg(\mathrm{W}) = 2g - 2$.

COROLARIO 1.48 *Si* U *es un divisor arbitrario tal que* $\deg(\mathrm{U}) > 2g - 2$ *ó* $\deg(\mathrm{U}) = 2g - 2$ *y* $\mathrm{U} \notin \mathrm{W}$, *entonces* $\ell(\mathrm{U}^{-1}) = \deg(\mathrm{U}) - g + 1$ *y en particular* $\ell(\mathrm{U}^{-1}) \geq g - 1$.

COROLARIO 1.49 *Sea* P *un divisor primo y sea* $n > 2g-1$ ($n > 0$ *si* $g = 0$). *Entonces existe un elemento* $x \in \mathrm{F}$ *tal que* $\mathrm{N}_x = \mathrm{P}^n$.

PROPOSICIÓN 1.50 *Para un campo de funciones* F/K *las siguientes condiciones son equivalentes:*

(*a*) F/K *es de funciones racionales, es decir* $\mathrm{F} = \mathrm{K}(x)$ *para algún elemento* x *trascendente sobre* K.

(*b*) F/K *tiene género cero, y existe algún divisor* $\mathrm{A} \in D_{\mathrm{F}}$ *con* $\deg \mathrm{A} = 1$.

DEFINICIÓN 1.51 *Sea* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$.
(*a*) *Para* $x \in \mathrm{F}$ *sea* $\iota_\mathrm{P}(x) \in \Lambda_\mathrm{F}$ *la repartición cuya* P *componente es* x, *y las otras son cero.*
(*b*) *Para una diferencial* $\omega \in Dif_\mathrm{F}$ *definimos su componente local* $\omega_\mathrm{P} : \mathrm{F} \to \mathrm{K}$ *por* $\omega_\mathrm{P}(x) = \omega(\iota_\mathrm{P}(x))$. *De hecho* $\omega_\mathrm{P} : \Lambda_\mathrm{F} \to \mathrm{K}$, $\omega_\mathrm{P}(\xi) := \omega(\xi_\mathrm{P})$.

PROPOSICIÓN 1.52 *Sea* $\omega \in Dif_\mathrm{F}$ *y* $\xi = (\xi_\mathrm{P}) \in \Lambda$. *Entonces* $\omega_\mathrm{P}(\xi_\mathrm{P}) \neq 0$ *para a lo más una cantidad finita de lugares* P *y* $\omega(\xi) = \sum_{\mathrm{P} \in \mathbb{P}_\mathrm{F}} \omega_\mathrm{P}(\xi_\mathrm{P})$.

PROPOSICIÓN 1.53 *En el campo de funciones racionales* $\mathrm{F} = \mathrm{K}(x)$ *se cumple lo siguiente:*
(*a*) *El divisor* P_∞^{-2} *es canónico.*
(*b*) *Existe una única diferencial* $\omega \in Dif_{\mathrm{K}(x)}$ *con* $(\omega) = \mathrm{P}_\infty^{-2}$ *y* $\omega_{\mathrm{P}_\infty}(x^{-1}) = -1$.
(*c*) ω *está determinada por las condiciones* $\omega(\Lambda(\mathrm{P}_\infty^2) + \mathrm{F}) = 0$, $\omega_{\mathrm{P}_\infty}(x^{-1}) = -1$.
(*d*) *Las componente locales de la diferencial* ω *de* (*b*) *satisfacen:* $\omega_{\mathrm{P}_\infty}((x-a)^n) = 0$ *cuando* $n \neq -1$, *y es* -1 *si* $n = -1$; $\omega_{\mathrm{P}_a}((x-a)^n) = 0$ *cuando* $n \neq -1$, *y es* 1 *si* $n = -1$.

1.2. Extensiones de Campos de Funciones

DEFINICIÓN 1.54 *Sean* F/K *y* F'/K' *dos campos de funciones. Se dice que* F' *es una extensión de* F *si* $\mathrm{F} \subseteq \mathrm{F}'$ *y además* $\mathrm{K}' \cap \mathrm{F} = \mathrm{K}$. *Si* F'/F *es algebraica diremos que la extensión de campos de funciones es algebraica.*

DEFINICIÓN 1.55 *Consideremos una extensión algebraica* F'/K' *de* F/K. *Decimos que un lugar* $\mathrm{P}' \in \mathbb{P}_{\mathrm{F}'}$ *está sobre* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$ (*ó* P' *es una extensión de* P) *si* $\mathrm{P} \subseteq \mathrm{P}'$ *y lo denotamos como* $\mathrm{P}'|\mathrm{P}$.

PROPOSICIÓN 1.56 *Sea* F'/K' *una extensión de* F/K. *Entonces las siguientes condiciones son equivalentes:*
(*a*) $[\mathrm{K}' : \mathrm{K}] < \infty$.
(*b*) $[\mathrm{F}' : \mathrm{F}] < \infty$.
(*c*) *Si* P' *es cualquier lugar de* F' *sobre un lugar* P *de* F, *entonces* $[\mathrm{F}'_{\mathrm{P}'} : \mathrm{F}_\mathrm{P}] < \infty$

DEMOSTRACIÓN Ver [15]

PROPOSICIÓN 1.57 *Sea* F'/K' *una extensión de* F/K. *Entonces las siguientes condiciones son equivalentes:*
(*a*) K' *es algebraico sobre* K.
(*b*) F' *es algebraico sobre* F.
(*c*) *Si* P' *es cualquier lugar de* F' *sobre un lugar* P *de* F, $\mathrm{F}'_{\mathrm{P}'}$ *es algebraico sobre* F_{P}.

DEMOSTRACIÓN Ver [15]

PROPOSICIÓN 1.58 *Sea* F'/K' *una extensión algebraica de* F/K. *Supongamos que* P (*resp.* P') *es un lugar de* F (*resp.* F'), *sea* $\mathcal{O}_{\mathrm{P}}$ (*resp.* $\mathcal{O}_{\mathrm{P}'}$) *su anillo de valuación correspondiente y* v_{P} (*resp.* $v_{\mathrm{P}'}$) *la valuación discreta correspondiente. Entonces las siguientes afirmaciones son equivalentes:*
(*a*) $\mathrm{P}'|\mathrm{P}$.
(*b*) $\mathcal{O}_{\mathrm{P}} \subseteq \mathcal{O}_{\mathrm{P}'}$.
(*c*) *Existe un entero* $e \geq 1$ *tal que* $v_{\mathrm{P}'}(x) = ev_{\mathrm{P}}(x)$ *para todo* $x \in \mathrm{P}$.
Más aún, si $\mathrm{P}'|\mathrm{P}$ *entonces* $\mathrm{P} = \mathrm{P}' \cap \mathrm{F}$ *y* $\mathcal{O}_{\mathrm{P}} = \mathcal{O}_{\mathrm{P}'} \cap \mathrm{F}$. *Por esta razón a* P *también se le llama la restricción de* P' *a* F.

DEFINICIÓN 1.59 *Sea* F'/K' *una extensión algebraica de* F/K *y sea* P' *un lugar de* F'/K' *que está sobre* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$.
(*a*) *Al entero positivo* $e(\mathrm{P}'|\mathrm{P}) = e$ *tal que* $v_{\mathrm{P}'}(x) = ev_{\mathrm{P}}(x)$ *para todo* $x \in \mathrm{P}$ *le llamamos el índice de ramificación de* P' *sobre* P. *Decimos que* $\mathrm{P}'|\mathrm{P}$ *es ramificada si* $e(\mathrm{P}'|\mathrm{P}) > 1$ *y no ramificada si* $e(\mathrm{P}'|\mathrm{P}) = 1$.
(*b*) $f(\mathrm{P}'|\mathrm{P}) = [\mathrm{F}'_{\mathrm{P}'} : \mathrm{F}_{\mathrm{P}}]$ *es llamado el grado relativo de* P' *sobre* P.

PROPOSICIÓN 1.60 *Sea* F'/K' *una extensión algebraica de* F/K *y sea* P' *un lugar de* F'/K' *que está sobre* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$. *Entonces*
(*a*) $f(\mathrm{P}'|\mathrm{P}) < \infty$ *si y sólo si* $[\mathrm{F}' : \mathrm{F}] < \infty$.
(*b*) *Si* $\mathrm{F}''/\mathrm{K}''$ *una extensión algebraica de* F'/K' *y* $\mathrm{P}'' \in \mathbb{P}_{\mathrm{F}''}$ *es una extensión de* P', *entonces* $e(\mathrm{P}''|\mathrm{P}) = e(\mathrm{P}''|\mathrm{P}')e(\mathrm{P}'|\mathrm{P})$ *y* $f(\mathrm{P}''|\mathrm{P}) = f(\mathrm{P}''|\mathrm{P}')f(\mathrm{P}'|\mathrm{P})$.

PROPOSICIÓN 1.61 *Sea* F'/K' *una extensión algebraica de* F/K.
(*a*) *Para cualquier lugar* $\mathrm{P}' \in \mathbb{P}_{\mathrm{F}'}$ *existe un único lugar* P *de* F *tal que* $\mathrm{P}'|\mathrm{P}$, *a saber* $\mathrm{P} = \mathrm{P}' \cap \mathrm{F}$.
(*b*) *Para cualquier lugar* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *existe al menos una extensión* $\mathrm{P}' \in \mathbb{P}_{\mathrm{F}'}$ *y la cantidad de dichas extensiones es finita.*

DEFINICIÓN 1.62 *Sea* F'/K' *una extensión algebraica de* F/K *y* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$. *Definimos la conorma de* P (*con respecto a* F'/F) *como* $Con_{\mathrm{F}'/\mathrm{F}}(\mathrm{P}) = \prod_{\mathrm{P}'|\mathrm{P}}(\mathrm{P}')^{e(\mathrm{P}'|\mathrm{P})}$. *Esto se extiende a un homomorfismo de* D_{F} *a* $D_{\mathrm{F}'}$: $Con_{\mathrm{F}'/\mathrm{F}}(\prod \mathrm{P}^{n_{\mathrm{P}}}) = \prod Con_{\mathrm{F}'/\mathrm{F}}(\mathrm{P})^{n_{\mathrm{P}}}$.

TEOREMA 1.63 *Sea* F'/K' *una extensión de* F/K (*finita o infinita*). *Sea* P *un lugar de* F *y sean* $\mathrm{P}'_1, \ldots, \mathrm{P}'_h$ *los lugares de* F' *sobre* P. *Entonces*

$$[\mathrm{F}' : \mathrm{F}] = \sum_{i=1}^{h} e(\mathrm{P}'_i|\mathrm{P}) f(\mathrm{P}'_i|\mathrm{P}).$$

COROLARIO 1.64 *Sea* F'/K' *una extensión finita de* F/K *y* $\mathrm{A} \in D_{\mathrm{F}}$. *Entonces*

$$\deg(Con_{\mathrm{F}'/\mathrm{F}}(\mathrm{A})) = \frac{[\mathrm{F}' : \mathrm{F}]}{[\mathrm{K}' : \mathrm{K}]} \deg(\mathrm{A}).$$

PROPOSICIÓN 1.65 *Sea* M/L *una extensión finita y separable. Consideremos una base* $\{x_1, \ldots, x_n\}$ *de* M/L. *Entonces existen* $x_1^*, \ldots, x_n^* \in \mathrm{M}$, *tales que* $Tr_{\mathrm{M}/\mathrm{L}}(x_i x_j^*) = \delta_{ij}$ (δ_{ij} *es el símbolo de Kronecker*). *El conjunto* $\{x_1^*, \ldots, x_n^*\}$ *es una base de* M/L *llamada la base dual de* $\{x_1, \ldots, x_n\}$ *con respecto a la traza.*

TEOREMA 1.66 *Sea* F'/K' *una extensión finita y separable del campo de funciones* F/K *y* P *un lugar de éste. Entonces la cerradura entera* $\mathcal{O}'_{\mathrm{P}}$ *de* $\mathcal{O}_{\mathrm{P}}$ *en* F' *es* $\mathcal{O}'_{\mathrm{P}} = \cap_{\mathrm{P}'|\mathrm{P}} \mathcal{O}_{\mathrm{P}'}$. *Existe una base* $\{x_1, \ldots, x_n\}$ *de* F'/F *tal que* $\mathcal{O}'_{\mathrm{P}} = \bigoplus_{i=1}^{n} \mathcal{O}_{\mathrm{P}} x_i$. *A la base* $\{x_1, \ldots, x_n\}$ *le llamamos base entera de* $\mathcal{O}'_{\mathrm{P}}$ *sobre* $\mathcal{O}_{\mathrm{P}}$ (*o una base entera local de* F'/F *para el lugar* P).

1.3. El Diferente

1.3.1. La Cotraza y La Fórmula del Género de Hurwitz

En esta sección las hipótesis generales son: F/K es un campo de funciones algebraicas con campo de constantes K, F'/F es una extensión finita y separable donde K' es el campo de constantes de F'.

DEFINICIÓN 1.67 *Para* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$, *denotemos por* $\mathcal{O}'_{\mathrm{P}}$ *a la cerradura entera de* $\mathcal{O}_{\mathrm{P}}$ *en* F'. *Al conjunto* $\mathcal{C}_{\mathrm{P}} = \{z \in \mathrm{F}' | Tr_{\mathrm{F}'/\mathrm{F}}(z \cdot \mathcal{O}'_{\mathrm{P}}) \subseteq \mathcal{O}_{\mathrm{P}}\}$ *le llamaremos el módulo complementario sobre* $\mathcal{O}_{\mathrm{P}}$.

PROPOSICIÓN 1.68 *Utilizando la notación de la definición anterior, se tiene lo siguiente:*
(a) $\mathcal{C}_{\mathrm{P}}$ *es un* $\mathcal{O}'_{\mathrm{P}}$*-módulo y* $\mathcal{O}'_{\mathrm{P}} \subseteq \mathcal{C}_{\mathrm{P}}$.
(b) Si $\{z_1, \ldots, z_n\}$ *es una base entera de* $\mathcal{O}'_{\mathrm{P}}$ *sobre* $\mathcal{O}_{\mathrm{P}}$*, entonces* $\mathcal{C}_{\mathrm{P}} = \sum_{i=1}^{n} \mathcal{O}_{\mathrm{P}} \cdot z_i^*$*, donde* $\{z_1^*, \ldots, z_n^*\}$ *es la base dual de* $\{z_1, \ldots, z_n\}$.
(c) Existe un elemento $t \in \mathrm{F}'$*, que depende de* P*, tal que* $\mathcal{C}_{\mathrm{P}} = t \cdot \mathcal{O}'_{\mathrm{P}}$*. Más aún,* $v_{\mathrm{P}'}(t) \leq 0$ *para toda* $\mathrm{P}'|\mathrm{P}$*, y si* $t' \in \mathrm{F}'$*, entonces* $\mathcal{C}_{\mathrm{P}} = t' \cdot \mathcal{O}'_{\mathrm{P}}$ *si y sólo si* $v_{\mathrm{P}'}(t') = v_{\mathrm{P}'}(t)$ *para toda* $\mathrm{P}'|\mathrm{P}$.
(d) $\mathcal{C}_{\mathrm{P}} = \mathcal{O}'_{\mathrm{P}}$ *para casi todo* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$.

DEFINICIÓN 1.69 *Consideremos un lugar* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *y la cerradura entera* $\mathcal{O}'_{\mathrm{P}}$ *de* $\mathcal{O}_{\mathrm{P}}$ *en* F'*. Sea* $\mathcal{C}_{\mathrm{P}} = t \cdot \mathcal{O}'_{\mathrm{P}}$ *el módulo complementario sobre* $\mathcal{O}_{\mathrm{P}}$*. Se define el exponente diferente de* P' *sobre* P *por* $d(\mathrm{P}'|\mathrm{P}) = -v_{\mathrm{P}'}(t)$.

Por la Proposición 1.68, $d(\mathrm{P}'|\mathrm{P})$ está bien definido y $d(\mathrm{P}'|\mathrm{P}) \geq 0$. Además $d(\mathrm{P}'|\mathrm{P}) = 0$ para casi todo $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ y $\mathrm{P}'|\mathrm{P}$, pues $\mathcal{C}_{\mathrm{P}} = 1 \cdot \mathcal{O}'_{\mathrm{P}}$ para casi todo $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$. Por lo tanto podemos definir el divisor $Diff_{\mathrm{F}'/\mathrm{F}} = \prod_{\mathrm{P} \in \mathbb{P}_{\mathrm{F}}} \prod_{\mathrm{P}'|\mathrm{P}} (\mathrm{P}')^{d(\mathrm{P}'|\mathrm{P})}$. Este divisor es llamado el $diferente$ de F'/F.

Sea $\Lambda_{\mathrm{F}'/\mathrm{F}} = \{\xi \in \Lambda_{\mathrm{F}'} | \xi_{\mathrm{P}'} = \xi_{\mathrm{Q}'}$ siempre que $\mathrm{P}' \cap \mathrm{F} = \mathrm{Q}' \cap \mathrm{F}\}$. $\Lambda_{\mathrm{F}'/\mathrm{F}}$ es un F'-subespacio de $\Lambda_{\mathrm{F}'}$. La traza $Tr_{\mathrm{F}'/\mathrm{F}} : \mathrm{F}' \to \mathrm{F}$ pude ser extendida a una transformación F-lineal (también denotada por $Tr_{\mathrm{F}'/\mathrm{F}}$) de $\Lambda_{\mathrm{F}'/\mathrm{F}}$ a Λ_{F} definiendo su p-componente de la siguiente manera $(Tr_{\mathrm{F}'/\mathrm{F}}(\xi))_{\mathrm{P}} = Tr_{\mathrm{F}'/\mathrm{F}}(\xi_{\mathrm{P}'})$, $\xi \in \Lambda_{\mathrm{F}'/\mathrm{F}}$, y P' es cualquier lugar de F' que está sobre P.

TEOREMA 1.70 *Para toda diferencial* ω *de* F/K*, existe una única diferencial* ω' *de* F'/K' *tal que* $Tr_{\mathrm{K}'/\mathrm{K}}(\omega'(\xi)) = \omega(Tr_{\mathrm{F}'/\mathrm{F}}(\xi))$ *para toda* $\xi \in \Lambda_{\mathrm{F}'/\mathrm{F}}$*. Esta diferencial es llamada la cotraza de* ω *en* F'/F*, y será denotada por* $Cotr_{\mathrm{F}'/\mathrm{F}}(\omega)$*. Si* $\omega \neq 0$ *y* $(\omega) \in D_{\mathrm{F}}$ *es el divisor de* ω*, entonces* $Cotr_{\mathrm{F}'/\mathrm{F}}(\omega) = Con_{\mathrm{F}'/\mathrm{F}}((\omega)) Diff_{\mathrm{F}'/\mathrm{F}}$.

COROLARIO 1.71 *Para una torre* $\mathrm{F} \subseteq \mathrm{F}' \subseteq \mathrm{F}''$ *de extensiones separables finitas, tenemos lo siguiente:*
(a) $Diff_{\mathrm{F}''/\mathrm{F}} = Con_{\mathrm{F}''/\mathrm{F}'}(Diff_{\mathrm{F}'/\mathrm{F}}) Diff_{\mathrm{F}''/\mathrm{F}'}$.
(b) $d(\mathrm{P}''|\mathrm{P}) = e(\mathrm{P}''|\mathrm{P}')d(\mathrm{P}'|\mathrm{P}) + d(\mathrm{P}''|\mathrm{P}')$*, si* P'' *(resp.* P'*,* P*) es un lugar de* F'' *(resp.* F'*,* F*) con* $\mathrm{P}''|\mathrm{P}'$ *y* $\mathrm{P}'|\mathrm{P}$.

Teorema (Fórmula del Género de Hurwitz) 1.72 *Sea* F/K *un campo de funciones algebraicas de género* g *y* F'/F *una extensión finita y separable. Sea* K' *el campo de constantes de* F' *y* g' *el género de* F'/K'. *Entonces se tiene que*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg Dif f_{F'/F}.$$

1.3.2. Ramificación

En esta sección consideraremos una extensión finita y separable F'/F donde F/K, resp. F'/K' son campos de funciones con campos de constantes K resp. K'. También suponemos que K es perfecto.

Teorema del Diferente de Dedekind 1.73 *Sean* P *un lugar de* F *y* $P' \in \mathbb{P}_{F'}$ *una extensión de* P. *Entonces tenemos que*
(*a*) $d(P'|P) \geq e(P'|P) - 1$.
(*b*) $d(P'|P) = e(P'|P) - 1$ *si y sólo si* $e(P'|P)$ *no es divisible por car*(K).

Definición 1.74 *Sean* F'/F *una extensión algebraica de campos de funciones y* $P \in \mathbb{P}_F$.

(*a*) *Una extensión* P' *de* P *en* F *se dice moderadamente* (*resp. salvajemente*) *ramificada si* $e(P'|P) > 1$ *y car*(K) *no divide a* $e(P'|P)$ (*resp. car*(K) *divide a* $e(P'|P)$).

(*b*) *Decimos que* P *se ramifica* (*resp. no se ramifica*) *en* F'/F *si existe al menos un* $P' \in \mathbb{P}_{F'}$ *sobre* P *tal que* $P'|P$ *es ramificada* (*resp. si toda extensión* $P'|P$ *no es ramificada*). *El lugar* P *es moderadamente ramificado en* F'/F *si es ramificado en* F'/F *y no existe una extensión de* P *en* F' *que sea salvajemente ramificada. Si existe al menos una extensión* $P'|P$ *salvajemente ramificada nosotros diremos que* P *es salvajemente ramificado en* F'/F.

(*c*) P *es totalmente ramificado en* F'/F *si existe sólo una extensión* P' *de* P *en* F' *y el índice de ramificación es* $e(P'|P) = [F' : F]$.

(*d*) F'/F *es ramificada* (*resp. no ramificada*) *si al menos un* $P \in \mathbb{P}_F$ *se ramifica en* F'/F (*resp. si todo* $P \in \mathbb{P}_F$ *no se ramifica en* F'/F).

(*e*) F'/F *se dice moderada* (*o moderadamente ramificada*) *si no hay lugares* $P \in \mathbb{P}_F$ *que sean salvajemente ramificados en* F'/F.

Corolario 1.75 *Sea* F'/F *una extensión finita y separable de campos de funciones.*
(*a*) *Sean* $P \in \mathbb{P}_F$ *y* $P' \in \mathbb{P}_{F'}$ *tales que* $P'|P$, *entonces* $P'|P$ *es ramificada si y sólo si*

$\mathrm{P}'|Diff_{\mathrm{F}'/\mathrm{F}}$.
Si $\mathrm{P}'|\mathrm{P}$ *es ramificada,* $d(\mathrm{P}'|\mathrm{P}) = e(\mathrm{P}'|\mathrm{P}) - 1$ *si y sólo si* $\mathrm{P}'|\mathrm{P}$ *es moderadamente ramificada,* $d(\mathrm{P}'|\mathrm{P}) \geq e(\mathrm{P}'|\mathrm{P})$ *si y sólo si* $\mathrm{P}'|\mathrm{P}$ *es salvajemente ramificada.*
(*b*) *Casi todos los lugares de* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *no se ramifican en* F'/F.

Corolario 1.76 *Supongamos que* F'/F *es una extensión finita y separable de campos de funciones con el mismo campo de constantes. Denotemos por* g (*resp.* g') *al género de* F (*resp.* F′). *Entonces* $g \leq g'$.

Corolario 1.77 *Sea* $\mathrm{F}/\mathrm{K}(x)$ *una extensión finita y separable de un campo de funciones racionales de grado mayor que* 1 *tal que* K *es el campo de constantes de* F. *Entonces* $\mathrm{F}/\mathrm{K}(x)$ *es ramificada.*

Teorema 1.78 *Supongamos que* $\mathrm{F}' = \mathrm{F}(y)$ *es una extensión finita y separable de un campo de funciones* F *de grado* $[\mathrm{F}' : \mathrm{F}] = n$. *Sea* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *tal que el polinomio mínimo* $\varphi(T)$ *de* y *sobre* F *tiene coeficientes en* $\mathcal{O}_{\mathrm{P}}$ *y sean* $\mathrm{P}_1, \ldots, \mathrm{P}_r$ *todos los lugares de* F′ *que están encima de* P. *Entonces se tiene lo siguiente:*
(*a*) $d(\mathrm{P}_i|\mathrm{P}) \leq v_{\mathrm{P}_i}(\varphi'(y))$ *para* $1 \leq i \leq r$.
(*b*) $\{1, y, \ldots, y^{n-1}\}$ *es una base entera de* F'/F *en el lugar* P *si y sólo si* $d(\mathrm{P}_i|\mathrm{P}) = v_{\mathrm{P}_i}(\varphi'(y))$ *para* $1 \leq i \leq r$.
$\varphi'(T)$ *denota la derivada de* $\varphi(T)$ *en el anillo de polinomios* $\mathrm{F}[T]$.

1.4. Extensiones de Galois

Decimos que una extensión F'/K' de un campo de funciones F/K es de Galois si F'/F es una extensión de Galois.

Lema 1.79 *Sea* F^*/F *una extensión algebraica de campos de funciones,* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *y* $\mathrm{P}^* \in \mathbb{P}_{\mathrm{F}^*}$ *con* $\mathrm{P}^*|\mathrm{P}$. *Consideremos un automorfismo* σ *de* F^*/F. *Entonces* $\sigma(\mathrm{P}^*) = \{\sigma(x)|x \in \mathrm{P}^*\}$ *es un lugar de* F*, y además*
(*a*) $v_{\sigma(\mathrm{P}^*)}(y) = v_{\mathrm{P}^*}(\sigma^{-1}(y))$ *para todo* $y \in \mathrm{P}^*$.
(*b*) $\sigma(\mathrm{P}^*)|\mathrm{P}$.
(*c*) $e(\sigma(\mathrm{P}^*)|\mathrm{P}) = e(\mathrm{P}^*|\mathrm{P})$ *y* $f(\sigma(\mathrm{P}^*)|\mathrm{P}) = f(\mathrm{P}^*|\mathrm{P})$.

Sea P un lugar de F/K. Entonces $G(\mathrm{F}'/\mathrm{F})$ (el grupo de F-automorfismos de F′) actúa sobre el conjunto de todas las extensiones $\mathrm{P}' \in \mathbb{P}_{\mathrm{F}'}$ de P vía $\sigma(\mathrm{P}') = \{\sigma(x)|x \in \mathrm{P}'\}$.

TEOREMA 1.80 *Sea* F'/K' *una extensión de Galois de* F/K *y* $\mathrm{P}_1, \mathrm{P}_2 \in \mathbb{P}_{\mathrm{F}'}$ *extensiones de* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$. *Entonces* $\mathrm{P}_2 = \sigma(\mathrm{P}_1)$ *para alguna* $\sigma \in G(\mathrm{F}'/\mathrm{F})$. *En otras palabras, el grupo de Galois actúa transitivamente sobre el conjunto de extensiones de* P.

COROLARIO 1.81 *La notación es como en el Teorema 1.80. Sean* $\mathrm{P}_1, \ldots, \mathrm{P}_h$ *todos los lugares de* F' *que están sobre* P. *Entonces se tiene que:*
(a) $e(\mathrm{P}_i|\mathrm{P}) = e(\mathrm{P}_j|\mathrm{P})$ *y* $f(\mathrm{P}_i|\mathrm{P}) = f(\mathrm{P}_j|\mathrm{P})$ *para toda* i, j.
(b) $[\mathrm{F}' : \mathrm{F}] = e(\mathrm{P}_i|\mathrm{P}) f(\mathrm{P}_i|\mathrm{P}) h$.
(c) $d(\mathrm{P}_i|\mathrm{P}) = d(\mathrm{P}_j|\mathrm{P})$ *para toda* i, j.

PROPOSICIÓN 1.82 *Sea* F/K *un campo de funciones en el cual* K *contiene a una* n*-ésima raíz primitiva de la unidad con* $n > 1$ *y* n *primo relativo con la característica de* K. *Supongamos que* $u \in \mathrm{F}$ *cumple con:* $u \neq w^d$ *para todo* $w \in \mathrm{F}$ *y* $d|n$, $d > 1$. *Sea* $\mathrm{F}' = \mathrm{F}(y)$ *con* $y^n = u$. *Entonces*

(a) El polinomio mínimo de y *sobre* F *es* $\mathrm{T}^n - u$. *La extensión* F'/F *es de Galois de grado* n *y su grupo de Galois es cíclico.*

(b) Sea $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *y* $\mathrm{P}' \in \mathbb{P}_{\mathrm{F}'}$ *una extensión de* P. *Entonces* $e(\mathrm{P}'|\mathrm{P}) = \frac{n}{r_{\mathrm{P}}}$ *y* $d(\mathrm{P}'|\mathrm{P}) = \frac{n}{r_{\mathrm{P}}} - 1$, *donde* $r_{\mathrm{P}} = (n, v_{\mathrm{P}}(u))$.

(c) Si K' *denota al campo de constantes de* F' *y* g *(resp.* g'*) el género de* F *(resp.* F'*), entonces*

$$g' = 1 + \frac{n}{[\mathrm{K}' : \mathrm{K}]} \left(g - 1 + \frac{1}{2} \sum_{\mathrm{P} \in \mathbb{P}_{\mathrm{F}}} \left(1 - \frac{r_{\mathrm{P}}}{n}\right) \deg \mathrm{P} \right).$$

LEMA 1.83 *Sea* F/K *un campo de funciones algebraicas de característica* $p > 0$. *Dado un elemento* $u \in \mathrm{F}$ *y un lugar* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$, *se cumple lo siguiente:*
(a) existe un elemento $z \in \mathrm{F}$ *tal que* $v_{\mathrm{P}}(u - (z^p - z)) \geq 0$, *o*
(b) para algún $z \in \mathrm{F}$, $v_{\mathrm{P}}(u - (z^p - z)) = -m < 0$ *con* $m \not\equiv 0 \bmod p$.
En el último caso, el entero m *está unívocamente determinado por* u *y* P, *a saber* $-m = max\{v_{\mathrm{P}}(u - (w^p - w)) | w \in \mathrm{F}\}$.

PROPOSICIÓN 1.84 *Sea* F/K *una extensión algebraica de campos de funciones de característica* $p > 0$. *Supongamos que* $u \in \mathrm{F}$ *satisface la siguiente condición:* $u \neq w^p - w$ *para todo* $w \in \mathrm{F}$. *Sea* $\mathrm{F}' = \mathrm{F}(y)$ *con* $y^p - y = u$. *Para* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ *definimos un*

entero m_{P} *como* m *si existe un elemento* $z \in \mathrm{F}$ *tal que* $v_{\mathrm{P}}(u-(z^p-z)) = -m < 0$ *y* $m \not\equiv 0 \bmod p$, *como* -1 *si* $v_{\mathrm{P}}(u-(z^p-z)) \geq 0$ *para algún* $z \in \mathrm{F}$. *Entonces tenemos lo siguiente:*
(*a*) P *es no ramificado en* F'/F *si y sólo si* $m_{\mathrm{P}} = -1$.
(*b*) P *es ramificado en* F'/F *si y sólo si* $m_{\mathrm{P}} > 0$. *Denotemos por* P' *al único lugar de* F' *que está sobre* P. *Entonces el exponente diferente* $d(\mathrm{P}'/\mathrm{P})$ *está dado por* $d(\mathrm{P}'/\mathrm{P}) = (p-1)(m_{\mathrm{P}}+1)$.
(*c*) *Si al menos un lugar* Q *de* F *satisface* $m_{\mathrm{Q}} > 0$, *entonces* K *es algebraicamente cerrado en* F' *y*

$$g' = p \cdot g + \frac{p-1}{2}\left(-2 + \sum_{\mathrm{P} \in \mathbb{P}_{\mathrm{F}}} (m_{\mathrm{P}}+1)\deg \mathrm{P}\right),$$

donde g' (*resp.* g) *es el género de* F'/K *y* (*resp.* F/K).

Sea F'/F una extensión de Galois de campos de funciones con grupo de Galois $G = G(\mathrm{F}'/\mathrm{F})$. Tomemos un lugar P de F y P' una extensión de P en F'.

Definición 1.85 (*a*) $G_Z(\mathrm{P}'|\mathrm{P}) = \{\sigma \in G | \sigma(\mathrm{P}') = \mathrm{P}'\}$ *es llamado el grupo de descomposición de* P' *sobre* P.
(*b*) $G_T(\mathrm{P}'|\mathrm{P}) = \{\sigma \in G | v_{\mathrm{P}'}(\sigma(z)-z) > 0$ *para todo* $z \in \mathcal{O}_{\mathrm{P}'}\}$ *es llamado el grupo de inercia de* $\mathrm{P}'|\mathrm{P}$.
(*c*) *El campo fijo* $Z = Z(\mathrm{P}'|\mathrm{P})$ *de* $G_Z(\mathrm{P}'|\mathrm{P})$ *es llamado el campo de descomposición de* $\mathrm{P}'|\mathrm{P}$, *el campo fijo* $T = T(\mathrm{P}'|\mathrm{P})$ *de* $G_T(\mathrm{P}'|\mathrm{P})$ *es llamado el campo de inercia de* P' *sobre* P.

$G_Z(\mathrm{P}'|\mathrm{P})$ y $G_T(\mathrm{P}'|\mathrm{P})$ son subgrupos de G con $G_T(\mathrm{P}'|\mathrm{P}) \subseteq G_Z(\mathrm{P}'|\mathrm{P})$.

Teorema 1.86 (*a*) *El orden del grupo de descomposición es* $e(\mathrm{P}'|\mathrm{P}) \cdot f(\mathrm{P}'|\mathrm{P})$.
(*b*) *El grupo de inercia es un subgrupo normal de* $G_Z(\mathrm{P}'|\mathrm{P})$ *de orden* $e(\mathrm{P}'|\mathrm{P})$.
(*c*) *La extensión de campos residuales* $\mathrm{F}'_{\mathrm{P}'}/\mathrm{F}_{\mathrm{P}}$ *es de Galois. Cualquier automorfismo* $\sigma \in G_Z(\mathrm{P}'|\mathrm{P})$ *induce un automorfismo* $\bar{\sigma}$ *de* $\mathrm{F}'_{\mathrm{P}'}$ *sobre* F_{P} *de la siguiente manera:* $\bar{\sigma}(z(\mathrm{P}')) = \sigma(z)(\mathrm{P}')$ *para* $z \in \mathcal{O}_{\mathrm{P}'}$. *La correspondencia* $\sigma \mapsto \bar{\sigma} \in G(\mathrm{F}'_{\mathrm{P}'}/\mathrm{F}_{\mathrm{P}})$, *es un homomorfismo suprayectivo cuyo kernel es el grupo de inercia. En particular,* $G(\mathrm{F}'_{\mathrm{P}'}/\mathrm{F}_{\mathrm{P}})$ *es isomorfo a* $G_Z(\mathrm{P}'|\mathrm{P})/G_T(\mathrm{P}'|\mathrm{P})$.
(*d*) *Sea* P_Z (*resp.* P_T) *la restricción de* P' *al campo de descomposición* (*resp. al campo*

de inercia). Entonces: $e(\mathrm{P}'|\mathrm{P}_T) = e(\mathrm{P}'|\mathrm{P}) = [\mathrm{F}' : T]$ *y* $f(\mathrm{P}'|\mathrm{P}_T) = 1$*;* $f(\mathrm{P}_T|\mathrm{P}_Z) = f(\mathrm{P}'|\mathrm{P}) = [T : Z]$ *y* $e(\mathrm{P}_T|\mathrm{P}_Z) = 1$*;* $e(\mathrm{P}_Z|\mathrm{P}) = f(\mathrm{P}_Z|\mathrm{P}) = 1$.

Teorema 1.87 *Consideremos una extensión de Galois* F'/F *de campos de funciones, un lugar* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$ *y una extensión* P' *de* P *en* F'*. Para un campo intermedio* $\mathrm{F} \subseteq \mathrm{M} \subseteq \mathrm{F}'$ *denotemos por* P_M *a la restricción de* P' *a* M*. Entonces tenemos que*
(*a*) $\mathrm{M} \subseteq Z(\mathrm{P}'|\mathrm{P})$ *si y sólo si* $e(\mathrm{P}_\mathrm{M}|\mathrm{P}) = f(\mathrm{P}_\mathrm{M}|\mathrm{P}) = 1$.
(*b*) $\mathrm{M} \supseteq Z(\mathrm{P}'|\mathrm{P})$ *si y sólo si* P' *es el único lugar de* F' *que está sobre* P_M.
(*c*) $\mathrm{M} \subseteq T(\mathrm{P}'|\mathrm{P})$ *si y sólo si* $e(\mathrm{P}_\mathrm{M}|\mathrm{P}) = 1$.
(*d*) $\mathrm{M} \supseteq T(\mathrm{P}'|\mathrm{P})$ *si y sólo si* P_M *es totalmente ramificado en* F'/M.

Definición 1.88 *Sea* F'/F *una extensión de Galois de campos de funciones con grupo de Galois* $G = G(\mathrm{F}'/\mathrm{F})$*. Tomemos un lugar* $\mathrm{P} \in \mathrm{F}$ *y una extensión* P' *de* P *en* F'*. Para cada* $i \geq -1$ *se define el* i*-ésimo grupo de ramificación de* $\mathrm{P}'|\mathrm{P}$ *por* $G_i(\mathrm{P}'|\mathrm{P}) = \{\sigma \in G \mid v_{\mathrm{P}'}(\sigma(z) - z) \geq i + 1 \text{ para todo } z \in \mathcal{O}_{\mathrm{P}'}\}$.

Cada $G_i(\mathrm{P}'|\mathrm{P})$ es un subgrupo de G. Denotaremos al i-ésimo grupo de ramificación $G_i(\mathrm{P}'|\mathrm{P})$ como G_i.

Proposición 1.89 *Algunas propiedades de los grupos de ramificación son:*
(*a*) $G_{-1} = G_Z(\mathrm{P}'|\mathrm{P})$ *y* $G_0 = G_T(\mathrm{P}'|\mathrm{P})$.
(*b*) $G_{-1} \supseteq G_0 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \cdots$ *y* $G_m = \{1\}$ *para* m *suficientemente grande.*
(*c*) *Sea* $\sigma \in G_0$*,* $i \geq 0$ *y* t *un elemento primo de* P'*. Entonces* $\sigma \in G_i$ *si y sólo* $v_{\mathrm{P}'}(\sigma t - t) \geq i + 1$.
(*d*) *Si* $car(\mathrm{F}) = 0$ *entonces* $G_i = \{1\}$ *para* $i \geq 1$ *y* G_0 *es cíclico.*
(*e*) *Si* $car(\mathrm{F}) = p > 0$ *entonce* G_1 *es un subgrupo normal de* G_0*. El orden de* G_1 *es un potencia de* p *y el grupo cociente* G_0/G_1 *es cíclico cuyo orden es primo relativo con* p.
(*f*) *Si* $car(\mathrm{F}) = p > 0$ *entonces* G_{i+1} *es un subgrupo normal de* G_i *(para* $i \geq 1$*) y* G_i/G_{1+i} *es isomorfo a un subgrupo aditivo del campo residual* $\mathrm{F}_{\mathrm{P}'}$.

Teorema (Fórmula del Diferente de Hilbert) 1.90 *Tomemos una extensión de Galois* F'/F *de campos de funciones, un lugar* $\mathrm{P} \in \mathbb{P}_\mathrm{F}$ *y u lugar* $\mathrm{P}' \in \mathbb{P}_{\mathrm{F}'}$ *que esté sobre* P*. Entonces el exponente diferente* $d(\mathrm{P}'|\mathrm{P})$ *es*

$$d(\mathrm{P}'|\mathrm{P}) = \sum_{i=0}^{\infty} (ord\, G_i(\mathrm{P}'|\mathrm{P}) - 1).$$

Por el inciso (b) de la Proposición 1.89 la suma anterior es una suma finita.

1.5. Campos de Funciones Elípticas

En esta sección K denota a un perfecto.

DEFINICIÓN 1.91 *Un campo de funciones algebraicas* F/K *se dice que es un campo de funciones elípticas si cumple con las siguientes condiciones:*

(*a*) *el género de* F *es uno, y*

(*b*) *existe un divisor* $P \in \mathbb{P}_F$ *de grado uno.*

PROPOSICIÓN 1.92 *Sea* F/K *un campo de funciones elípticas.*

(*a*) *Si* $car(K) \neq 2$, *existen* $x, y \in F$ *tales que* $F = K(x, y)$ *y*

$$y^2 = f(x) \in K[x] \tag{1}$$

donde $f(x)$ *es un polinomio libre de cuadrados de grado* 3.

(*b*) *Si* $car(K) = 2$, *existen* $x, y \in F$ *tales que* $F = K(x, y)$ *y*

$$y^2 + y = f(x) \in K[x] \ \ con \ \ \deg f(x) = 3, \ \ o \tag{2}$$

$$y^2 + y = x + \frac{1}{ax + b} \ \ con \ \ a, b \in K \ \ y \ \ a \neq 0. \tag{3}$$

La siguiente proposición nos dice que la ecuaciones (1), (2) y (3) definen a un campo de funciones elípticas.

PROPOSICIÓN 1.93 (*a*) $car(F) \neq 2$. *Supongamos que* $F = K(x, y)$ *con* $y^2 = f(x) \in K[x]$, *donde* $f(x)$ *es un polinomio libre de cuadrados de grado* 3. *Consideremos la descomposición* $f(x) = c\prod_{i=1}^{r} p_i(x)$ *de* $f(x)$ *en polinomios mónicos irreducibles* $p_i(x) \in K[x]$ *con* $0 \neq c \in K$. *Denotemos por* $Q_i \in \mathbb{P}_{K(x)}$ *al lugar de* $K(x)$ *que le corresponde a* $p_i(x)$ *y por* Q_∞ *al polo de* x. *Entonces tenemos lo siguiente:*

(1) K *es el campo de constantes de* F *y* F/K *es un campo de funciones elípticas.*

(2) *La extensión* $\mathrm{F}/\mathrm{K}(x)$ *es cíclica de grado* 2. *Los lugares* $\mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *y* Q_∞ *son ramificados en* F*; cada uno de ellos tiene sólo una extensión en* F*, digamos* $\mathrm{P}_1, \ldots, \mathrm{P}_r$ *y* P_∞. *Además* $e(\mathrm{P}_i|\mathrm{Q}_i) = e(\mathrm{P}_\infty|\mathrm{Q}_\infty) = 2$, $\deg \mathrm{P}_i = \deg \mathrm{Q}_i$ *y* $\deg \mathrm{P}_\infty = 1$.

(3) $\mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *y* Q_∞ *son los únicos lugares de* $\mathrm{K}(x)$ *que se ramifican en* F*, y el diferente de* F/K *es* $Dif f_{\mathrm{F}/\mathrm{K}} = \mathrm{Q}_1 \cdots \mathrm{Q}_r \mathrm{Q}_\infty$.

(*b*) $car(\mathrm{F}) = 2$. *Supongamos que* $\mathrm{F} = \mathrm{K}(x, y)$ *con*

$$y^2 + y = f(x) \in \mathrm{K}[x] \ \ con \ \ \deg f(x) = 3, \ \ o \tag{1.1}$$

$$y^2 + y = x + \frac{1}{ax + b} \ \ con \ \ a, b \in \mathrm{K} \ \ y \ \ a \neq 0. \tag{1.2}$$

Denotemos por $\mathrm{Q}_\infty \in \mathbb{P}_{\mathrm{K}(x)}$ *al polo de* x *en* $\mathrm{K}(x)$ *y por* $\mathrm{Q}' \in \mathbb{P}_{\mathrm{K}(x)}$ *al cero de* $ax + b$ (*caso (1.2)*). *Entonces se tiene que:*

(1) K *es el campo de constantes de* F *y* F/K *es un campo de funciones elípticas.*

(2) *La extensión* $\mathrm{F}/\mathrm{K}(x)$ *es cíclica de grado* 2. *Los lugares de* $\mathrm{K}(x)$ *ramificados en* F *son* Q_∞*, en el caso (1.1);* Q_∞ *y* Q'*, en el caso (1.2). Sea* P_∞ (*resp.* P') *el lugar de* F *que está sobre* Q_∞ (*resp.* Q'). *Entonces* $\deg \mathrm{P}_\infty = \deg \mathrm{P}' = 1$ *y* $Dif f_{\mathrm{F}/\mathrm{K}} = \mathrm{P}_\infty^4$ *en el caso (1.1),* $Dif f_{\mathrm{F}/\mathrm{K}} = (\mathrm{P}_\infty \mathrm{P}')^2$ *en el caso (1.2).*

Proposición 1.94 *Sea* F/K *un campo de funciones elípticas. Definimos* $\mathbb{P}_{\mathrm{F}}^{(1)} = \{\mathrm{P} \in \mathbb{P}_{\mathrm{F}} | \deg \mathrm{P} = 1\}$. *Entonces se tiene lo siguiente:*
(*a*) *Para cualquier divisor* A *de* F *con* $\deg \mathrm{A} = 1$*, existe un único lugar* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}^{(1)}$ *con* $\mathrm{A} \sim \mathrm{P}$. *En particular,* $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}^{(1)} \neq \emptyset$.
(*b*) *Fijemos un lugar* $\mathrm{P}_0 \in \mathbb{P}_{\mathrm{F}}^{(1)}$. *Sea* $C_{\mathrm{P}}^0 \subseteq C_{\mathrm{F}}$ *el subgrupo que consiste de las clases de divisores de grado cero. Entonces la función:* $\Phi : \mathbb{P}_{\mathrm{F}}^{(1)} \to C_{\mathrm{F}}^0$, $\mathrm{P} \mapsto [\mathrm{P}\mathrm{P}_0^{-1}]$*, es biyectiva.*

Definición 1.95 *Un campo de funciones hiperelípticas sobre* K *es un campo de funciones algebraicas* F/K *de género* $g \geq 2$ *el cual contiene a un campo de funciones racionales* $\mathrm{K}(x) \subseteq \mathrm{F}$ *con* $[\mathrm{F} : \mathrm{K}(x)] = 2$.

Lema 1.96 (*a*) *Un campo de funciones* F/K *de género* $g \geq 2$ *es hiperelíptico si y sólo si existe un divisor* $\mathrm{A} \in D_{\mathrm{F}}$ *con* $\deg \mathrm{A} = 2$ *y* $dim \mathrm{A} \geq 2$.
(*b*) *Cualquier campo de funciones* F/K *de género* 2 *es hiperelíptico.*

1.6. Extensiones Separablemente Generadas

Sea K un campo perfecto de característica $p > 0$ y F/K un campo de funciones con campo de constantes K. Un elemento $x \in \mathrm{F}$ es llamado *elemento separable* para F/K si $\mathrm{F/K}(x)$ es una extensión separable finita. F/K se dice *separablemente generado* si existe un elemento separable para F/K.

PROPOSICIÓN 1.97 (*a*) *Sea* $z \in \mathrm{F}$ *tal que* $v_{\mathrm{P}}(z) \not\equiv 0 \bmod p$ *para algún* $\mathrm{P} \in \mathbb{P}_{\mathrm{P}}$. *Entonces* z *es un elemento separable para* F/K.
(*b*) *Existen* $x, y \in \mathrm{F}$ *tales que* $\mathrm{F} = \mathrm{K}(x, y)$.
(*c*) *Para* $n \geq 1$, *el conjuto* $\mathrm{F}^{p^n} = \{z^{p^n} \mid z \in \mathrm{F}\}$ *es un subcampo de* F. *Este campo tiene las siguientes propiedades:*
(1) $\mathrm{K} \subseteq \mathrm{F}^{p^n} \subseteq \mathrm{F}$ *y* $\mathrm{F/F}^{p^n}$ *es puramente inseparable de grado* p^n.
(2) *Supongamos que* $\mathrm{K} \subseteq \mathrm{F}_0 \subseteq \mathrm{F}$ *y* $\mathrm{F/F}_0$ *es puramente inseparable de grado* p^n. *Entonces* $\mathrm{F}_0 = \mathrm{F}^{p^n}$.
(*d*) *Un elemento* $z \in \mathrm{F}$ *es un elemento separable para* F/K *si y sólo si* $z \notin \mathrm{F}^p$.

Capítulo 2

Puntos de Weierstrass

Este capítulo contiene el objetivo principal del presente trabajo, el cual consiste en establecer que en ciertas extensiones cíclicas moderadamente y salvajemente ramificadas los lugares totalmente ramificados son puntos de Weierstrass.

2.1. La Sucesión Laguna de un Lugar

Definición 2.1 *Sea* F/K *un campo de funciones y sea* P *un divisor primo de* F. *Un número natural* λ *es llamado un número laguna de* P *si no existe un elemento de* F *para el cual su divisor de polos sea* P^{λ}.

Definición 2.2 *Sea* F/K *una campo de funciones. Un entero positivo* λ *es llamado un número polo de un divisor primo* P *de* F *si* λ *no es número laguna de* P.

Observación. λ es un número polo del divisor primo P si y sólo si $\dim(\mathrm{P}^{-\lambda}) > \dim(\mathrm{P}^{-\lambda+1})$. Equivalentemente λ es un número laguna de P si y sólo si $\ell(\mathrm{P}^{-\lambda}) = \ell(\mathrm{P}^{-\lambda+1})$.
Sea F/K un campo de funciones tal que K es algebraicamente cerrado. Si F tiene género cero la Proposición 1.50 asegura que F es un campo de funciones racionales, entonces todo número natural λ es un número polo de cualquier divisor primo de F. Por otro lado, si $g = 1$, F es un campo de funciones elípticas (ver Definición 1.91), el Lema 2.4 establece que $\lambda = 1$ no es un número polo de todo divisor primo de grado 1 de F.

LEMA 2.3 *Un número natural λ es un número laguna de un divisor primo* P *si y sólo si* $\delta(\mathrm{P}^{\lambda-1}) - \delta(\mathrm{P}^{\lambda}) = \deg(\mathrm{P})$.

DEMOSTRACIÓN
Por el Teorema de Riemann-Roch se tiene que

$$\ell(\mathrm{P}^{-\lambda}) = \deg(\mathrm{P}^{\lambda}) - g + 1 + \ell((\omega)^{-1}\mathrm{P}^{\lambda})$$
$$\ell(\mathrm{P}^{-\lambda+1}) = \deg(\mathrm{P}^{\lambda-1}) - g + 1 + \ell((\omega)^{-1}\mathrm{P}^{\lambda-1}).$$

Entonces

$$\ell((\omega)^{-1}\mathrm{P}^{\lambda-1}) - \ell((\omega)^{-1}\mathrm{P}^{\lambda}) = \deg(\mathrm{P}) + \ell(\mathrm{P}^{-\lambda+1}) - \ell(\mathrm{P}^{-\lambda}) \tag{1}$$

Por la observación anterior y (1) λ es un número laguna de P si y sólo si

$$\ell((\omega)^{-1}\mathrm{P}^{\lambda-1}) - \ell((\omega)^{-1}\mathrm{P}^{\lambda}) = \deg(\mathrm{P}). \tag{2}$$

La demostración se termina si recordamos que $\ell((\omega)^{-1}\mathrm{A})$ es igual a la dimensión $\delta(\mathrm{A})$ de las diferenciales divisibles por A. ■

LEMA 2.4 *Si $g > 0$, cada divisor primo* P *de* F *de grado uno tiene solamente g números laguna y además éstos son menores que $2g$. Más aún $\lambda = 1$ es un número laguna de* P.

DEMOSTRACIÓN
En (1) se tienen las desigualdades $\ell((\omega)^{-1}\mathrm{P}^{\lambda-1}) \geq \ell((\omega)^{-1}\mathrm{P}^{\lambda})$ y $\ell(\mathrm{P}^{-\lambda}) \geq \ell(\mathrm{P}^{-\lambda+1})$. Así que $0 \leq \delta(\mathrm{P}^{\lambda-1}) - \delta(\mathrm{P}^{\lambda}) \leq 1$. Por otro lado se sabe que la dimensión sobre K del espacio de las diferenciales holomorfas es g y que $\delta(\mathrm{A}) = 0$ si $\deg(\mathrm{A}) \geq 2g-1$ o $\deg(\mathrm{A}) = 2g-2$ y $\mathrm{A} \notin \mathrm{W}$ (ver el Corolario 1.48). Entonces supongamos que $\mathrm{P}^{2g-2} \in \mathrm{W}$. Así $(\omega)^{-1}\mathrm{P}^{2g-2}$ es principal para alguna diferencial ω no cero, luego $\ell((\omega)^{-1}\mathrm{P}^{2g-2}) = 1$ por el Lema 1.20. Ahora

$$g = \dim_{\mathrm{K}} D(\mathrm{N}) = \sum_{i=0}^{2g-2} \dim_{\mathrm{K}} \frac{D(\mathrm{P}^i)}{D(\mathrm{P}^{i+1})} + \dim_{\mathrm{K}} D(\mathrm{P}^{2g-2}) \tag{3}$$

con $\dim_{\mathrm{K}} D(\mathrm{P}^{2g-2}) = \ell((\omega)^{-1}\mathrm{P}^{2g-2}) = 1$. Si $\mathrm{P}^{2g-2} \notin \mathrm{W}$ se tiene que

$$g = \dim_{\mathrm{K}} D(\mathrm{N}) = \sum_{i=0}^{2g-j} \dim_{\mathrm{K}} \frac{D(\mathrm{P}^i)}{D(\mathrm{P}^{i+1})} + \dim_{\mathrm{K}} D(\mathrm{P}^{2g-j}) \tag{3a}$$

donde j es el menor natural tal que $\dim_{\mathrm{K}} D(\mathrm{P}^{2g-j}) > 0$, además $\dim_{\mathrm{K}} D(\mathrm{P}^{2g-j}) = 1$, ya que $\dim_{\mathrm{K}} D(\mathrm{P}^{2g-j+1}) = 0$ y $0 \leq \delta(\mathrm{P}^{2g-j}) - \delta(\mathrm{P}^{2g-j+1}) \leq 1$. De (3) y (3a) se concluye que existen solamente g índices i tales que $0 \leq i \leq 2g-2$ y $\delta(\mathrm{P}^i) - \delta(\mathrm{P}^{i+1}) = 1$. Entonces los g enteros $i+1$ son números laguna de P por el Lema 2.3.
Si $\lambda = 1$ es número polo de P existiría $x \in \mathrm{F}$ tal que $\mathrm{N}_x = \mathrm{P}$, entonces aplicando el Teorema 1.23 tenemos que $[\mathrm{F} : \mathrm{K}(x)] = 1$ y por lo tanto $g = 0$, lo cual es una contradicción. ■
Sean $1 = i_1 \leq \cdots \leq i_g \leq 2g-1$ los números laguna de un divisor primo P. A la sucesión finita $i_1, \ldots, i_g$ le llamamos la *sucesión laguna* de P.

LEMA 2.5 *Sea* F/H *una extensión cíclica de campos de funciones de grado* p^n*, con* $n \geq 1$ *y* p *un número primo. Si* E *es el campo intermedio con* $[\mathrm{E} : \mathrm{H}] = p$*, entonces los primos de* H *que se ramifican en* E *son aquéllos que se ramifican totalmente en* F*.*

DEMOSTRACIÓN
Si P es un divisor primo de H ramificado totalmente en F, éste se ramificará en E. Tomemos ahora un divisor primo P de H ramificado en E, entonces $e(\mathrm{P}_1|\mathrm{P}) = p$, donde P_1 es un divisor primo de E que extiende a P. Sea P_2 un divisor primo de F que extienda a P_1. Si suponemos que P_1 no se ramifica totalmente en F $e(\mathrm{P}_2|\mathrm{P}_1) = p^m$, $0 \leq m \leq n-2$. Entonces el Teorema 1.86 implica que $p^{n-m-1} = [G(\mathrm{F}/\mathrm{H}) : G_T(\mathrm{P}_2|\mathrm{P})]$. Además $[G(\mathrm{F}/\mathrm{H}) : G_T(\mathrm{P}_2|\mathrm{P})] = [T(\mathrm{P}_2|\mathrm{P}) : \mathrm{H}]$. Como la extensión es cíclica, lo anterior implica que $\mathrm{E} \subseteq T(\mathrm{P}_2|\mathrm{P})$, y por el Teorema 1.87 $e(\mathrm{P}_1|\mathrm{P}) = 1$ lo cual no es posible. ■

LEMA 2.6 *Sea* F/K *un campo de funciones con* K *algebraicamente cerrado. Sea* $\mathrm{F}/\mathrm{K}(x)$ *una extensión cíclica de grado* p^n*,* $n \geq 1$*, tal que* $G(\mathrm{F}/\mathrm{K}(x)) = \langle\sigma\rangle$*. Entonces el número de divisores primos fijados por* σ *es mayor o igual a uno.*

DEMOSTRACIÓN
Primero veamos que el número de divisores primos fijados por σ es finito. Por el Teorema 1.80, $\langle\sigma\rangle$ actúa transitivamente sobre el conjunto de divisores primos de F que extienden a un divisor primo de $\mathrm{K}(x)$. Entonces como K es algebraicamente cerrado un divisor primo P de F es dejado fijo por σ si y sólo si dicho divisor se ramifica totalmente en $\mathrm{F}/\mathrm{K}(x)$. Pero como sólo una cantidad finita de divisores primos se ramifican el número de divisores primos fijados por σ es finito.
Sea E el subcampo de F tal que $[\mathrm{E} : \mathrm{K}(x)] = p$. Sabemos que $\mathrm{E}/\mathrm{K}(x)$ (ver Corolario

1.77) es ramificada. Tomemos pues un divisor primo Q de K(x) ramificado en E. Por el Lema 2.5 Q se ramifica totalmente en F, entonces el único lugar de F que está sobre Q es fijado por σ. ■

Consideremos un campo de funciones F/K con $g_{\mathrm{F}} > 0$ donde K es algebraicamente cerrado. Sea P un divisor primo de F. Como K es algebraicamente cerrado, P es de grado uno. Así por el Lema 2.4 existen solamente $g = g_{\mathrm{F}}$ números laguna $i_1, \ldots, i_g$ de P tales que $1 = i_1 < \cdots < i_g < 2g$. La sucesión $i_1, \ldots, i_g$ depende de P. En el caso clásico, esto es, cuando K es el campo de los números complejos, la sucesión laguna de P es $1, \ldots, g$ para casi todo lugar P [16]. Todo divisor primo con sucesión laguna $1, \ldots, g$ es llamado *punto ordinario* y el conjunto finito de divisores primos de F con sucesión laguna diferente es llamado el conjunto de *puntos de Weierstrass*.
En el caso de característica positiva Schmidt [11] demuestra que casi todos los lugares de F tienen la misma sucesión laguna. A esta sucesión le llamaremos la *sucesión laguna* de F y a sus elementos les llamaremos *números laguna* de F. La demostración de este importante hecho se basa en la teoría del determinante Wronskiano [16].

Definición 2.7 *Sea* F/K *un campo de funciones con* K *algebraicamente cerrado. Un divisor primo* P *de* F *es llamado un punto de Weierstrass si su sucesión laguna es diferente de la sucesión laguna del campo. Un divisor primo* P *cuya sucesión laguna es igual a la sucesión laguna del campo es llamado un punto ordinario.*

Cuando K es de característica $p > 0$, puede existir un único punto de Weierstrass aunque el género de F sea arbitrariamente grande. En contraste, si la característica es cero existen por lo menos $2g + 2$ puntos de Weierstrass. Notemos que el número de puntos de Weierstrass es finito, ya que casi todos los lugares de F poseen la misma sucesión laguna.
Cuando K no es algebraicamente cerrado, es posible tener dos conjuntos infinitos de divisores primos, cada uno con la misma sucesión laguna pero que estas dos sucesiones sean distintas. También puede suceder que toda sucesión laguna posible ocurra para una infinidad de divisores primos. Por lo anterior, en lo que resta de este capítulo nosotros supondremos que K es algebraicamente cerrado.

LEMA 2.8 *Si $g \leq 1$, F no tiene puntos de Weierstrass.*

DEMOSTRACIÓN
Sea P un divisor primo y supongamos que $g = 1$. Entonces $\delta(\mathrm{A}) = 0$ si $\deg(\mathrm{A}) \geq 2g - 1 = 1$, por lo tanto $g = 1 = \delta(\mathrm{N}) = \delta(\mathrm{P}^0) - \delta(\mathrm{P}^1)$, es decir $\lambda = 1$ es un número laguna de P. Pero para $g = 1$ la sucesión laguna de cada divisor primo consiste a lo más de un elemento, así que todos los primos de F son puntos ordinarios. Supongamos ahora que $g = 0$, entonces $\delta(\mathrm{P}^\lambda) = 0$ para $\lambda \geq 0$, y por el Lema 2.3 la sucesión laguna que le corresponde a cualquier divisor primo es vacía, lo cual implica que, también en este caso, todos los divisores primos son puntos ordinarios. ■

2.2. p-Extensiones Cíclicas

En esta sección supondremos que F/K es un campo de funciones de género $g > 1$ y el campo K es algebraicamente cerrado de característica $p > 0$. Además se hará uso de las siguientes notaciones y resultados.
Sea F/E una extensión cíclica de grado p^n, $n \geq 1$, tal que $G(\mathrm{F/E}) = \langle\sigma\rangle$. Como puede verse en [17], en términos de vectores de Witt (sección A.1), F es generado sobre E por las coordenadas de un vector $y = (y_1, \ldots, y_n)$ el cual es una solución de la ecuación $\pi(y) - y = \beta$, donde $\beta = (\beta_1, \ldots, \beta_n)$ (Teorema A.7). El índice de ramificación de cualquier divisor primo P de F puede ser determinado de β [10]. Si Q es un primo de E divisible por P, se escoge un vector de Witt c tal que el vector $\alpha = \beta + \pi(c) - c$ satisfaga la condición: Para $j = 1, \ldots, n$, $(\alpha_j) = \mathrm{A}_j\mathrm{Q}^{\nu_j}$, con A_j primo relativo a Q y $\nu_j \geq 0$ ó $\nu_j < 0$ y primo relativo con p. Se define $\lambda_j = \max\{-\nu_j, 0\}$. P se ramifica si y sólo si alguno de los λ_j es distinto de cero. Si λ_μ es el primer λ_j no cero, entonces el índice de ramificación es p^e con $e = n + 1 - \mu$. También el exponente de P en el $Diff_{\mathrm{F/E}}$ puede ser calculado de los λ_j. Definimos

$$M_j = \max\{p^{j-\nu}\lambda_\nu | 1 \leq \nu \leq j\}. \tag{4}$$

La fórmula para el exponente diferente es

$$d = (p-1)\sum_{j=\mu}^{n}(M_j + 1)p^{j-\mu}. \tag{5}$$

Denotemos por Q_i, $i = 1, \ldots, s$ a los divisores primos de E totalmente ramificados en F y por P_i al divisor primo de F que divide a Q_i. Finalmente denotemos por $\nu(i, j)$,

$\lambda(i,j)$ y $M(i,j)$ a las cantidades ν_j, λ_j y M_j que le corresponden a P_i.

Cuando F/E es una extensión separable se puede obtener información de los números laguna de divisores primos de F del espacio de diferenciales de E. La relación entre diferenciales de F y E se puede encontrar en [13]. Sea ω_1 una diferencial de E, entonces $\omega = Cotr_{\mathrm{F/E}}\omega_1$ es una diferencial de F, donde $Cotr_{\mathrm{F/E}}$ denota a la cotraza de F/E. La relación entre los divisores de estas diferenciales está dada por

$$(\omega) = Diff_{\mathrm{F/E}}Con_{\mathrm{F/E}}(\omega_1). \tag{6}$$

El lema siguiente da información acerca de los números laguna para divisores primos de F que no se ramifiquen sobre E.

Lema 2.9 *Sea* F/E *una extensión separable con* P *un divisor primo de* F *no ramificado sobre* E *y* P_1 *el divisor primo de* E *divisible por* P. *Sea* A *un divisor de* E *tal que* $Diff_{\mathrm{F/E}}Con_{\mathrm{F/E}}(\mathrm{A})$ *es entero y primo relativo a* P. *Si para un entero positivo* λ, $\delta((\mathrm{P}_1)^{\lambda-1}\mathrm{A}) - \delta((\mathrm{P}_1)^{\lambda}\mathrm{A}) = 1$, *entonces* λ *es un número laguna de* P.

Demostración
Como $\delta((\mathrm{P}_1)^{\lambda-1}\mathrm{A}) - \delta((\mathrm{P}_1)^{\lambda}\mathrm{A}) = 1$, existe una diferencial ω_1 de E tal que $(\omega_1) = (\mathrm{P}_1)^{\lambda-1}\mathrm{AB}$, donde B es un divisor entero primo relativo con P_1. Si $\omega = Cotr_{\mathrm{F/E}}(\omega_1)$, entonces de (6) obtenemos que

$$(\omega) = Diff_{\mathrm{F/E}}Con_{\mathrm{F/E}}((\mathrm{P}_1)^{\lambda-1}\mathrm{AB}).$$

Ya que $Diff_{\mathrm{F/E}}Con_{\mathrm{F/E}}(\mathrm{AB})$ es entero y primo relativo con P, ω es una diferencial holomorfa y el exponente de P en (ω) es $\lambda - 1$. Por lo tanto $\delta(\mathrm{P}^{\lambda-1}) - \delta(\mathrm{P}^{\lambda}) = 1$ y λ es un número laguna de P. ■

Observación. Sea F/E una extensión separable. Si P es un divisor primo de F no ramificado en F/E el divisor $Diff_{\mathrm{F/E}}$ es primo relativo a P. Entonces, suponiendo que A = N del Lema 2.9 deducimos lo siguiente: si λ es un número laguna de $\mathrm{P}|_{\mathrm{E}}$, λ es un número laguna de P. Además, podemos aplicar este resultado cuando E es un campo de funciones racionales, pues el campo de constantes de F es perfecto y por lo tanto F tiene un elemento separable (Proposición 1.97).

LEMA 2.10 *Sea* $\mathrm{F/E}$ *una extensión cíclica de grado* p^n, $n \geq 1$, *tal que* $G(\mathrm{F/E}) = \langle\sigma\rangle$. *Denotemos por* $\mathrm{P}_1, \ldots, \mathrm{P}_s$ *a los divisores primos de* F *totalmente ramificados sobre* E. *Sea* H *el campo fijo de* $\langle\sigma^{p^{n-1}}\rangle$ *y* $\mathrm{R}_1, \ldots, \mathrm{R}_s$ *los divisores primos de* H *divisibles por* $\mathrm{P}_1, \ldots, \mathrm{P}_s$ *respectivamente. Sea* $\bar{d}_i$ *el exponente de* P_i *en el diferente de* $\mathrm{F/H}$. *Entonces* $\sum_{i=1}^{s} \left[\frac{\bar{d}_i}{p}\right] \geq p^n + 1$ *al menos que alguna de las siguientes condiciones se cumpla:*

(A) $n = 2$, $s = 1$, $\lambda(1,1) = 1$;

(B) $n = 3$, $s = 1$, $\lambda(1,1) = 1$, $p = 2$;

(C) $n = 2$, $s = 2$, $\lambda(1,1) = \lambda(2,1) = 1$, $p = 2$.

DEMOSTRACIÓN
Estamos suponiendo que la extensión $\mathrm{F/E}$ está generada por el vector $(\beta_1, \ldots, \beta_n)$. El vector $(\beta_1, \ldots, \beta_{n-1})$ determina una extensión H_1/E de grado p^{n-1} (observación al Teorema A.7). Por otro lado $[\mathrm{H} : \mathrm{E}] = p^{n-1}$. Pero como en las extensiones cíclicas para cada divisor del grado de la extensión existe un único subcampo intermedio, se tiene la igualdad $\mathrm{H}_1 = \mathrm{H}$. Si d'_i es el exponente de R_i en el diferente de $\mathrm{H/E}$, entonces se sigue de (5) que

$$d'_i = (p-1)\sum_{j=1}^{n-1}(M(i,j)+1)p^{j-1}. \tag{7}$$

Sea d_i el exponente diferente de P_i. Por la transitividad del diferente (Corolario 1.71) $\bar{d}_i = d_i - pd'_i$. Entonces de (5) y (7) se obtiene que

$$\begin{aligned}\bar{d}_i &= (p-1)\sum_{j=1}^{n}(M(i,j)+1)p^{j-1} - p(p-1)\sum_{j=1}^{n-1}(M(i,j)+1)p^{j-1} \\ &= (p-1)(M(i,n)+1)p^{n-1} - (p-1)^2\sum_{j=1}^{n-1}(M(i,j)+1)p^{j-1}.\end{aligned}$$

De (4) se sigue que $p^{n-j}M(i,j) = \max\{p^{n-\nu}\lambda(i,\nu) | 1 \leq \nu \leq j\} \leq M(i,n)$. Utilizando

esta desigualdad en la expresión anterior llegamos a

$$\begin{aligned}
\bar{d}_i &\geq (p-1)(M(i,n)+1)p^{n-1} - (p-1)^2 \sum_{j=1}^{n-1} \left(\frac{M(i,n)}{p^{n-j}} + 1 \right) p^{j-1} \\
&= (p-1)(M(i,n)+1)p^{n-1} - \frac{(p-1)^2 M(i,n)}{p^n} \sum_{j=1}^{n-1} p^{2j-1} - (p-1)^2 \sum_{j=1}^{n-1} p^{j-1} \\
&= (p-1)(M(i,n)+1)p^{n-1} - \frac{p(p-1)M(i,n)(p^{2n-2}-1)}{p^n(p+1)} - (p-1)(p^{n-1}-1) \\
&= (p-1)M(i,n)\frac{(p+1)p^{2n-1} - (p^{2n-2}-1)p}{p^n(p+1)} + p - 1 \\
&= (p-1)M(i,n)\frac{p^{2n}+p}{p^n(p+1)} + p - 1.
\end{aligned}$$

Anteriormente vimos que $M(i,n) \geq p^{n-j}M(i,j)$, pero como $M(i,j) \geq \lambda(i,1)$ también se cumple que $M(i,n) \geq p^{n-1}\lambda(i,1)$. Usando ahora la última desigualdad se obtiene lo siguiente

$$\bar{d}_i \geq \frac{(p-1)\lambda(i,1)p^{2n-1}}{p+1} + \frac{(p-1)\lambda(i,1)}{p+1} + p - 1,$$

y entonces

$$\left[\frac{\bar{d}_i}{p} \right] \geq \left[p^n \lambda(i,1) \frac{(p-1)p^{n-2}}{p+1} + \frac{(p-1)\lambda(i,1)}{p(p+1)} + \frac{p-1}{p} \right]. \tag{8}$$

Sea $t = \sum_{i=1}^{s} \left[\frac{\bar{d}_i}{p} \right]$. Para $p \geq 3$ y $n \geq 3$, (8) implica que

$$t \geq \left[\frac{\bar{d}_i}{p} \right] \geq \left[p^n \lambda(i,1) \frac{(p-1)p}{p+1} \right] \geq \left[p^n \frac{3}{2} \right] \geq p^n + 1.$$

Para $p \geq 5$ y $n = 2$, de (8) se tiene que

$$\left[\frac{\bar{d}_i}{p} \right] \geq \left[p^2 \lambda(i,1) \frac{(p-1)}{p+1} \right] \geq \left[p^2 \lambda(i,1) \frac{2}{3} \right] > \frac{2}{3} p^2 \lambda(i,1) - 1. \tag{9}$$

Si para algún i, $\lambda(i,1) \geq 2$, $t > \frac{4}{3}p^2 - 1 > p^2 + 1$. Si $\lambda(i,1) = 1$ para todo i y $s \geq 2$, $t > s(\frac{2}{3}p^2 - 1) \geq \frac{4}{3}p^2 - 2 > p^2 + 1$.

Para $p = 3$ y $n = 2$, (8) implica que

$$\left[\frac{\bar{d}_i}{3}\right] \geq \left[\frac{9}{2}\lambda(i,1) + \frac{\lambda(i,1)}{6} + \frac{2}{3}\right]. \tag{10}$$

Entonces si algún $\lambda(i,1) \geq 2$, $t \geq \left[9 + \frac{1}{3} + \frac{2}{3}\right] = 3^2 + 1$. Si $\lambda(i,1) = 1$ para todo i y $s \geq 2$, $t \geq s\left[\frac{9}{2} + \frac{1}{6} + \frac{2}{3}\right] = 5s \geq 3^2 + 1$.
Para $p = 2$ y $n \geq 4$, de (8) se tiene que

$$t \geq \left[\frac{\bar{d}_i}{2}\right] \geq \left[2^n\frac{4}{3}\lambda(i,1)\right] \geq \left[2^n\frac{4}{3}\right],$$

ahora $3(2^n + 1) \leq 3 \cdot 2^n + 2^n = 2^{n+2}$, entonces $\left[2^n\frac{4}{3}\right] \geq 2^n + 1$.
Para $p = 2$ y $n = 3$, de (8) se tiene que

$$\left[\frac{\bar{d}_i}{2}\right] \geq \left[\frac{16}{3}\lambda(i,1) + \frac{\lambda(i,1)}{6} + \frac{1}{2}\right]. \tag{11}$$

Como $\lambda(i,1)$ debe ser primo relativo con p, ninguno de los $\lambda(i,1)$ es igual a 2. Así, si algún $\lambda(i,1) \geq 3$, $t \geq \left[16 + \frac{1}{2} + \frac{1}{2}\right] = 17 > 2^3 + 1$. Si $\lambda(i,1) = 1$ para todo i y $s \geq 2$, $t \geq s\left[\frac{16}{3} + \frac{1}{6} + \frac{1}{2}\right] = 6s \geq 12 \geq 2^3 + 1$.
Para $p = 2$ y $n = 2$, (8) implica que

$$\left[\frac{\bar{d}_i}{2}\right] \geq \left[\frac{4}{3}\lambda(i,1) + \frac{\lambda(i,1)}{6} + \frac{1}{2}\right]. \tag{12}$$

Si para algún i, $\lambda(i,1) \geq 3$, $t > \left[4 + \frac{1}{2} + \frac{1}{2}\right] = 2^2 + 1$. Si $\lambda(i,1) = 1$ para todo i y $s \geq 3$, $t > s\left[\frac{4}{3} + \frac{1}{6} + \frac{1}{2}\right] \geq 2s \geq 6 \geq 2^2 + 1$. ■

En el siguiente teorema se tomarán las convenciones y notaciones dadas al principio de esta sección, suponiendo además que $\mathrm{E} = \mathrm{K}(x)$.

Teorema 2.11 *Sea* $\mathrm{F}/\mathrm{K}(x)$ *un extensión cíclica de grado* p^n, $n \geq 2$. *Entonces todo divisor primo de* F *que sea totalmente ramificado sobre* $\mathrm{K}(x)$ *es un punto de Weierstrass.*

Demostración
Sean Q_i, $i = i, \ldots, s$ los divisores primos de $\mathrm{K}(x)$ totalmente ramificados en F y sea

P_i el divisor primo de F que divide a Q_i. Para cada Q_i existe un elemento de $\mathrm{K}(x)$ para el cual Q_i es su divisor de polos. En F dicho elemento tiene a P^{p^n}, como su divisor de polos. Es decir p^n no es un número laguna para cualquier P_i.
Sea H el campo fijo de $\langle \sigma^{p^{n-1}} \rangle$ y sean $\mathrm{R}_1, \ldots, \mathrm{R}_s$ los divisores primos de H divisibles por $\mathrm{P}_1, \ldots, \mathrm{P}_s$ respectivamente. Sea $\bar{d}_i$ el exponente de P_i en el diferente de F/H. Consideremos el divisor A de H definido como $\mathrm{A} = \prod_{i=1}^{s} (\mathrm{R}_i)^{a_i}$, donde $a_i = -\left[\frac{\bar{d}_i}{p}\right]$. El grado de A es $-t = -\sum_{i=1}^{s} \left[\frac{\bar{d}_i}{p}\right]$. Además $Diff_{\mathrm{F/H}} Con_{\mathrm{F/H}}(\mathrm{A})$ es un divisor entero de F.
Veamos ahora que los números $1, \ldots, t-1$ forman parte de la sucesión laguna de F. Sea P un divisor primo de F no ramificado sobre H con R el divisor primo de H divisible por P. Si $1 \leq \lambda \leq t-1$, entonces $\deg((\mathrm{A}(\mathrm{R})^{\lambda})^{-1}) = t - \lambda > 0$. El Lema 1.17 nos dice que $\ell((\mathrm{A}(\mathrm{R})^{\lambda})^{-1}) = 0$. Similarmente, $\ell((\mathrm{A}(\mathrm{R})^{\lambda-1})^{-1}) = 0$. La ecuación (1) nos conduce a la igualdad $\delta(\mathrm{A}(\mathrm{R})^{\lambda-1}) - \delta(\mathrm{A}(\mathrm{R})^{\lambda}) = 1$. Por el Lema 2.3, λ es un número laguna de P. Pero como casi todos los divisores primos de F no se ramifican sobre H, se tiene que λ está en la sucesión laguna de F.
Con excepción de los tres casos de Lema 2.10 obtenemos $t \geq p^n + 1$, por lo que p^n está en la sucesión laguna de F y por tanto cada P_i es un punto de Weierstrass, cuando estamos fuera de estos casos.
Consideremos ahora los casos listados en el Lema 2.10. Sea G el campo fijo de σ^p y sean $\mathrm{T}_1, \ldots, \mathrm{T}_s$ los divisores primos de G que son divididos por $\mathrm{P}_1, \ldots, \mathrm{P}_s$ respectivamente. $\mathrm{G}/\mathrm{K}(x)$ es una extensión cíclica de grado p determinada por el vector de Witt (β_1). El exponente diferente $\widetilde{d}$ de T_i está dado por (5), $\widetilde{d} = (p-1)(\lambda(i,1)+1)$. Por el Lema 2.5 los T_i son los únicos divisores primos de G que se ramifican sobre $\mathrm{K}(x)$, y utilizando la fórmula del género de Hurwitz obtenemos

$$g_{\mathrm{G}} = \frac{p-1}{2}\left(\sum_{i=1}^{s}(\lambda(i,1)+1) - 2\right), \tag{13}$$

donde g_{G} es el género de G. En los casos (A) y (B) la igualdad de (13) se reduce a $g_{\mathrm{G}} = 0$, así G es un campo de funciones racionales. Un argumento similar al dado al principio de la prueba demuestra que p^{n-1} no es un número laguna de cualquier P_i. Entonces para probar que los P_i son puntos de Weierstrass es suficiente demostrar que $t \geq p^{n-1} + 1$.

Caso (A). Si $p \geq 5$, de (9) se sigue que

$$t = \left[\frac{\bar{d}_1}{p}\right] > \frac{2}{3}p^2 - 1 \geq 2p - 1 > p + 1.$$

Si $p = 3$, de (10) obtenemos la desigualdad

$$t = \left[\frac{\bar{d}_1}{3}\right] \geq [\frac{9}{2} + \frac{1}{6} + \frac{1}{3}] = 5.$$

Por el Lema 1.96 cuando $p = 2$ el campo F es un campo de funciones hipereliptícas y entonces en [11] encontramos que los puntos de Weierstrass de F son aquellos divisores primos de F que ramifican sobre G.
Caso (B). De (11) se llega a que

$$t = \left[\frac{\bar{d}_1}{2}\right] \geq [\frac{16}{3} + \frac{1}{6} + \frac{1}{2}] = 6.$$

Caso (C). Basta probar que 4 es un número laguna de F, pues 4 es un número polo de los divisores primos ramificados. De (12) se tiene que

$$t = \left[\frac{\bar{d}_1}{2}\right] + \left[\frac{\bar{d}_2}{2}\right] \geq 2[\frac{4}{3} + \frac{1}{6} + \frac{1}{2}] = 4.$$

Cuando $t > 4$ podemos utilizar los argumentos dados al principio para concluir que 4 es un número laguna de F. Así, supongamos que $t = 4$. Entonces $\left[\frac{\bar{d}_1}{2}\right] = \left[\frac{\bar{d}_2}{2}\right] = 2$, pues $\left[\frac{\bar{d}_1}{2}\right], \left[\frac{\bar{d}_2}{2}\right] \geq 2$. Como $n = 2$, H = G, $\mathrm{P}_i = \mathrm{T}_i$, $i = 1, 2$, y $\mathrm{A} = (\mathrm{T}_1\mathrm{T}_2)^{-2}$. Sea P un divisor primo de F no ramificado sobre $\mathrm{K}(x)$. Sea T el divisor primo de G que es divisible por P. El grado de $(\mathrm{T}^3\mathrm{A})^{-1}$ es uno, así $\ell((\mathrm{T}^3\mathrm{A})^{-1}) = 0$. Pero $\deg((\mathrm{T}^4\mathrm{A})^{-1}) = 0$, así $\ell((\mathrm{T}^4\mathrm{A})^{-1}) = 1$ o 0 dependiendo de si $\mathrm{T}^4\mathrm{A}$ es principal o no (ver Lema 1.20). Debido al Lema 2.3 sólo es necesario considerar la situación en la cual $\mathrm{T}^4\mathrm{A}$ es principal, digamos $(z) = \mathrm{T}^4\mathrm{A}$. Sea S otro divisor primo tal que $(z_1) = \mathrm{S}^4\mathrm{A}$, entonces $(zz_1^{-1}) = \mathrm{T}^4\mathrm{S}^{-4}$. Ahora, (13) nos dice que el género de G es uno. Fijemos al divisor primo S, aplicando la Proposición 1.94 cada clase de divisores de grado cero es representada de manera única por un divisor $\mathrm{T}'\mathrm{S}^{-1}$, en el cual T′ es primo. En G existen cuatro clases de divisores para quienes su cuarta potencia es principal [7]. Por lo tanto existe una cantidad infinita de elecciones del divisor primo P en las cuales $\mathrm{T}^4\mathrm{A}$ no es principal. Si éste es el caso $\ell((\mathrm{T}^4\mathrm{A})^{-1}) = 0$, y de (1) se concluye que $\delta(\mathrm{T}^3\mathrm{A}) - \delta(\mathrm{T}^4\mathrm{A}) = 1$. Entonces por el Lema 2.3 cuatro es un número laguna de F. ■

2.2.1. El Caso $n = 1$

Sea K como antes y F/K(x) una extensión cíclica de grado p. Por el Teorema A.6 existe $y \in$ F tal que F = K(x, y) y $y^p - y = \alpha$, $\alpha \in$ K(x). Este tipo de extensiones pueden ser normalizadas de tal manera que la ecuación que las define tome la forma (ver [15]):

$$y^p - y = \frac{f(x)}{\prod_{i=1}^{r}(x - a_i)^{m_i}},$$

donde $a_1, \ldots, a_r$ son elementos distintos de K y $f(x) \in$ K[x] es un polinomio de grado menor que $m = m_1 + \cdots + m_r$; $f(a_i) \neq 0$ y $(m_i, p) = 1$ para cada $i = 1, \ldots, r$.
El siguiente teorema es el caso para $n = 1$ del Teorema 2.11 y fue demostrado por Boseck en [3] (también vea [5]).

TEOREMA 2.12 *Sea* F/K(x) *una extensión cíclica de grado* p *con* K *algebraicamente cerrado de característica* $p > 2$ *y* $g_{\mathrm{F}} \geq 2$. *Entonces todo divisor primo ramificado de* F *es un punto de Weierstrass, excepto si* F = K(x, y) *con* $y^p - y = \alpha$, $\alpha \in$ K(x) *y el divisor de polos de* α *es el producto de dos primos distintos de* K(x).

El lema que sigue es una versión débil del teorema anterior.

LEMA 2.13 *Sea* F/K(x) *una extensión cíclica de grado* p. *Si al menos* $p+1$ *divisores primos de* F *se ramifican, entonces todo divisor primo ramificado de* F *es un punto de Weierstrass.*

DEMOSTRACIÓN
Sean Q_i, $i = 1, \ldots, s$ los divisores primos de K(x) ramificados en F y sea P_i el divisor primo de F que divide a Q_i. Para cada Q_i existe un elemento de K(x) para el cual Q_i es su divisor de polos. En F dicho elemento tiene a P_i^p, como su divisor de polos. Es decir p no es un número laguna para cualquier P_i. Sea d_i el exponente de P_i en el diferente de F/K(x). Sea A un divisor de K(x) definido como $\mathrm{A} = \prod_{i=1}^{s}(\mathrm{Q}_i)^{a_i}$, donde $a_i = -\left[\frac{d_i}{p}\right]$. El grado de A es $-t = -\sum_{i=1}^{s}\left[\frac{d_i}{p}\right]$. Por los argumentos dados al principio de la demostración del Teorema 2.11, $1, \ldots, t-1$ son números laguna de F. Veamos que $t \geq p+1$. Se tiene que $d_i = (p-1)(m_i+1)$ con $m_i \geq 1$ (Proposición 1.84), luego $\left[\frac{d_i}{p}\right] = \left[\frac{(p-1)(m_i+1)}{p}\right] \geq 1$, por lo tanto $t \geq p+1$, pues $s \geq p+1$. ■

Para $p = 2$ y $n = 1$ se cumple el siguiente Lema, el cual es un caso particular de la Proposición 3.22.

LEMA 2.14 *Sean* K *un campo algebraicamente cerrado de característica* $p = 2$ *y* $\mathrm{F}/\mathrm{K}(x)$ *una extensión de grado dos. Si* $g_{\mathrm{F}} \geq 2$*, entonces todo divisor primo de* F *ramificado es un punto de Weierstrass.*

DEMOSTRACIÓN
Supongamos que Q_i, $i = 1, \ldots, s$ son los divisores primos de $\mathrm{K}(x)$ ramificados en F y sea P_i el divisor primo de F que divide a Q_i. Entonces 2 no es un número laguna para los P_i. Sea $\mathrm{A} = \prod_{i=1}^{s}(\mathrm{Q}_i)^{a_i}$, donde $a_i = -\left[\frac{d_i}{p}\right]$ y d_i el exponente diferente de P_i. Veamos que $-\deg(\mathrm{A}) = t \geq 3$. En efecto, por la Proposición 1.84 $\frac{p-1}{p}\left(-2 + \sum_{i=1}^{s}(m_i + 1)\right) = g_{\mathrm{F}} \geq 2$, así $\frac{p-1}{p}\sum_{i=1}^{s}(m_i + 1) \geq p + 1$. Ahora, como $p = 2$ y $m_i \not\equiv 0 \bmod p$ se tiene la igualdad $\left[\frac{d_i}{p}\right] = \frac{(p-1)(m_i+1)}{p}$, luego $t \geq 2 + 1$. Sea P un lugar no ramificado de F y Q es su restricción a $\mathrm{K}(x)$. Entonces $\deg((\mathrm{Q}^{\lambda}\mathrm{A})^{-1})$, $\deg((\mathrm{Q}^{\lambda-1}\mathrm{A})^{-1}) > 0$ cuando $1 \leq \lambda \leq t - 1$ y $Diff_{\mathrm{F}/\mathrm{K}(x)}Con_{\mathrm{F}/\mathrm{K}(x)}(\mathrm{A})$ es entero y primo relativo a P. Por lo tanto P cumple con las hipótesis del Lema 2.9, así que 2 es un número laguna de cualquier divisor primo no ramificado de F, luego los P_i son puntos de Weierstrass de F (pues casi todos los lugares de F son no ramificados). ■

El Teorema 2.11, junto con el Teorema 2.12 y la Proposición 3.22 sobre puntos de Weierstrass en campos de funciones hiperelípticas, conducen al siguiente:

TEOREMA (H.L. SCHMID) 2.15 *Sea* $\mathrm{F}/\mathrm{K}(x)$ *una extensión cíclica de grado* p^n *con* K *algebraicamente cerrado de característica* p*. Todo divisor primo totalmente ramificado de* F *es un punto de Weierstrass, excepto si* F *es de la forma:*

$$\mathrm{F} = \mathrm{K}(x, y), \quad y^p - y = z, \quad z \in \mathrm{K}(x),$$

donde el divisor de polos de z *es el producto de dos divisores primos distintos de* $\mathrm{K}(x)$*.*

2.3. Extensiones Cíclicas Moderadamente Ramificadas

En esta sección consideraremos extensiones cíclicas para las cuales su grado m es primo relativo con la característica de K. K algebraicamente cerrado.

Sea $\mathrm{F}/\mathrm{K}(x)$ un extensión de Kummer cíclica (Sección A.3). Existe un polinomio irreducible $f(x)$ en $\mathrm{K}[x]$ tal que su divisor primo $\mathrm{Q}_{f(x)}$ no se ramifica en F. Sea $y = f(x)^{-1}$, entonces $\mathrm{K}(x) = \mathrm{K}(y)$ y el divisor primo infinito R_∞ de $\mathrm{K}(y)$ no se ramifica. Por lo tanto podemos suponer que el divisor Q_∞ de $\mathrm{K}(x)$ no se ramifica en $\mathrm{F}/\mathrm{K}(x)$. La aritmética de $\mathrm{F}/\mathrm{K}(x)$ la podemos encontrar en [6]. Por el Teorema A.3 la extensión $\mathrm{F}/\mathrm{K}(x)$ es de la forma $\mathrm{K}(x)(y)$ para algún $y \in \mathrm{F}$ tal que $y^m \in \mathrm{K}(x)$, luego $y^m = \prod_{i=1}^{s}(x-a_i)^{\alpha_i}(\prod_{i=1}^{t}(x-b_i)^{\beta_i})^{-1}$, donde los a_i, b_i son elementos diferentes de K y $0 < \alpha_i,\ \beta_i < m$. Si $z = \prod_{i=1}^{t}(x-b_i)^{\beta_i}y$, $\mathrm{K}(x)(y) = \mathrm{K}(x)(z)$ y además $z^m \in \mathrm{K}[x]$. Entonces se puede suponer que $\mathrm{F} = \mathrm{K}(x)(y)$ con $y^m = \prod_{i=1}^{s}(x-a_i)^{\lambda_i}$, $a_i \in \mathrm{K}$ y $0 < \lambda_i < m$. Sean $\mathrm{P} \in \mathbb{P}_\mathrm{F}$ y $\mathrm{Q} \in \mathbb{P}_{\mathrm{K}(x)}$ tal que $\mathrm{P}|\mathrm{Q}$. Entonces, por la Proposición 1.82 $e(\mathrm{P}|\mathrm{Q}) = \frac{m}{r_\mathrm{Q}}$ y $d(\mathrm{P}|\mathrm{Q}) = \frac{m}{r_\mathrm{Q}} - 1$, donde $r_\mathrm{Q} = (m, v_\mathrm{P}(y^m))$. Aplicando ahora el Teorema del Diferente de Dedekind concluímos que los divisores primos ramificados de $\mathrm{K}(x)$ son aquellos divisores $\mathrm{Q}_1, \ldots, \mathrm{Q}_s$ determinados por los polinomios $x-a_1, \ldots, x-a_s$, respectivamente. Sea $e_i = \frac{m}{(m,\lambda_i)}$ el índice de ramificación de Q_i . Así, Q_i es totalmente ramificado si y sólo si $(m, \lambda_i) = 1$. Supongamos que los primeros r Q_i son los divisores totalmente ramificados y denotemos al único divisor primo de F que divide a Q_i por P_i. El diferente de $\mathrm{F}/\mathrm{K}(x)$ está dado por (ver Proposición 1.82):

$$Diff_{\mathrm{F}/\mathrm{K}(x)} = \mathrm{P}_1^{m-1} \cdots \mathrm{P}_r^{m-1} \prod_{i=r+1}^{s} (Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_i)^{d_i}, \qquad d_i = \frac{e_i - 1}{e_i}.$$

Sea dx la única diferencial de $\mathrm{K}(x)$ determinada por: $dx(\Lambda(\mathrm{Q}_\infty)+\mathrm{K}) = 0$, $dx(\xi) = -1$, donde $\xi_{\mathrm{Q}_\infty} = \frac{1}{x}$, $\xi_\mathrm{Q} = 0$ para $\mathrm{Q} \neq \mathrm{Q}_\infty$ (Proposición 1.53). El divisor de dx es Q_∞^{-2}. Denotemos también por dx a la cotraza de dx en $\mathrm{F}/\mathrm{K}(x)$. Por el Teorema 1.70 $(Cotr(dx)) = (Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_\infty)^{-2} Diff_{\mathrm{F}/\mathrm{K}(x)}$.

Observación. Para $1, \ldots, r$ se tiene que $(x-a_i)_\mathrm{F} = \mathrm{P}_i^m (Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_\infty)^{-1}$. Para $i = r+1, \ldots, s$, $(x-a_i)_\mathrm{F} = Con_{\mathrm{F}/\mathrm{K}(x)}(\mathrm{Q}_i\mathrm{Q}_\infty^{-1})$. Como estamos suponiendo que Q_∞ no se ramifica, $Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_\infty = \prod_{i=1}^{m}\mathrm{R}_i$, donde $\mathrm{R}_1, \ldots, \mathrm{R}_m$ son los m divisores primos distintos de F que extienden a Q_∞. Por lo tanto

$$(\prod_{i=1}^{s}(x-a_i)^{\lambda_i})_\mathrm{F} = \mathrm{P}_1^{m\lambda_1} \cdots \mathrm{P}_r^{m\lambda_r} \prod_{i=r+1}^{s} (Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_i)^{\lambda_i} \left(\prod_{i=1}^{m}\mathrm{R}_i\right)^{-\sum_{i=1}^{s}\lambda_i}.$$

Así que $t = \sum_{i=1}^{s}\lambda_i$, con $t = \deg \mathrm{N}_y$, y en consecuencia

$$(y) = \mathrm{P}_1^{\lambda_1} \cdots \mathrm{P}_r^{\lambda_1} \prod_{i=r+1}^{s} (Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_i)^{\ell_i} (Con_{\mathrm{F}/\mathrm{K}(x)}\mathrm{Q}_\infty)^{-t}, \qquad \ell_i = \frac{\lambda_i}{m}.$$

Sea $\omega_i = (x-a_i)dx$ con $1 \leq i \leq r$. El divisor de (ω_i) es $\mathrm{P}_i^m(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{-3}Diff_{\mathrm{F/K}(x)}$. Esto nos motiva a pensar en la existencia de una diferencial ω en F tal que $(\omega) = \mathrm{P}_i^m\mathrm{A}$, donde A es un divisor entero y primo relativo con P_i. Esta diferencial nos servirá para probar que $m+1$ es un número laguna de P_i. Veamos cómo podemos encontrar esta diferencial. Como

$$(\omega_1) = \mathrm{P}_i^m\mathrm{P}_1^{m-1}\cdots\mathrm{P}_r^{m-1}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{-3}\prod_{i=r+1}^{s}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_i)^{d_i},$$

una forma para intentar conseguir la diferencial ω es escoger una potencia negativa adecuada de (y), digamos $(y)^{-\alpha}$, con $\alpha > 0$, y multiplicar a (ω_1) por $(y)^{-\alpha}$ para eliminar al divisor $(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{-3}$. Haciendo esto obtenemos lo siguiente

$$(\omega_1)(y)^{-\alpha} = \mathrm{P}_i^m\mathrm{P}_1^{m-1-\alpha\lambda_1}\cdots\mathrm{P}_r^{m-1-\alpha\lambda_r}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{\alpha t-3}\prod_{i=r+1}^{s}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_i)^{d_i-\alpha\ell_i},$$

además nos gustaría que $m-1-\alpha\lambda_i = 0$, cosa que en general tal vez no ocurra. Puesto que $(\lambda_i, m) = 1$ existe $0 < a < m$ tal que $a\lambda_i \equiv m-1(\mathrm{mód})m$, entonces $a\lambda_i = k_i m + m - 1$. Multiplicando ahora a $(\omega_1)(y)^{-a}$ por el divisor $(x-a_i)^{k_i}$ logramos que el exponente de P_i sea m. Por otro lado, también se requiere que $m-1-a\lambda_j \geq 0$, $i \neq j$, para ello expresamos a $a\lambda_j$ como $a\lambda_j = k_j m + c_j$, $0 \leq c_j < m$ y multiplicamos a $(\omega_1)(y)^{-a}(x-a_i)^{k_i}$ por $(x-a_j)^{k_j}$, con esto se logra que el exponente de P_j en $(\omega_1)(y)^{-a}(x-a_i)^{k_i}\prod_{j=1,j\neq i}^{r}(x-a_j)^{k_j}$ sea $m-1-a\lambda_j+k_jm = m-1-c_j \geq 0$. Hasta ahora se ha llegado al divisor

$$(\omega_2) = \mathrm{P}_i^m\mathrm{B}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{at-3}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{-\sum_{i=1}^{r}k_i}\prod_{i=r+1}^{s}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_i)^{d_i-a\ell_i},$$

con $\omega_2 = (x-a_i)\prod_{i=1}^{r}(x-a_i)^{k_i}y^a dx$ y $\mathrm{B} = \mathrm{P}_1^{m-1-c_1}\cdots\mathrm{P}_{i-1}^{m-1-c_{i-1}}\mathrm{P}_{i+1}^{m-1-c_{i+1}}\cdots\mathrm{P}_r^{m-1-c_r}$. Observemos que $d_i - a\ell_i = \frac{e_i-1}{e_i} - \frac{a\lambda_i}{m}$ puede ser negativo. Pero $\frac{a\lambda_i}{m} = \frac{a\lambda_i}{e_i(\lambda_i,m)}$ y $\frac{a\lambda_i}{(\lambda_i,m)} = b_i e_i + c_i$, con $0 \leq c_i < e_i$. Entonces el exponente de $Con_{\mathrm{F/K}(x)}\mathrm{Q}_i$ en el divisor $(\omega_2)\prod_{i=r+1}^{s}(x-a_i)^{b_i}$ es $\frac{e_i-1}{e_i} - \frac{a\lambda_i}{m} + b_i = \frac{e_i-1}{e_i} - b_i - \frac{c_i}{e_i} + b_i = \frac{e_i-1-c_i}{e_i} \geq 0$. Resumiendo lo anterior, hemos encontrado una diferencial $\omega_3 = (x-a_i)\prod_{i=1}^{r}(x-a_i)^{k_i}\prod_{i=r+1}^{s}(x-a_i)^{b_i}y^a dx$ para la cual su divisor es

$$\mathrm{P}_i^m\mathrm{B}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)^{at-3-\sum_{i=1}^{r}k_i-\sum_{i=r+1}^{s}b_i}\prod_{i=r+1}^{s}(Con_{\mathrm{F/K}(x)}\mathrm{Q}_i)^{d_i-a\ell_i+b_i}.$$

El problema de encontrar la diferencial ω se reduce ahora a decidir cuándo la suma $u = at - 3 - \sum_{i=1}^{r} k_i - \sum_{i=r+1}^{s} b_i$ es un entero no negativo. Ahora, $k_i = \frac{a\lambda_i}{m} - \frac{c_i}{e_i}$, ya que si $1 \leq i \leq r$ se tiene que $e_i = m$, y $b_i = \frac{a\lambda_i}{m} - \frac{c_i}{e_i}$. Luego $u = \sum_{i=1}^{s} \frac{c_i}{e_i} + at - \frac{a}{m}\sum_{i=1}^{s} \lambda_i - 3 = \sum_{i=1}^{s} \frac{c_i}{e_i} - 3$. Observemos qué pasa con los c_i cuando $1 \leq j \leq r$. Si $j = i$, $c_j = m - 1$ y para $1 \leq j \leq r$, $j \neq i$, $c_j \geq 1$ pues $(m, a) = (m, \lambda_j) = 1$. Así que $\frac{1}{m}\sum_{i=1}^{r} c_j - 3 \geq \frac{1}{m}(m - 1 + (r-1)) - 3 = \frac{r-2(m+1)}{m}$. Ya que u es entero y $u \geq \frac{r-2(m+1)}{m}$, una condición necesaria bajo la cual $u \geq 0$ es que $\frac{r-2(m+1)}{m} > -1$, lo cual se satisface si y sólo si $r > m+2$. Por lo tanto si $r \geq m+3$ la diferencial ω_3 cumple con lo pedido.

Si K es de característica $p > 0$, Schmidt [11] demuestra que la sucesión laguna de F satisface la siguiente condición arítmetica: Sea φ_j, $j = 1, \ldots, g$, la sucesión laguna de F. Sea $\mu_j = \varphi_j - 1$. Si μ es uno de los μ_j, entonces todo entero no negativo ν, cuyos coeficientes p-ádicos no son mayores que los correspondientes coeficientes de μ ocurre entre los μ_j. La diferencial ω y el resultado anterior nos ayudarán en la demostración del siguiente

Teorema 2.16 *Sea* $\mathrm{F/K}(x)$ *una extensión cíclica de grado* m *con* K *un campo algebraicamente cerrado de característica* p *y* $(m, p) = 1$. *Supongamos que al menos* $m + 3$ *divisores primos de* F *son totalmente ramificados, entonces todo divisor primo totalmente ramificado es un punto de Weierstrass.*

Demostración

Conservando las notaciones del desarrollo precedente, tenemos que el divisor principal asociado al elemento $\frac{1}{x-a_i}$ en F es $(Con_{\mathrm{F/K}(x)}\mathrm{Q}_\infty)\mathrm{P}_i^{-m}$. Por lo tanto m no es un número laguna de P_i. Fijemos un P_i, $i \leq r$.

Anteriormente se concluyó que cuando $r \geq m+3$ existe una diferencial ω en F para la cual su divisor es de la forma $\mathrm{P}_i^m\mathrm{A}$, donde A es un divisor entero y primo relativo con P_i. Así, $\omega \in D(\mathrm{P}_i^m)$, $\omega \notin D(\mathrm{P}_i^{m+1})$, y como $0 \leq \delta(\mathrm{P}_i^m) - \delta(\mathrm{P}_i^{m+1}) \leq 1$ (demostración del Lema 2.4), concluímos que $\delta(\mathrm{P}_i^m) - \delta(\mathrm{P}_i^{m+1}) = 1$. Entonces $m + 1$ es un número laguna de P_i (Lema 2.3).

Como $(m, p) = 1$ el primer coeficiente de la expansión p-ádica de m es el entero positivo r, donde $m = kp + r$ con $0 < r < p$. Si la expansión p-ádica de k es $k = a_0 + a_1 p + \cdots + a_n p^n$, la expansión p-ádica de m será $m = r + a_0 p + \cdots + a_n p^{n+1}$. Análogamente la expansión para $m - 1$ es $m - 1 = r - 1 + a_0 p + \cdots + a_n p^{n+1}$. Se concluye que los coeficientes p-ádicos de $m-1$ no son mayores que los correspondientes coeficientes para m. Pero como m no es un número laguna de P_i, la sucesión laguna

de P_i no satisface la condición arítmetica de la sucesión laguna de F. Es decir, P_i no es un punto ordinario. ■

2.4. Un Resultado Adicional

Hasta aquí hemos tratado con los primos fijados por un automorfismo σ de un campo de funciones F, cuyo campo fijo es un campo de funciones de género cero, para decidir cuándo dichos primos son puntos de Weierstrass. Cuando la sucesión laguna del campo F es la clásica la hipótesis sobre el género de campo fijo de σ puede ser omitida.

Sea F un campo de funciones con sucesión laguna clásica y sea σ un automorfismo de F de orden $p^n m$ con $(p, m) = 1$. Con el fin de poder utilizar la expresión del exponente diferente dada en (5) sea E el campo fijo de σ^m, entonces la extensión F/E es cíclica de grado p^n. Escribamos la fórmula de género de Hurwitz para esta extensión

$$g = 1 + p^n(g_{\mathrm{E}} - 1) + \frac{1}{2}\deg Diff_{\mathrm{F/E}}, \tag{14}$$

donde g_{E} es el género de E y $Diff_{\mathrm{F/E}}$ es el diferente de F/E. De acuerdo a (5) la contribución de un divisor primo P fijo al grado del diferente es

$$d = (p-1)\sum_{j=1}^{n}(M_j + 1)p^{j-1}.$$

Para un divisor primo P totalmente ramificado el primer λ_μ no cero para P es λ_1 (ver la relación (4)), por lo tanto $M_j = \max\{p^{j-\nu}\lambda_\nu \mid 1 \leq \nu \leq j\} \geq p^{j-1}$. Entonces

$$d \geq (p-1)\sum_{j=1}^{n}(p^{j-1} + 1)p^{j-1} = \frac{p^{2n} - 1}{p+1} + p^n - 1. \tag{15}$$

Sea Q el primo de E divisible por P. Ya que Q tiene g_{E} números laguna, existe $\lambda \leq g_{\mathrm{E}} + 1$ y un elemento x en E tal que P^λ es su divisor de polos. En F el divisor de polos de x es $\mathrm{P}^{p^n\lambda}$. Pero como estamos suponiendo que la sucesión laguna de F es la clásica P es un punto de Weierstrass si

$$p^n(g_{\mathrm{E}} + 1) \leq g. \tag{16}$$

TEOREMA 2.17 *Sea* F *un campo de funciones para el cual su sucesión laguna es la clásica y sea* σ *un automorfismo de* F *de orden* $p^n m$ *con* $(p, m) = 1$. *Cada primo fijado por* σ *es un punto de Weierstrass, si cualquiera de las siguientes condiciones se cumple:*
(1) $n \geq 2$, $p \geq 5$*;*
(2) $n \geq 1$, *el número de primos fijos es al menos* 3*;*
(3) (*Lewittes*) *el número de primos fijos es al menos* 5.

DEMOSTRACIÓN
De (14), (15) y (16) se sigue que P es un punto de Weierstrass si

$$p^n(g_{\mathrm{E}} + 1) \leq 1 + p^n(g_{\mathrm{E}} - 1) + \frac{1}{2}\left(\frac{p^{2n} - 1}{p + 1} + p^n - 1\right).$$

Simplificando esta desigualdad obtenemos la siguiente

$$3p^n + 3p^{n-1} \leq p^{2n-1} + 1,$$

para $n \geq 2$ y $p \geq 5$ se cumplen las siguientes desigualdades

$$p^{2n-1} + 1 > p^{n-1}p^n \geq pp^n \geq 3p^n + 2p^n \geq 3p^n + pp^{n-1} \geq 3p^n + 3p^{n-1}.$$

Con esto terminamos la parte (1).
Supongamos que σ fija al menos a tres divisores primos. De (15) se obtiene la desigualdad

$$\deg Diff_{\mathrm{F/E}} \geq 3\left(\frac{p^{2n} - 1}{p + 1} + p^n - 1\right).$$

Utilizando nuevamente (14) y (16) concluímos que P es un punto de Weierstrass si

$$p^n(g_{\mathrm{E}} + 1) \leq 1 + p^n(g_{\mathrm{E}} - 1) + \frac{3}{2}\left(\frac{p^{2n} - 1}{p + 1} + p^n - 1\right).$$

Simplificando esta desigualdad llegamos a la siguiente

$$p^{n+1} + p^n + p + 4 \leq 3p^{2n},$$

para $n \geq 1$ se cumple lo siguiente

$$3p^{2n} = 2p^{2n} + p^{2n} \geq (p^{n+1} + 4) + (p^n + p).$$

Aquí terminamos la parte (2).
Finalmente supongamos que el número de primos fijados por σ es al menos cinco. Siguiendo un procedimiento similar al anterior llegamos a la desigualdad

$$3p + 8 \leq 5p^{2n} + p^{n+1} + p^n,$$

la cual se satisface para todo entero positivo n y cualquier número primo p. Supongamos ahora que $n = 0$. Sea E el campo fijo de σ, entonces F/E es una extensión de grado m y por la fórmula del género de Hurwitz se tiene la igualdad

$$g = 1 + m(g_{\mathrm{E}} - 1) + \frac{1}{2}\deg Diff_{\mathrm{F/E}}.$$

El índice de ramificación de los divisores primos fijados por σ es m y entonces su exponente diferente es igual a $m - 1$, por el teorema del diferente de Dedekind (Teorema 1.73). De la misma forma como se obtuvo la relación (16) concluímos que para este caso un primo P fijado por σ es un punto de Weierstrass si

$$m(g_{\mathrm{E}} + 1) \leq g. \tag{17}$$

Pero como $\deg Diff_{\mathrm{F/E}} \geq 5(m-1)$, P es un punto de Weierstrass si

$$m(g_{\mathrm{E}} + 1) \leq 1 + m(g_{\mathrm{E}} - 1) + \frac{5}{2}(m-1).$$

La desigualdad anterior es válida para cada $m \geq 3$. En el caso $m = 2$ todos los divisores primos ramificados en F/E son totalmente ramificados (ver Teorema 1.63 y Corolario 1.81), por lo tanto los primos ramificados coinciden con los primos fijados por σ y su exponente diferente es igual a 1 (Teorema 1.73). Recordemos ahora que un divisor primo de F/E se ramifica si y sólo si divide al $Diff_{\mathrm{F/E}}$ y que por la fórmula del género de Hurwitz $\frac{1}{2}\deg Diff_{\mathrm{F/E}}$ es un entero. Entonces cuando $m = 2$ el número de divisores primos ramificados debe ser par, es decir, el número de primos fijados por σ es par y está acotado inferiormente por 5. Así que $\frac{1}{2}\deg Diff_{\mathrm{F/E}} \geq 3$, luego

$$g = 1 + 2(g_{\mathrm{E}} - 1) + \frac{1}{2}\deg Diff_{\mathrm{F/E}} \geq 1 + 2(g_{\mathrm{E}} - 1) + 3,$$

la desigualdad anterior nos conduce a la siguiente

$$2(g_{\mathrm{E}} + 1) \leq g$$

esto establece la condición necesaria (ver (17)) para que los primos fijos sean puntos de Weierstrass. ■

Capítulo 3

Ejemplos

Antes de presentar ejemplos de campos de funciones de característica positiva, que nos muestren las diferencias con el caso clásico, necesitamos enunciar resultados correspondientes a las diferenciales de Hasse-Schmidt. La mayoría de los resultados de este capítulo no tienen una demostración pero éstas pueden encontrarse en [16]. En este capítulo F/K es un campo de funciones donde K es algebraicamente cerrado.

3.1. Diferenciales de Hasse-Schmidt

En un campo de funciones racionales K(x) se pude definir la derivada usual, esto es, aquella dada por:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \quad y \quad f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

con $f(x) \in \mathrm{K}[x]$. Repitiendo el proceso con $f'(x)$ obtenemos $f''(x)$ y así sucesivamente. Desafortunadamente en característica $p > 0$, la función no constante $f(x) = x^p$ satisface que $f^n(x) = 0$ para todo $n \geq 1$, donde f^n denota la n-ésima derivada. Esto nos sugiere que debemos modificar la definición usual de derivada si se ha de usar en campos de funciones de característica positiva. Este trabajo fue realizado por H. Hasse y F. L. Schmidt [16]. La nueva definición de derivación es utilizada para estudiar el *determinante Wronskiano* y la teoría aritmética de los puntos de Weierstrass.

Definición 3.1 *Sea* F/K *un campo de funciones. Una sucesión* $\{D^{(n)}\}_{n\in\mathbb{N}\cup\{0\}}$ *de funciones* $D^{(n)} : \mathrm{F} \to \mathrm{F}$ *es llamada una diferenciación* (*derivación*) *de* F/K *si*

(*a*) $D^{(0)} = \mathrm{Id}_{\mathrm{F}}$.
(*b*) $D^{(n)}|_{\mathrm{K}} = 0$ *para todo* $n \geq 1$
(*c*) *Para cada* $x, y \in \mathrm{F}$,

$$D^{(n)}(x+y) = D^{(n)}(x) + D^{(n)}(y)$$

y

$$D^{(n)}(xy) = \sum_{m=0}^{n} D^{(m)}(x) D^{(n-m)}(y)$$

La diferenciación $\{D^{(n)}\}_{n\in\mathbb{N}\cup\{0\}}$ *se llama iterativa si*
(*d*) *Para todo* $n, m \in \mathbb{N} \cup \{0\}$

$$D^{(n)} \circ D^{(m)} = \binom{n+m}{m} D^{(n+m)}.$$

Consideremos el campo $\mathrm{F_P} = \mathrm{K}((\pi))$, $\mathrm{F_P}$ es la completación de F en un lugar P con elemento primo π. Supongamos que $\mathrm{car}(\mathrm{K}) = p$ y sea $\alpha \in \mathrm{F}$. El elemento α en $\mathrm{F_P}$ se expresa como $\alpha = \sum_{i=m}^{\infty} a_i \pi^i$, donde $m \in \mathbb{Z}$.
Aplicando a α la derivada usual con respecto a π obtenemos

$$\frac{d^n \alpha}{d\pi^n} = \sum_{i=m}^{\infty} i(i-1)\cdots(i-n+1) a_i \pi^{i-n}.$$

Por lo tanto si $n \geq p$, se tiene que $i(i-1)\cdots(i-n+1) \equiv 0 \,\mathrm{mód}\, p$ para todo i. Así $\frac{d^n}{d\pi^n} \equiv 0$ para $n \geq p$.
Si en vez de $\frac{d^n}{d\pi^n}$ definimos

$$D_{\pi}^{(n)}(\alpha) := \sum_{i=m}^{\infty} \binom{i}{n} a_i \pi^{i-n}, \quad \text{si } i < n \ \binom{i}{n} = 0,$$

entonces $D_{\pi}^{(n)}$ no es cero. Además $\{D^{(n)}\}_{n\in\mathbb{N}\cup\{0\}}$ satisface la igualdad (*d*) de la Definición 3.1. Esta es la motivación para construir derivaciones que sean iterativas.
Sea F/K un campo de funciones y $D = \{D^{(n)}\}_{n\in\mathbb{N}\cup\{0\}}$ una diferenciación sobre F. Sea $\mathrm{M} = \mathrm{F}[[u]]$ el anillo de series de potencias en u con coeficientes en F. Definimos

$$\begin{aligned} \phi : \mathrm{F} &\to \mathrm{M} \\ y &\mapsto \phi(y) = \sum_{n=0}^{\infty} D^{(n)}(y) u^n. \end{aligned} \tag{1}$$

PROPOSICIÓN 3.2 *ϕ es un monomorfismo de anillos.*

Supongamos que existe una diferenciación iterativa $\{D^{(n)}\}_{n\in\mathbb{N}\cup\{0\}}$ sobre F y sea ϕ como en (1). Entonces

$$\phi(D^{(m)}(y)) = \sum_{n=0}^{\infty}(D^{(n)} \circ D^{(m)})(y)u^n = \sum_{n=0}^{\infty}\binom{n+m}{m}D^{(n+m)}(y)u^n.$$

Sea $D_u^{(m)}(u^n) = \binom{n}{m}u^{n-m}$ ($D_u^{(m)}u^n = 0$ para $m > n$), luego

$$\begin{aligned} D_u^{(m)}(\phi(y)) &= D_u^{(m)}\left(\sum_{n=0}^{\infty}D^{(n)}(y)u^n\right) := \sum_{n=0}^{\infty}D^{(n)}(y)D_u^{(m)}(u^n) \\ &= \sum_{n=0}^{\infty}D^{(n)}(y)\binom{n}{m}u^{n-m} = \sum_{n=m}^{\infty}\binom{n}{m}D^{(n)}(y)u^{n-m} \\ &= \sum_{t=0}^{\infty}\binom{t+m}{m}D^{(t+m)}(y)u^t = \phi(D^{(m)}(y)). \end{aligned}$$

De esta manera obtenemos la

PROPOSICIÓN 3.3 *Una derivación D es iterativa si y sólo si*

$$D_u^{(m)}(\phi(y)) = \phi(D^{(m)}(y)).$$

PROPOSICIÓN 3.4 *Para cada elemento separable x de* F/K*, existe una diferenciación iterativa única $D_x = \{D_x^{(n)}\}_{n\in\mathbb{N}\cup\{0\}}$ de* F/K *tal que*

$$D_x^{(1)}(x) = 1 \quad y \quad D_x^{(n)}(x) = 0 \quad n \geq 2.$$

La diferenciación de la proposición anterior es llamada *diferenciación con respecto a x* y denotaremos a $D_x^{(1)}$ como $\frac{d}{dx}$.

TEOREMA 3.5 *Sea D una diferenciación iterariva de un campo de funciones* F/K *separablemente generado tal que $D^{(1)} \not\equiv 0$, entonces existe $x \in \mathrm{F} \setminus \mathrm{K}$ tal que $D = D_x$.*

3.2. El Wronskiano

En esta sección se considera una diferenciación iterativa D sobre F/K tal que si $D^{(n)}(a) = 0$ para todo $n \geq 1$, entonces $a \in \mathrm{K}$ y $D^{(1)} \not\equiv 0$.

PROPOSICIÓN 3.6 *Sea* $\{y_0, \ldots, y_n\} \subseteq \mathrm{F}$ *linealmente independiente sobre* K. *Para* $0 \leq i \leq n$, *definimos*

$$Y_i := \phi(y_i) = \sum_{n=0}^{\infty} D^{(n)}(y_i)u^n.$$

Entonces $\{Y_1, \ldots, Y_n\} \subseteq \mathrm{F}[[u]]$ *es linealmente independiente sobre* F.

TEOREMA 3.7 *Si* $\{y_0, \ldots, y_n\}$ *es linealmente independiente sobre* K, *entonces existen* n *números enteros* $m_1, \ldots, m_n$ *tales que* $0 < m_1 < m_2 < \cdots < m_n$ *y*

$$\Delta_{m_1,\ldots,m_n}(y_0, \ldots, y_n) := \det \begin{bmatrix} y_0 & \cdots & y_n \\ D^{(m_1)}(y_0) & \cdots & D^{(m_1)}(y_n) \\ \vdots & \cdots & \vdots \\ D^{(m_n)}(y_0) & \cdots & D^{(m_n)}(y_n) \end{bmatrix} \neq 0 \tag{2}$$

Escribamos $\xi = (y_0, \ldots, y_n)$ y $D^{(m)}\xi = (D^{(m)}(y_0), \ldots, D^{(m)}(y_n))$. Definimos enteros $\epsilon_0, \ldots, \epsilon_n$ como sigue: Sea $\epsilon_0 = 0$ y si $\epsilon_1, \ldots, \epsilon_i$ ya están definidos y $i \leq n-1$, sea

$$\epsilon_{i+1} = \text{mín}\{j \in \mathbb{N} \mid D^{(\epsilon_{i+1})}\xi \text{ es l.i. de } D^{(\epsilon_0)}\xi, \ldots, D^{(\epsilon_i)}\xi\}.$$

Así $\epsilon_0 < \epsilon_1 < \cdots < \epsilon_n$ y el conjunto $\{\epsilon_0, \ldots, \epsilon_n\}$ satisface al Teorema 3.7, y es minimal en el siguiente sentido, si $\{\delta_0, \ldots, \delta_n\}$ también cumple con (2) entonces existe un $0 \leq i \leq n$ tal que $\epsilon_i \leq \delta_i$.

DEFINICIÓN 3.8 *Sean* $\{\epsilon_0, \ldots, \epsilon_n\}$ *y* $\xi = \{y_0, \ldots, y_n\}$ *como arriba. Entonces*

$$W = \Delta_{\epsilon_1,\ldots,\epsilon_n}(y_0, \ldots, y_n)$$

es llamado el determinante Wronskiano de ξ. *Al conjunto* $\{\epsilon_0, \ldots, \epsilon_n\}$ *le llamamos el orden de* W *con respecto a* D *y cada* ϵ_i *es llamado un orden de* W.

PROPOSICIÓN 3.9 *Continuamos con la notación de la definición anterior. Sea* $\{\alpha_0, \ldots, \alpha_n\}$ *un conjunto de números naturales tales que* $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_n$ *y* $\Delta_{\alpha_1,\ldots,\alpha_n}(y_0, \ldots, y_n) \neq 0$. *Entonces* $\epsilon_i \leq \alpha_i$ *para cada* $0 \leq i \leq n$.

Supongamos que $\{y_0, \ldots, y_n\}$ es un subconjunto de F linealmente independiente sobre K y V es el K-espacio vectorial generado por $\{y_0, \ldots, y_n\}$. Si $\{z_0, \ldots, z_n\}$ es otra base de V, consideremos la matriz A definida por

$$z_i = \sum_{j=0}^{n} a_{ij} y_j \quad para \quad i = 0, \ldots, n \quad y \quad a_{ij} \in \mathrm{K}.$$

Entonces $D^{(m)}(z_i) = \sum_{j=0}^{n} a_{ij} D^{(m)} y_j$ para todo $m \geq 0$. Por lo tanto

PROPOSICIÓN 3.10 *Para* $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_n$ *se cumple que*

$$\Delta_{\{\alpha_1,\ldots,\alpha_n\}}(z_0, \ldots, z_n) = (\det A)\Delta_{\{\alpha_1,\ldots,\alpha_n\}}(y_0, \ldots, y_n).$$

Una consecuencia de lo anterior es que el determinante Wronskiano es un invariante del espacio V. El determinante Wronskiano puede ser calculado con la ayuda de las series de potencias de (1).

DEFINICIÓN 3.11 *Dos dominios enteros* P, P_1 *con derivaciones iterativas* D *y* D_1 *respectivamente son llamados diferencialmente isomorfos si existe un isomorfismo de anillos* $\theta : \mathrm{P} \to \mathrm{P}_1$ *tal que* $\theta(D^{(n)}(y)) = D_1^{(n)}(\theta(y))$ *para todo elemento* $y \in \mathrm{P}$, $n \in \mathbb{Z}$, $n \geq 0$.

Para el campo de funciones F/K sea $\mathrm{T} = \phi(\mathrm{F})$, donde ϕ es el monomorfismo de la Proposición 3.2, esto es $\phi(y) = \sum_{n=0}^{\infty}(D^{(n)}(y))u^n$. Definimos $D_u^{(n)}$ en T por

$$D_u^{(n)}\left(\sum_{m=0}^{\infty} a_m u^m\right) = \sum_{m=n}^{\infty} \binom{m}{n} a_m u^{m-n}.$$

Entonces $D_u = \{D_u^{(n)}\}$ es una diferenciación iterativa del campo de funciones T/K y por la Proposición 3.3 F y T son diferencialmente isomorfos.

DEFINICIÓN 3.12 *Sean* $z_0, \ldots, z_n \in \mathrm{M} = \mathrm{F}[[u]]$. *Definimos el determinante Wronskiano de* $\{z_0, \ldots, z_n\}$ *por*

$$\Delta_{\epsilon_1,\ldots,\epsilon_n}(z_0, \ldots, z_n) := \det \begin{bmatrix} D_u^{(0)}(z_0) & \cdots & D_u^{(0)}(z_n) \\ D_u^{(\epsilon_1)}(z_0) & \cdots & D_u^{(\epsilon_1)}(z_n) \\ \vdots & \cdots & \vdots \\ D_u^{(\epsilon_n)}(z_0) & \cdots & D_u^{(\epsilon_n)}(z_n) \end{bmatrix}.$$

Sea $\{y_0, \ldots, y_n\} \subseteq$ F linealmente independiente sobre K y $\phi(y_i) = Y_i$ para $0 \leq i \leq n$. Por la Proposición 3.6 $\{Y_0, \ldots, Y_n\}$ es linealmente independiente sobre K y como F $\cong$ T podemos considerar el determinante Wronskiano de $\Gamma = \{Y_0, \ldots, Y_n\}$ en el campo de funciones T/K con orden $\{\Upsilon_0, \ldots, \Upsilon_n\}$ con respecto a $D_u^{(n)}$. Ya que T y F son diferencialmente isomorfos se cumple que

$$\phi(\Delta_{\epsilon_1,\ldots,\epsilon_n}(y_0, \ldots, y_n)) = \Delta_{\epsilon_1,\ldots,\epsilon_n}(Y_0, \ldots, Y_n),$$

donde $0 < \epsilon_1 < \cdots < \epsilon_n$. Por lo tanto $\Delta(y_0, \ldots, y_n)$ y $\Delta(Y_0, \ldots, Y_n)$ tienen los mismos órdenes, digamos $\epsilon_0, \ldots, \epsilon_n$. De esta manera $\{\epsilon_1, \ldots, \epsilon_n\}$ es el conjunto mínimo (Proposición 3.9), ordenado con respecto al orden lexicográfico, tal que

$$\Delta_{\epsilon_1,\ldots,\epsilon_n}(Y_0, \ldots, Y_n) \not\equiv 0 \text{ mód } u.$$

Sea U el F-espacio vectorial generado por $\{Y_0, \ldots, Y_n\}$. Para cualquier otra base $\{Z_0, \ldots, Z_n\}$ de U, se sigue de la Proposición 3.10 que los determinantes Wronskiano $\Delta(Y_0, \ldots, Y_n)$ y $\Delta(Z_0, \ldots, Z_n)$ tienen los mismos órdenes. Se puede escoger una base $\{Z_0, \ldots, Z_n\}$ de U tal que

$$Z_j = u^{h_j} + \sum_{h_j+1}^{\infty} a_n^{(j)} u^n \quad \text{para } 0 \leq j \leq n \tag{3}$$

con $0 \leq h_0 < h_1 < \cdots < h_n$. Notemos que h_0 es el mayo entero tal que u^{h_0} divide a todo elemento de U y, en general, h_{i+1} es el máximo entero tal que $u^{h_{i+1}}$ divide a todo elemento de U que sea divisible por u^{h_i+1}. Por tanto $h_0, \ldots, h_n$ son invariantes del espacio vectorial U.

Definición 3.13 *Las potencias h_i, $0 \leq i \leq n$, son llamadas los invariantes Hermitianos de* U *y la base dada en* (3) *es llamada base Hermitiana de* U *sobre* F.

Ya que los Y_i son las series de potencias correspondientes a los y_i, se cumple que $h_0 = 0$.

Teorema 3.14 *Sean $Y_0, \ldots, Y_n$ las series de potencias asociadas a los elementos $y_0, \ldots, y_n$ de* F*, esto es $Y_i = \phi(y_i)$ para $0 \leq i \leq n$. Entonces los órdenes del determinante Wronskiano $\Delta(y_0, \ldots, y_n)$ son los invariantes Hermitianos $\{h_1, \ldots, h_n\}$ del*

F-*espacio vectorial* U *generado por* $\{Y_0, \ldots, Y_n\}$.
Además, si $\{Z_0, \ldots, Z_n\}$ *es una base Hermitiana de* U *y* $A \in M_{n+1}(\mathrm{F})$ *es la matriz de cambio de base, es decir,* $Y_i = AZ_i$ *para* $0 \leq i \leq n$. *Entonces*

$$\Delta_{h_1,\ldots,h_n}(y_0, \ldots, y_n) = \det A.$$

Por Teorema 3.5 cualquier diferenciación iterativa es de la forma D_x. Al determinante Wronskiano de un subconjunto $\{y_0, \ldots, y_n\}$ de F linealmente independiente sobre K con respecto a D_x lo denotaremos como $W_x(y_0, \ldots, y_n)$.

3.3. Teoría Aritmética de Puntos de Weierstrass

En esta sección se considera un campo de funciones F/K de género g, donde K es un campo algebraicamente cerrado de característica $p \geq 0$.
Sea W la clase canónica en F y ω una diferencial no cero. Por el Corolario 1.47, $\ell((\omega)_{\mathrm{F}}^{-1}) = N(\mathrm{W}) = g$. Sea $\{y_0, \ldots, y_{g-1}\}$ una base de $L_{\mathrm{F}}((\omega)_{\mathrm{F}}^{-1})$. Sea x un elemento separable para F. Denotemos por $0, \mu_1, \ldots, \mu_{g-1}$ a los órdenes de $W_x(y_0, \ldots, y_{g-1})$.

Definición 3.15 *Definimos el divisor de ramificación como*

$$\mathrm{B_F} := (\omega)_{\mathrm{F}}^{g}(W_x(y_0, \ldots, y_{g-1}))_{\mathrm{F}}(dx)_{\mathrm{F}}^{\sum_{i=0}^{g-1}\mu_i}.$$

dx es la cotraza de la única diferencial que se menciona en la Proposición 1.53.

Teorema 3.16 *El divisor de ramificación* $\mathrm{B_F}$ *es independiente de la diferencial* ω, *de la base* $y_0, \ldots, y_{g-1}$ *de* $L_{\mathrm{F}}((\omega)_{\mathrm{F}}^{-1})$ *y del elemento separable* x. *Así,* $\mathrm{B_F}$ *es un invariante del campo* F.

Teorema 3.17 *Sea* F/K *un campo de funciones con* K *algebraicamente cerrado. Sea* ω *cualquier diferencial no cero de* K. *Sea* $\{y_0, \ldots, y_{g-1}\}$ *una base de* $L_{\mathrm{F}}((\omega)_{\mathrm{F}}^{-1})$ *y* x *un elemento separable de* F/K. *Denotemos por* $\mu_0, \mu_1, \ldots, \mu_{g-1}$ *a los órdenes del determinante Wronskiano* $W_x(y_0, \ldots, y_{g-1})$ *y* $\mathrm{B_F}$ *el divisor de ramificación de* F. *Entonces para cualquier divisor primo* B, *la sucesión laguna de* B *es* $\mu_0+1, \ldots, \mu_{g-1}+1$ *si y sólo si* $\mathrm{B} \nmid \mathrm{B_F}$. *En particular casi todos los divisores tienen la misma sucesión laguna.*

3.4. Campos con un Unico Punto de Weierstrass

En los campos de funciones hiperelípticas encontramos dos ejemplos interesantes del comportamiento de los puntos de Weierstrass, en uno de ellos el número de puntos de Weierstrass es tan grande como el género y en el otro existe un único punto de Weierstrass aun cuando el género es arbitrariamente grande. Mientras que la cantidad de puntos de Weierstrass no puede crecer arbitrariamente con respecto al género, pues en característica cero dicho número es a lo más $g^3 - g$ y cuando la característica es positiva está acotado por $(g-1)g(3g-1)$.

Teorema (Desigualdad de Riemann) 3.18 *Sea* $\mathrm{F/K}$ *un campo de funciones tal que* $\mathrm{F} = \mathrm{K}(x, y)$. *Entonces se tiene la siguiente estimación para el género* g *de* F*:*

$$g \leq ([\mathrm{F} : \mathrm{K}(x)] - 1) \cdot ([\mathrm{F} : \mathrm{K}(y)] - 1).$$

Demostración Ver [13, p. 132]

Proposición 3.19 *Sea* $\mathrm{F/K}$ *un campo de funciones hiperelípticas de género* g *y* $\mathrm{K}(x) \subseteq \mathrm{F}$ *tal que* $[\mathrm{F} : \mathrm{K}(x)] = 2$. *Entonces todos los subcampos de funciones racionales* $\mathrm{K}(z) \subseteq \mathrm{F}$ *con* $[\mathrm{F} : \mathrm{K}(z)] \leq g$ *están contenidos en* $\mathrm{K}(x)$.

Demostración
Supongamos que $[\mathrm{F} : \mathrm{K}(z)] \leq g$ pero $z \notin \mathrm{K}(x)$. Entonces $\mathrm{F} = \mathrm{K}(x, z)$ y por la desigualdad de Riemann

$$g \leq ([\mathrm{F} : \mathrm{K}(x)] - 1) \cdot ([\mathrm{F} : \mathrm{K}(z)] - 1) \leq g - 1,$$

lo cual es una contradicción. ■
Por la proposición anterior en un campo de funciones hiperelípticas $\mathrm{F/K}$ existe solo un subcampo de funciones racionales $\mathrm{K}(x) \subseteq \mathrm{F}$ para el cual $[\mathrm{F} : \mathrm{K}(x)] = 2$.

Dada una extensión finita de campos $\mathrm{F/H}$ el *grado separable* $[\mathrm{F} : \mathrm{H}]_s$ de $\mathrm{F/H}$ es el número de H-homomorfismos de F en una cerradura algebraica E de F. Se sabe que la extensión $\mathrm{F/H}$ es *puramente inseparable* si y sólo si $[\mathrm{F} : \mathrm{H}]_s = 1$.

Proposición 3.20 *Sea* $\mathrm{F/H}$ *una extensión finita de campos de característica* $p > 0$, *entonces* $[\mathrm{F} : \mathrm{H}] = [\mathrm{F} : \mathrm{H}]_s p^n$, *para algún* $n \geq 0$.

Demostración Ver [8, p. 63]

Lema 3.21 *Sea* $\mathrm{F/K}$ *un campo de funciones hiperelípticas con* K *algebraicamente cerrado, entonces la extensión* $\mathrm{F/K}(x)$ *de grado dos es separable.*

Demostración
Si $\mathrm{car(K)} = 0$ la extensión $\mathrm{F/K}(x)$ es separable. Ahora supongamos que $\mathrm{car(F)} = p > 0$. Por la proposición anterior $[\mathrm{F} : \mathrm{K}(x)] = [\mathrm{F} : \mathrm{K}(x)]_s p^n$. Además $\mathrm{F/K}(x)$ es separable si y sólo si $[\mathrm{F} : \mathrm{K}(x)] = [\mathrm{F} : \mathrm{K}(x)]_s$, entonces si $\mathrm{F/K}(x)$ no es separable p divide a $[\mathrm{F} : \mathrm{K}(x)] = 2$, luego $p = 2$. Por lo tanto supongamos que $\mathrm{F/K}(x)$ no es separable y que $\mathrm{car(K)} = 2$. Entonces $\mathrm{F/K}(x)$ es puramente inseparable, pues $[\mathrm{F} : \mathrm{K}(x)]_s = 1$. Por la Proposición 1.97 $\mathrm{K}(x) = \{z^2 \mid z \in \mathrm{F}\}$. Así que, existe $z \in \mathrm{F}$ tal que $z^2 = x$ y $z \notin \mathrm{K}(x)$, lo cual implica que $\mathrm{F} = \mathrm{K}(z)$. Esto contradice al hecho de que g_{F} sea positivo. Se concluye que en característica dos $\mathrm{F/K}(x)$ también es separable.

Proposición 3.22 *Si* $\mathrm{F/K}$ *es un campo de funciones hiperelípticas para un campo algebraicamente cerrado* K *de característica* $p \geq 0$*, entonces la sucesión laguna del campo es la clásica, esto es, igual a* $1, 2, \ldots, g$*. Los puntos de Weierstrass son los divisores primos ramificados de* $\mathrm{F/K}(x)$ *con* $[\mathrm{F} : \mathrm{K}(x)] = 2$ *y su sucesión laguna es* $1, 3, \ldots, 2g - 1$*.*

Demostración
Sea P un lugar de F no ramificado en $\mathrm{F/K}(x)$ y n un entero tal que $2 \leq n \leq g$. Si n es un número polo de P existe $z \in \mathrm{F}$ tal que $\mathrm{N}_z = \mathrm{P}^n$, luego $[\mathrm{F} : \mathrm{K}(z)] = n \leq g$ (Teorema 1.23). Entonces $z \in \mathrm{K}(x)$ por la Proposición 3.19. Denotemos por N al divisor de polos en $\mathrm{K}(x)$ de z. Así $\mathrm{P}^n = Con_{\mathrm{F/K}(x)}(\mathrm{N})$, entonces $\mathrm{N} = \mathrm{Q}^m$ con Q un lugar de $\mathrm{K}(x)$ y por lo tanto P es el único lugar de F encima de Q. Por el Teorema 1.63 $[\mathrm{F} : \mathrm{K}(x)] = e(\mathrm{P|Q})f(\mathrm{P|Q})$, pero como K es algebraicamente cerrado $f(\mathrm{P|Q}) = 1$, así que Q es totalmente ramificado. Por definición lo anterior implica que P es ramificado, lo que es una contradicción. Entonces los g enteros $1, 2, \ldots, g$ son números laguna de cualquier lugar de F no ramificado en $\mathrm{F/K}(x)$, lo que nos indica que la sucesión laguna de F es la clásica, pues casi todos los lugares no se ramifican (Corolario 1.75).
Consideremos ahora un lugar $\mathrm{P} \in \mathbb{P}_{\mathrm{F}}$ ramificado en $\mathrm{F/K}(x)$ y entonces totalmente ramificado (ver Teorema 1.63). Sea $\mathrm{Q} = \mathrm{P} \cap \mathrm{K}(x)$. Existe un elemento en $\mathrm{K}(x)$ para el cual su divisor de polos es Q. En F este elemento tiene a P^2 como su divisor de

polos. Por lo tanto los $g-1$ enteros pares entre 1 y $2g-1$ son números polo de P. Entonces por el Lema 2.4 los g enteros impares entre 1 y $2g-1$ forman la sucesión laguna de P. Se concluye que los divisores primos ramificados de $\mathrm{F}/\mathrm{K}(x)$ tienen la misma sucesión laguna y ésta es diferente de la de F, es decir estos lugares son los puntos de Weierstrass. ■

Sean $\mathrm{K}(x)$ un campo de funciones racionales donde K es de característica 2 y $\mathrm{F}/\mathrm{K}(x)$ una extensión cíclica de grado dos. Entonces $\mathrm{F}=\mathrm{K}(x,y)$ para algún $y\in\mathrm{F}$ tal que $y^2-y=u\in\mathrm{F}$ y $y\notin\mathrm{K}(x)$ (Teorema A.6). Bajo estas condiciones la extensión $\mathrm{F}/\mathrm{K}(x)$ es ramificada (Corolario 1.77). Por la parte (c) de la Proposición 1.84 el género g de F está dado por

$$g=\frac{1}{2}\left(-2+\sum_{\mathrm{P}\in\mathbb{P}_{\mathrm{F}}}(m_{\mathrm{P}}+1)\cdot\deg\mathrm{P}\right).$$

Deseamos encontrar una cota para la cantidad s de lugares ramificados en este tipo de extensiones. Sean $\mathrm{P}_1,\ldots,\mathrm{P}_s$ los lugares ramificados de $\mathrm{F}/\mathrm{K}(x)$. Para i entre 1 y s el entero m_{P_i} es positivo, luego

$$\begin{aligned} g&=\frac{1}{2}\left(-2+\sum_{i=1}^{s}(m_{\mathrm{P}_i}+1)\cdot\deg\mathrm{P}_i\right)\geq\frac{1}{2}\left(-2+\sum_{i=1}^{s}2\right)\\ &=s-1, \end{aligned}$$

entonces $1\leq s\leq g+1$. En particular si K es algebraicamente cerrado F tiene a lo más $g+1$ puntos de Weierstrass (Proposición 3.22), ésto marca una diferencia con el caso clásico en donde existen al menos $2g+2$ puntos de Weierstrass. En seguida veremos dos ejemplos en donde ocurren los casos extremos para s.
Sea K un campo algebraicamente cerrado con $\mathrm{car}(\mathrm{K})=2$. En el campo hiperelíptico $\mathrm{F}=\mathrm{K}(x,y)$ con

$$y^2-y=f(x)\in\mathrm{K}[x],\quad \deg f=2m+1\quad y\quad m\geq 1,$$

el polo P_∞ de x en $\mathrm{K}(x)$ es el único lugar ramificado en $\mathrm{F}/\mathrm{K}(x)$ (Proposición 1.84 (b)). Entonces el género de F es (Fórmula del Género de Hurwitz)

$$g_{\mathrm{F}}=1+[\mathrm{F}:\mathrm{K}(x)](g_{\mathrm{K}(x)}-1)+\frac{1}{2}(2-1)((2m+1)+1)=\frac{2m+2}{2}-1=m.$$

Ya que F es un campo hiperelíptico, existen campos de género g suficientemente grande con un sólo punto de Weierstrass (Proposición 3.22).
Sea K como en el ejemplo anterior y F el campo hiperelíptico $\mathrm{K}(x, y)$ donde

$$y^2 - y = \prod_{i=1}^{m+1} (x - a_i)^{-1}, \quad \text{los } a_i \text{ son distintos a pares y } m \geq 0.$$

Por la Proposición 1.84 el género g de F es igual a

$$\begin{aligned} g &= \frac{1}{2}\left(-2 + \sum_{i=1}^{m+1} (m_{\mathrm{P}_i} + 1) \cdot \deg \mathrm{P}_i\right) = \frac{1}{2}\left(-2 + \sum_{i=1}^{m+1} (1+1)\right) \\ &= m \end{aligned}$$

Como F es un campo hiperelíptico, existen campos de género g con $g+1$ puntos de Weierstrass.

Proposición 3.23 *Sea* K *un campo de característica distinta de* 2.
(*a*) *Sea* F/K *un campo de funciones hiperelípticas de género* g. *Entonces existen* $x, y \in \mathrm{F}$ *tales que* $\mathrm{F} = \mathrm{K}(x, y)$ *y*

$$y^2 = f(x) \in \mathrm{K}[x] \tag{4}$$

con $f(x)$ *libre de cuadrado y de grado* $2g+1$ *o* $2g+2$.
(*b*) *Inversamente, si* $\mathrm{F} = \mathrm{K}(x, y)$ *y* $y^2 = f(x) \in \mathrm{K}[x]$ *con* $f(x)$ *libre de cuadrado de grado mayor que* 4, *entonces* F/K *es hiperelíptico de género* $\frac{m-1}{2}$ *si* $m \equiv 1 \bmod 2$ *o* $\frac{m-2}{2}$ *en otro caso.*
(*c*) *Sea* $\mathrm{F} = \mathrm{K}(x, y)$ *con* $y^2 = f(x)$ *como en* (4). *Entonces los lugares* $\mathrm{P} \in \mathbb{P}_{\mathrm{K}(x)}$ *que se ramifican en* $\mathrm{F}/\mathrm{K}(x)$ *son los siguientes:*

todos los ceros de $f(x)$ *si* $\deg f(x) \equiv 0 \bmod 2$,
todos los ceros de $f(x)$ *y el polo de* x *si* $\deg f(x) \equiv 1 \bmod 2$.

Por lo tanto, si $f(x)$ *se descompone en factores lineales,* $2g+2$ *lugares de* $\mathrm{K}(x)$ *se ramifican en* $\mathrm{F}/\mathrm{K}(x)$.

Demostración Ver [13, p. 194].

PROPOSICIÓN 3.24 *Si* F/K *es un campo de funciones hiperelípticas para un campo algebraicamente cerrado* K *de característica distinta de* 2*, entonces* F/K *tiene* $2g+2$ *puntos de Weierstrass.*

DEMOSTRACIÓN
Se sigue de la Proposición 3.22 y el inciso (c) de la Proposición 3.23. ■

3.5. Campos con Sucesión Laguna no Clásica

En esta sección supondremos que K es un campo algebraicamente cerrado de característica $p > 0$.

TEOREMA 3.25 *Sea* $\mathrm{F} = \mathrm{K}(x, y)$ *un campo de funciones definido por la ecuación*

$$y^q - y = x^m$$

donde $q = p^u$*,* $m > 1$ *y* m *divide a* $q+1$*. Sea* $q+1 = mn$*. Entonces*

$$g_{\mathrm{F}} = \frac{(m-1)(q-1)}{2}.$$

Además la sucesión laguna del campo está formada por los elementos del conjunto

$$\mathrm{A} = \{rq + s + 1 \mid r, s \geq 0,\ (r+1)n + (s+1) \leq q\}.$$

DEMOSTRACIÓN
El género de F *es* $\frac{(m-1)(q-1)}{2}$.
Primero consideremos una raíz α de $T^q - T - x^m$. Entonces para cualquier $\mu \in \mathbb{F}_{p^u}$,

$$(\alpha+\mu)^q - (\alpha+\mu) = \alpha^q + \mu^q - \alpha - \mu = \alpha^q + \mu - \alpha - \mu = \alpha^q - \alpha = x^m.$$

Por tanto $\{\alpha + \mu \mid \mu \in \mathbb{F}_q\}$ es el conjunto de las raíces de $T^q - T - x^m$.
En particular $\mathrm{F}/\mathrm{K}(x)$ es una extensión de Galois. Sea B un divisor primo de F que divida al primo infinito P_∞ (el polo de x en $\mathrm{K}(x)$) de $\mathrm{K}(x)$. Tenemos que

$$v_{\mathrm{B}}(y^q - y) = m v_{\mathrm{B}}(x) = m e(\mathrm{B}|\mathrm{P}_\infty) v_{\mathrm{P}_\infty}(x) = -m e(\mathrm{B}|\mathrm{P}_\infty) < 0.$$

Por lo tanto $v_{\mathrm{B}}(y) < 0$, pues en otro caso $v_{\mathrm{B}}(y^q - y) \geq \min\{v_{\mathrm{B}}(y^q), v_{\mathrm{B}}(y)\} \geq 0$. Así

$$v_{\mathrm{B}}(y^q - y) = \min\{v_{\mathrm{B}}(y^q), v_{\mathrm{B}}(y)\} = q v_{\mathrm{B}}(y).$$

Se sigue que $qv_{\mathrm{B}}(y) = -me(\mathrm{B}|\mathrm{P}_\infty)$. Ya que $(q, m) = 1$, q divide a $e(\mathrm{B}|\mathrm{P}_\infty)$. Luego, P_∞ es totalmente ramificado en $\mathrm{F}/\mathrm{K}(x)$. También se tiene que $v_{\mathrm{B}}(y) = -m$ y $v_{\mathrm{B}}(x) = -q$. Para cada $\mu \in \mathbb{F}_q$, sea $\sigma_\mu \in G(\mathrm{F}/\mathrm{K}(x))$ definido por

$$\sigma_\mu(y) = y + \mu$$

Entonces $\theta : (\mathbb{F}_q, +) \to G(\mathrm{F}/\mathrm{K}(x))$ es un isomorfismo de grupos.
Sea P un divisor primo diferente de B, entonces $0 \leq v_{\mathrm{P}}(x^m) = v_{\mathrm{P}}(y^q - y)$, así que $v_{\mathrm{P}}(y) \geq 0$. Por lo tanto $y \in \mathcal{O}_{\mathrm{P}}$. Por otro lado

$$\beta(T) = T^q - T - x^m = \prod_{\mu \in \mathbb{F}_q} (T - y - \mu).$$

Entonces $\beta(T)' = \sum_{\nu \in \mathbb{F}_q} \prod_{\mu \neq \nu} (T - y - \mu)$, luego $\beta(y)' = \prod_{\mu \neq 0}(y - y - \mu) = (-1)^{q-1} \prod_{\mu \neq 0} \mu$. Por tanto $(\beta(y)')_{\mathrm{F}}$ es el divisor unidad y por el Teorema 1.78 se sigue que P no se ramifica en $\mathrm{F}/\mathrm{K}(x)$. Lo anterior implica que $Dif f_{\mathrm{F}/\mathrm{K}(x)} = \mathrm{B}^s$ para algún s. Lo que sigue es determinar los grupos de ramificación para B.
Ya que $v_{\mathrm{B}}(y) = -m$ y $v_{\mathrm{B}}(x) = -q$, se tiene que $v_{\mathrm{B}}(y^{-n}x) = nm - q = 1$. Así $y^{-n}x$ es un elemento primo para B. Ahora $G_{-1} = G_0 = G$ y para $\mu \in \mathbb{F}_q^*$

$$\sigma_\mu(y^{-n}x) - y^{-n}x = (y + \mu)^{-n}x - y^{-n}x = x\frac{y^n - (y + \mu)^n}{(y + \mu)^n y^n} = \frac{-\mu y^{n-1} + \cdots}{(y^2 + \mu y)^n}x.$$

De esta manera

$$\begin{aligned} v_{\mathrm{B}}(\sigma_\mu(y^{-n}x) - y^{-n}x) &= (n-1)v_{\mathrm{B}}(y) + v_{\mathrm{B}}(x) - 2nv_{\mathrm{B}}(y) \\ &= (n+1)m - q = q + 1 + m - q = m + 1. \end{aligned}$$

Del Teorema 1.89 se sigue que $\sigma_\mu \in G_m$ y $\sigma_\mu \notin G_{m+1}$. Por lo tanto

$$G = G_{-1} = G_0 = \cdots = G_m, \quad G_{m+1} = \{1\}.$$

El Teorema 1.90 nos dice que

$$s = \sum_{i=0}^{\infty}(|G_i| - 1) = \sum_{i=0}^{m}(q - 1) = (m + 1)(q - 1).$$

Aplicando la fórmula del género de Riemann-Hurwutz obtenemos

$$g_{\mathrm{F}} = 1 + q(0 - 1) + \frac{1}{2}(m + 1)(q - 1) = \frac{(m - 1)(q - 1)}{2}.$$

La cardinalidad de A *es* $g = g_{\mathrm{F}}$.
Para $r \geq 0$ se tiene que

$$(r+1)n + (s+1) \leq q \text{ si y sólo si } s \leq q - (r+1)n - 1.$$

Sea $a_r = \text{máx}\{q-(r+1)n, 0\}$. Entonces $0 \leq s \leq a_r - 1$. Además $(r+1)n \leq q = nm-1$. Entonces $r \leq m - \frac{1}{n} - 1$ y $r \leq m-2$. Se sigue que

$$\begin{aligned} |\mathrm{A}| &= \sum_{r=0}^{m-2} a_r = \sum_{r=0}^{m-2} \{q-(r+1)n\} = (m-1)q - n\frac{m(m-1)}{2} \\ &= (m-1)q - \frac{(q+1)(m-1)}{2} = (m-1)\frac{2q-q-1}{2} \\ &= \frac{(m-1)(q-1)}{2} = g_{\mathrm{F}}. \end{aligned}$$

El conjunto $\{x^r y^s \,|\, r, s \geq 0,\ (r+1)n + (s+1) \leq q\}$ *es una base para* $L((dx)_{\mathrm{F}}^{-1})$.
Sea dx la única diferencial en $D_{\mathrm{K}(x)}$ con $(\mathrm{dx}) = \mathrm{P}_\infty^{-2}$ y $\mathrm{dx}_{\mathrm{P}_\infty}(x^{-1}) = -1$ (Proposición 1.53). Denotemos por dx a la cotraza de dx en $\mathrm{F}/\mathrm{K}(x)$. Por el Teorema 1.70

$$(dx)_{\mathrm{F}} = Con_{\mathrm{F}/\mathrm{K}(x)}(\mathrm{dx})_{\mathrm{K}(x)} Diff_{\mathrm{F}/\mathrm{K}(x)} = \mathrm{B}^{-2q+(m+1)(q-1)} = \mathrm{B}^{m(q-n-1)}.$$

Las diferenciales $\omega = x^r y^s dx$, con $r, s \geq 0$ tales que $(r+1)n + (s+1) \leq q$, son holomorfas. En efecto, para todo $\mathrm{P} \neq \mathrm{B}$ se cumple que $v_{\mathrm{P}}((\omega_{\mathrm{F}})) \geq 0$. Para el lugar B tenemos lo siguiente

$$\begin{aligned} v_{\mathrm{B}}((\omega)_{\mathrm{F}}) &= r v_{\mathrm{B}}((x)_{\mathrm{F}}) + s v_{\mathrm{B}}((y)_{\mathrm{F}}) + v_{\mathrm{B}}((dx)_{\mathrm{F}}) \\ &= -rq - sm + m(q-n-1) = -rq + m(q-(n+s+1)) \\ &\geq -rq + m(q + (rn-q)) = r(mn-q) \\ &= r \geq 0. \end{aligned}$$

Sea $\{a_{r,s} \,|\, r, s \geq 0,\ (r+1)n+(s+1) \leq q\} \subseteq \mathrm{K}$ tal que $\sum_{r,s} a_{r,s}(x^r y^s dx) = 0$. Entonces $(\sum_{r,s} a_{r,s} x^r y^s)dx = 0$, luego $\sum_{r,s} a_{r,s} x^r y^s = 0$, pues dx es una diferencial distinta de cero (Teorema 1.70). Así, el polinomio $\sum_{r,s} a_{r,s} x^r X^s$ con coeficientes en $\mathrm{K}(x)$ tiene como raíz a y y es de grado menor que q, pero como $[\mathrm{F} : \mathrm{K}(x)] = q$ todos los $a_{r,s}$ son cero. Por lo tanto $\mathrm{H} = \{x^r y^s dx \,|\, r, s \geq 0,\ (r+1)n + (s+1) \leq q\}$ es linealmente independiente sobre K con g elementos y consiste de diferenciales holomorfas, es decir,

H es una base de las diferenciales holomorfas.
Sea $a \in L((dx)_{\mathrm{F}}^{-1})$. Entonces adx es una diferencial holomorfa y por lo tanto $adx = \sum_{r,s} a_{r,s}x^r y^s dx$, donde $a_{r,s} \in \mathrm{K}$. Se sigue que $a = \sum_{r,s} a_{r,s}x^r y^s$. Ya que $\ell((dx)_{\mathrm{F}}^{-1}) = g$ y los g elementos $x^r y^s$ en $L((dx)_{\mathrm{F}}^{-1})$ generan a este espacio sobre K el conjunto $\{x^r y^s \mid r, s \geq 0,\ (r+1)n + (s+1) \leq q\}$ es una base.
Los órdenes del Wronskiano $W_y(x^r y^s \mid r, s \geq 0,\ (r+1)n+(s+1) \leq q)$ *son* $\{rq+s\}_{r,s}$.
Para encontrar los órdenes del Wronskiano $W_y(x^r y^s \mid r, s \geq 0,\ (r+1)n + (s+1) \leq q)$ utilizaremos el Teorema 3.14. Primero debemos de encontrar las series de potencias $\phi(x^r y^s)$ con $D = D_y$ (ver (1)). Se tiene lo siguiente $Y = \phi(y) = y + u$ y $X = \phi(x) = x + \sum_{n=1}^{\infty} D_y^{(n)}(x)u^n$. Por otro lado $y^q - y = x^m = x^{\frac{q+1}{n}}$, así $x = (y^q - y)^{\frac{n}{q+1}}$. Ya que $\frac{1}{q+1} = q^2 - q + 1 - \frac{q^3}{q+1}$ se sigue que

$$x = (y^q - y)^{\frac{n}{q+1}} = (y^q - y)^{n(q^2-q+1)}(y^q - y)^{-\frac{n}{q+1}q^3} = (y^q - y)^{n(q^2-q+1)}x^{-q^3}.$$

Por lo tanto

$$X = (Y^q - Y)^{n(q^2-q+1)}X^{-q^3}. \tag{5}$$

Ahora, $X^{q^3} = x^{q^3} + u^{q^3}R(u)$ para algún $R(u) \in \mathrm{F}[[u]]$. Así

$$X^{-q^3} = x^{-q^3} - u^{q^3}R_1(u) \quad \text{para algún} \quad R_1(u) \in \mathrm{F}[[u]].$$

Usando (5) obtenemos que

$$X \equiv (y^q - y + u^q - u)^{n(q^2-q+1)}x^{-q^3} \text{ mód } (u^{q+1}).$$

También

$$\begin{aligned}(y^q - y + u^q - u)^{n(q^2-q)} &= (y^{q^2} - y^q - u^q + u^{q^2})^{n(q-1)} \\ &\equiv (y^{q^2} - y^q)^{n(q-1)} - n(q-1)(y^{q^2} - y^q)^{n(q-1)-1}u^q \text{ mód } u^{q+1}\end{aligned}$$

y

$$\begin{aligned}(y^q - y + u^q - u)^n &\equiv (y^q - y - u)^n + n(y^q - y - u)^{n-1}u^q \\ &\equiv (y^q - y - u)^n + n(y^q - y)^{n-1}u^q \text{ mód } u^{q+1}.\end{aligned}$$

Por lo tanto

$$\begin{aligned} X &\equiv (y^q - y + u^q - u)^{n(q^2-q)}(y^q - y + u^q - u)^n x^{-q^3} \\ &\equiv [(y^{q^2} - y^q)^{n(q-1)} - n(q-1)(y^{q^2} - y^q)^{n(q-1)-1}u^q] \\ &\quad [(y^q - y - u)^n + n(y^q - y)^{n-1}u^q]x^{-q^3} \equiv a(y^q - y - u)^n + bu^q \text{ mód } u^{q+1}. \end{aligned}$$

con

$$\begin{aligned} a &= x^{-q^3}[(y^{q^2} - y^q)^{n(q-1)} - n(q-1)(y^{q^2} - y^q)^{n(q-1)-1}u^q] \\ &= x^{-q^3}(y^q - y)^{n(q^2-q)-q}[(y^q - y)^q - n(q-1)u^q] \\ &= x^{-q^3}x^{mn(q^2-q)-mq}(x^{mq} - n(q-1)u^q) \neq 0 \quad \text{y} \\ b &= x^{-q^3}(y^{q^2} - y^q)^{n(q-1)}n(y^q - y)^{n-1} = nx^{-q^3}x^{mnq(q-1)}x^{m(n-1)} \neq 0. \end{aligned}$$

Así

$$X \equiv a(y^q - y - u)^n + bu^q \text{ mód } u^{q+1} \tag{6}$$

donde a y b son elementos no cero de F. Consideremos el K-espacio vectorial

$$L((dx)_{\mathrm{F}}^{-1}) = \bigoplus_{r,s} \mathrm{K}x^r y^s \quad \text{con} \quad (r+1)n + (s+1) \leq q,$$

y su respectivo F-espacio vectorial de series de potencias (ver Teorema 3.14)

$$\mathrm{U} = \bigoplus_{r,s} \mathrm{F}X^r Y^s \quad \text{con} \quad (r+1)n + (s+1) \leq q.$$

Deseamos encontrar los invariantes Hermitianos de U. Tenemos que

$$u^s = (Y - y)^s \equiv 0 \text{ mód } (\bigoplus_{i=0}^{s} \mathrm{F}Y^s), \tag{7}$$

y

$$\begin{aligned} (y^q - y - u)^n &= \sum_{m=0}^{n} \binom{n}{m} (y^q - y)^m (-1)^{n-m} u^{n-m} \\ &\in \sum_{m=0}^{n} \bigoplus_{i=0}^{n-m} \mathrm{F}Y^i = \bigoplus_{j=0}^{n} \mathrm{F}Y^j. \end{aligned}$$

Por lo tanto, usando (6) obtenemos que $X \equiv bu^q$ mód M_1 donde M_1 es el F-espacio vectorial $\langle u^{q+1}Z, Y^i \,|\, 0 \leq i \leq n\rangle$ para algún $Z \in \mathrm{F}[[u]]$. Ya que b es un elemento no cero de F, se sigue que $u^q \in \langle u^{q+1}Z, X, Y^i \,|\, 0 \leq i \leq n\rangle \subseteq \langle u^{q+1}Z, X^jY^i \,|\, j + \frac{i}{n} \leq 1\rangle$. Entonces el F-espacio vectorial $\mathrm{M} = \bigoplus_{j+\frac{i}{n}\leq 1} \mathrm{F}X^jY^i$ contiene una serie de la forma $P = u^q + u^{q+1}P_1$. De esta manera $P^r \equiv 0$ mód $\bigoplus_{j+\frac{i}{n}\leq r} \mathrm{F}X^jY^i$ y por (7) tenemos que $P^ru^s \equiv 0$ mód $\bigoplus_{j+\frac{i}{n}\leq r,\, t\leq s} \mathrm{F}X^jY^{i+t}$. Escogemos $r, s \geq 0$ tales que $(r+1)n+(s+1) \leq q$. Ahora $nj + i \leq nr$, así

$$(j+1)n + (i+t+1) \leq nr + n + s + 1 = (r+1)n + (s+1) \leq q.$$

De ahí $P^ru^s \in \mathrm{U}$ para todo r, s tales que $(r+1)n + (s+1) \leq q$. Pero como $P^ru^s = u^{rq+s} + u^{rq+s+1}P_2$ existen g series de potencias de la forma P^ru^s en U. Luego el conjunto $\{P^ru^s \,|\, r, s \geq 0, (r+1)n+(s+1) \leq q\}$ es linealmente independiente sobre F y por lo tanto es una base de U, más aún, es una base Hermitiana de U. El conjunto de invariantes Hermitianos para esta base es

$$\{rq + s \,|\, r, s \geq 0, (r+1)n + (s+1) \leq q\}$$

Por el Teorema 3.14 los órdenes del determinante Wronskiano

$$W_y(x^ry^s \,|\, r, s \geq 0,\ (r+1)n + (s+1) \leq q)$$

son $\{rq + s\}_{r,s}$.
Finalmente por el Teorema 3.17 la sucesión laguna esta formada por los elementos del conjunto $\{rq + s + 1\}_{r,s}$. ■

En el contexto del Teorema 3.25, sean $m = q + 1$ y $q \geq 3$. Entonces $n = 1$ y el género de F es $\frac{q(q-1)}{2}$. De esta manera la sucesión laguna de este campo es

$$\begin{aligned}
&\{rq + s + 1 \,|\, r, s \geq 0, (r+1)n + (s+1) \leq q\} \\
&= \{rq + s + 1 \,|\, r, s \geq 0, (r+1) + (s+1) \leq q\} \\
&= \{rq + s + 1 \,|\, r, s \geq 0, r + s \leq q - 2\} \\
&= \{1, \ldots, q-1, q+1, \ldots\} \neq \{1, \ldots, q, \ldots, \frac{q(q-1)}{2}\}.
\end{aligned}$$

Apéndice A

Algebra

Este capítulo contiene los resultados sobre extensiones de Galois finitas con grupo de Galois abeliano (extensiones abelianas) que serán requeridos en capítulos anteriores. Cualquier extensión abeliana finita es una composición de extensiones cíclicas para las cuales su grado es una potencia de un primo. Por esta razón, solo trataremos con extensiones cíclicas F/E de grado p^n, $n \geq 1$, para p un primo fijo. En el caso de que F contenga una p^n-ésima raíz primitiva de la unidad existe una descripción explícita para tales extensiones, esto es el contenido del Teorema A.3. Los casos $p = \mathrm{car(F)}$ y $p \neq \mathrm{car(F)}$ son tratados separadamente. Si $p \neq \mathrm{car(F)}$, el resultado correspondiente es un caso particular del Teorema A.3. El caso clásico $p = \mathrm{car(F)}$ y $n = 1$ es el Teorema A.6, que es generalizado por el Teorema A.7.

A.1. Vectores de Witt

En esta sección introduciremos el anillo de vectores de Witt. Este anillo será utilizado para la caracterización de aquellas extensiones cíclicas en las cuales $p = \mathrm{car(F)}$. Empezaremos introduciendo el anillo de polinomios $\mathrm{A} = \mathbb{Q}[\mathrm{X}_i, \mathrm{Y}_j, \mathrm{Z}_k]$, donde $i, j, k = 0, 1, 2, \ldots$ y denotemos por $\mathrm{A}^{\mathbb{N}}$ al producto directo de $|\mathbb{N}|$ copias de A. Los elementos de A tienen la forma $x = (x_0, x_1, \ldots, x_{n-1}, x_n, \ldots)$ para algunos $x_i \in \mathrm{A}$. Dicho conjunto adquiere la estructura de un anillo si definimos la dos operaciones componente a componente. Nosotros queremos definir otra estructura de anillo sobre el conjunto $\mathrm{A}^{\mathbb{N}}$. Para esta sección p es un número primo fijo y utilizaremos la siguiente

notación

$$\pi(x) = (x_0^p, x_1^p, \ldots, x_{n-1}^p, \ldots)$$

Los elementos $x_0, x_1, \ldots, x_{n-1}, \ldots$ de $\mathrm{A}^{\mathbb{N}}$ definen elementos

$$x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}$$

de $\mathrm{A}^{\mathbb{N}}$ por las siguientes fórmulas de recursión:

$$x^{(0)} = x_0 \quad \text{y} \quad x^{(i+1)} = (\pi(x))^{(i)} + p^{i+1}x_{i+1} \tag{1}$$

con $x = (x_0, x_1, \ldots, x_{n-1}, \ldots)$. De (1) se sigue que

$$x^{(0)} = x_0 \quad \text{y} \quad x^{(i+1)} = x_0^{p^{i+1}} + px_1^{p^i} + \cdots + p^{i+1}x_{i+1} \tag{2}$$

Los elementos $x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}, \ldots$ de $\mathrm{A}^{\mathbb{N}}$ definen elementos $x_0, x_1, \ldots, x_{n-1}, \ldots$ de $\mathrm{A}^{\mathbb{N}}$ mediante las fórmulas de recursión inversas:

$$x_0 = x^{(0)} \quad \text{y} \quad x_{i+1} = (\frac{1}{p^{i+1}})(x^{(i+1)} - x_0^{p^{i+1}} - px_1^{p^i} - \cdots - p^i x_i^p) \tag{3}$$

Con el fin de facilitar la escritura resumiremos la anterior así

$$[x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}, \ldots] = (x_0, x_1, \ldots, x_{n-1}, x_n, \ldots)$$

donde $x_0, x_1, \ldots, x_{n-1}, x_n, \ldots$ están definidas en términos de $x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}, \ldots$ por (3). Definamos ahora una nueva estructura de anillo sobre el conjunto $\mathrm{A}^{\mathbb{N}}$. Dados

$$x = (x_0, x_1, \ldots, x_{n-1}, \ldots),\ y = (y_0, x_1, \ldots, y_{n-1}, \ldots) \in \mathrm{A}^{\mathbb{N}}$$

definimos $x + y$ y xy como sigue:

$$x + y = [x^{(0)} + y^{(0)}, x^{(1)} + y^{(1)}, \ldots, x^{(n-1)} + y^{(n-1)}, \ldots]$$
$$xy = [x^{(0)}y^{(0)}, x^{(1)}y^{(1)}, \ldots, x^{(n-1)}y^{(n-1)}, \ldots]$$

Este nuevo anillo sera denotado como $W(\mathrm{A})$.
El anillo $W(\mathrm{A})$ es un anillo conmutativo de característica cero. Además este anillo es isomorfo a $\mathrm{A}^{\mathbb{N}}$ bajo la función

$$[x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}, \ldots] \mapsto (x_0, x_1, \ldots, x_{n-1}, \ldots)$$

Nos detendremos a analizar a los elementos $\mathrm{X}+\mathrm{Y}$ y XY, donde

$$\mathrm{X}=(\mathrm{X}_0,\mathrm{X}_1,\ldots,\mathrm{Y}_{n-1},\ldots) \quad \text{y} \quad \mathrm{Y}=(\mathrm{Y}_0,\mathrm{Y}_1,\ldots,\mathrm{Y}_{n-1},\ldots)$$

De (2) y (3) derivamos las igualdades

$$\begin{aligned}(\mathrm{X}+\mathrm{Y})_0 &= \mathrm{X}_0+\mathrm{Y}_0, (\mathrm{XY})_0=\mathrm{X}_0\mathrm{Y}_0\\ (\mathrm{X}+\mathrm{Y})_1 &= \mathrm{X}_1+\mathrm{Y}_1+(\frac{1}{p})(\mathrm{X}_0^p+\mathrm{Y}_0^p-(\mathrm{X}_0+\mathrm{Y}_0)^p)\\ (\mathrm{XY}) &= \mathrm{X}_0^p\mathrm{Y}_1+\mathrm{X}_1\mathrm{Y}_0^p+p\mathrm{X}_1\mathrm{Y}_1 \end{aligned} \tag{4}$$

En general, se tiene que $(\mathrm{X}+\mathrm{Y})_i$ y $(\mathrm{XY})_i$ son polinomios con coeficientes racionales en $\mathrm{X}_0,\mathrm{Y}_0,\ldots,\mathrm{X}_i,\mathrm{Y}_i$. También se cumple que

$$(\mathrm{X}+\mathrm{Y})_i=\mathrm{X}_i+\mathrm{Y}_i+f(\mathrm{X}_0,\mathrm{Y}_0,\ldots,\mathrm{X}_{i-1},\mathrm{Y}_{i-1}) \tag{5}$$

donde $f(\mathrm{X}_0,\mathrm{Y}_0,\ldots,\mathrm{X}_{i-1},\mathrm{Y}_{i-1})$ es un polinomio con coeficientes racionales en las variables indicadas. El siguiente teorema está demostrado en [8]

TEOREMA A.1 *Para $i\in\{0,1,2,\ldots\}$,*

$$(\mathrm{X}+\mathrm{Y})_i \text{ y } (\mathrm{XY})_i \text{ están en } \mathbb{Z}[\mathrm{X}_0,\mathrm{Y}_0,\ldots,\mathrm{X}_i,\mathrm{Y}_i]$$

Para cada $i\geq 0$ escribiremos $(\mathrm{X}+\mathrm{Y})_i=a_i(\mathrm{X}_r,\mathrm{Y}_s)$, $(\mathrm{XY})_i=m_i(\mathrm{X}_r,\mathrm{Y}_s)$, con $0\leq r,s\leq i$. Entonces, para cualesquiera $x,y\in W(\mathrm{A})$

$$(x+y)_i=a_i(x_r,y_s) \text{ y } (xy)_i=m_i(x_r,y_s) \tag{6}$$

Sea R un anillo conmutativo y sean $\alpha_i(\mathrm{X}_r,\mathrm{Y}_s)$ y $\mu_i(\mathrm{X}_r,\mathrm{Y}_s)$, donde $0\leq r,s\leq i$, los polinomios obtenidos de $a_i(\mathrm{X}_r,\mathrm{Y}_s)$ y $m_i(\mathrm{X}_r,\mathrm{Y}_s)$, respectivamente, al reemplazar sus coeficientes $c\in\mathbb{Z}$ por el elemento $\delta_c=c\cdot 1_{\mathrm{R}}$ del anillo primo de R. Ahora tenemos lo necesario para definir el anillo de Witt $W(\mathrm{R})$ de R y el n-ésimo anillo de Witt $W_n(\mathrm{R})$. Los elementos de $W(\mathrm{R})$ son sucesiones infinitas $a=(a_i)=(a_0,a_1,\ldots,a_{n-1},\ldots)$, $a_i\in\mathrm{R}$, con la igualdad de elementos definida de forma usual. Si $a=(a_i)$, $b=(b_i)$ son elementos de $W(\mathrm{R})$, definimos una adición y una multiplicación en $W(\mathrm{R})$ por

$$(a+b)_i=\alpha_i(a_r,b_s)\ ,\ (ab)_i=\mu_i(a_r,b_s) \qquad (0\leq r,s\leq i). \tag{7}$$

Los elementos de $W_n(\mathrm{R})$ son sucesiones finitas $a = (a_i) = (a_0, a_1, \ldots, a_{n-1})$, $a_i \in \mathrm{R}$, nuevamente la igualdad de dos elementos se define usualmente, pero con las operaciones de adición y multiplicación dadas por (7). Definamos ahora las funciones π y π_n como sigue:

$$\begin{array}{cc} \pi : W(\mathrm{R}) \to W(\mathrm{R}) & \pi : W_n(\mathrm{R}) \to W_n(\mathrm{R}) \\ (x_i) \mapsto (x_i^p) & (x_0, \ldots, x_{n-1}) \mapsto (x_0^p, \ldots, x_{n-1}^p) \end{array}$$

Teorema A.2 *Sea* R *un anillo conmutativo de característica* p *y sea* $n \geq 1$. *Entonces* $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ *es el anillo primo de* $W_n(\mathrm{R})$, *la característica de* $W_n(\mathrm{R})$ *es* p^n *y la de* $W(\mathrm{R})$ *es cero. Además* π *y* π_n *son homomorfismos de anillos.*

Este teorema está demosatrado en [8].

A.2. Extensiones Cíclicas

Los resultados que mencionaremos acontinuación no estarán acompañados de una demostración. Sus demostraciones las podemos encontrar en [8].

Teorema A.3 *Sea* $n \geq 1$ *un número entero, sea* F *un campo que contiene una raíz* n*-ésima primitiva de la unidad y sea* E/F *una extensión de campos.*

(*i*) E/F *es cíclica de grado un divisor de* n *si y sólo si* $\mathrm{E} = \mathrm{F}(\lambda)$ *para algún* $\lambda \in \mathrm{E}$ *tal que* $\lambda^n \in \mathrm{F}$.

(*ii*) *El polinomio mínimo sobre* F *de cualquier* $\lambda \in \mathrm{E}$ *con* $\lambda^n \in \mathrm{F}$ *es* $\mathrm{X}^d - \lambda^d$, *para algún* $d|n$.

Corolario A.4 *Sea* E/F *una extensión de grado* n *y supongamos que* F *contiene una raíz* n*-ésima primitiva de la unidad. Entonces* E/F *es cíclica si y sólo si* $\mathrm{E} = \mathrm{F}(\lambda)$ *para algún* $\lambda \in \mathrm{E}$ *tal que* $\mathrm{X}^n - \lambda^n$ *es el polinomio mínimo de* λ *sobre* F.

Corolario A.5 *Sea* n *un entero positivo y sea* F *un campo que contiene a todas las raíces* n*-ésimas de la unidad de una cerradura algebraica* $\bar{\mathrm{F}}$ *de* F. *Si* $\lambda \in \bar{\mathrm{F}}$ *es separable sobre* F *y* $\lambda^n \in \mathrm{F}$, *entonces* $\mathrm{F}(\lambda)/\mathrm{F}$ *es cíclica de grado un divisor de* n.

TEOREMA A.6 *Sea* F *un campo de característica* $p > 0$ *y sea* E/F *una extensión de campos.*

(*i*) E/F *es cíclica de grado* p *si y sólo si* $\mathrm{E} = \mathrm{F}(\lambda)$ *para algún* $\lambda \in \mathrm{E}$ *tal que* $\lambda^p - \lambda \in \mathrm{F}$ *y* $\lambda \notin \mathrm{F}$.

(*ii*) *El polinomio mínimo sobre* F *de cualquier* $\lambda \in \mathrm{E}$ *con* $\lambda^p - \lambda \in \mathrm{F}$ *y* $\lambda \notin \mathrm{F}$ *es* $\mathrm{X}^p - \mathrm{X} - (\lambda^p - \lambda)$.

(*iii*) *Para cualquier* $a \in \mathrm{F}$, *el polinomio* $\mathrm{X}^p - \mathrm{X} - a$ *es irreducible sobre* F *o se descompone en* p *factores lineales distintos sobre* F.

El teorema anterior es un caso particular del siguiente

TEOREMA A.7 *Sea* F *un campo de característica* $p > 0$, $n \geq 1$ *un número entero y* E/F *una extensión algebraica de campos. Entonces* E/F *es cíclica de grado* p^m, *con* $m \leq n$, *si y sólo si existen* $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ *en* E *tales que* $\mathrm{E} = \mathrm{F}(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ *y tal que el elemento* $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ *de* $W_n(\mathrm{E})$ *satisface que* $\pi(\lambda) - \lambda \in W_n(\mathrm{F})$. *Más aún, para cada* $a \in W_n(\mathrm{F})$, *existe una extensión cíclica* K/F *de grado un divisor de* p^n *y un elemento* $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ *en* $W_n(\mathrm{K})$ *tal que* $\pi(\lambda) - \lambda = a$.

OBSERVACIÓN. Supongamos que $\mathrm{E} = \mathrm{F}(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ es una extensión cíclica de F de grado p^m, $m \leq n$. Sea $\lambda \in W_n(\mathrm{E})$ tal que $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ y $\pi(\lambda) - \lambda \in W_n(\mathrm{F})$. Sea $\bar{\mathrm{E}}$ una cerradura algebraica de E. Notemos que, para $x \in W_n(\bar{\mathrm{E}})$,

$$(\pi(x) - x) - (\pi(\lambda) - \lambda) = 0$$

se tiene si y sólo si $\pi(x - \lambda) = x - \lambda$, lo cual es cierto si y sólo si $x - \lambda \in W_n(\mathbb{F}_p)$. Por lo tanto $\{\lambda + i | i \in \mathbb{Z}/p^n\mathbb{Z}\}$ es el conjunto de todas las raíces de $\pi(\mathrm{X}) - \mathrm{X} - (\pi(\lambda) - \lambda)$ en $W_n(\bar{\mathrm{E}})$ ya que $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$ por el Teorema A.2. Bajo estas condiciones tenemos el homomorfismo inyectivo

$$\begin{aligned} G(\mathrm{E}/\mathrm{F}) &\to W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z} \\ \sigma &\mapsto i_\sigma \end{aligned}$$

donde $\sigma(\lambda) = \lambda + i_\sigma$. Entonces $[\mathrm{E} : \mathrm{F}] = p^n$ si y sólo si este homomorfismo es suprayectivo. Si éste es el caso $[\mathrm{F}(\lambda_0, \lambda_1, \ldots, \lambda_i) : \mathrm{F}] = p^{i+1}$ para $0 \leq i \leq n - 1$.

En efecto, por el Teorema A.7 la extensión E_i/F, $\mathrm{E}_i = \mathrm{F}(\lambda_0, \lambda_1, \ldots, \lambda_i)$, es cíclica de grado p^m, $m \leq i+1$. Entonces existe un homomorfismo inyectivo

$$\begin{aligned} \varphi_i : G(\mathrm{E}_i/\mathrm{F}) &\to W_{i+1}(\mathbb{F}_p) = \mathbb{Z}/p^{i+1}\mathbb{Z} \\ \sigma &\mapsto j_\sigma \end{aligned}$$

donde $\sigma((\lambda_0, \lambda_1, \ldots, \lambda_i)) = (\lambda_0, \lambda_1, \ldots, \lambda_i) + j_\sigma$. Dado $j = (a_0, a_1, \ldots, a_n) \in W_n(\mathbb{F}_p)$ existe $\sigma \in G(\mathrm{E}/\mathrm{F})$ tal que $\sigma(\lambda) = \lambda + j$, luego $\sigma|_{\mathrm{E}_i}((\lambda_0, \lambda_1, \ldots, \lambda_i)) = (\lambda_0, \lambda_1, \ldots, \lambda_i) + (a_0, a_1, \ldots, a_i)$. Por lo tanto φ_i es sobre y esto implica que $[\mathrm{F}(\lambda_0, \lambda_1, \ldots, \lambda_i) : \mathrm{F}] = p^{i+1}$

A.3. Extensiones de Kummer

Sea F un campo y n un entero positivo. Decimos que una extensión de Galois E/F es de exponente n si el exponente de $G(\mathrm{E}/\mathrm{F})$ divide a n, es decir, si $\sigma^n = 1$ para toda $\sigma \in G(\mathrm{E}/\mathrm{F})$. Por una extensión de Kummer de exponente n, nosotros entenderemos a una extensión abeliana de exponente n finito, además suponemos que F contiene a una raíz n-ésima primitiva de la unidad ϵ_n. Para tales extensiones la característica de F no divide a n.

Usaremos el símbolo $\sqrt[n]{a}$, $a \in \mathrm{F}$, para denotar a cualquier elemento $\lambda \in \bar{\mathrm{F}}$ tal que $\lambda^n = a$ ($\bar{\mathrm{F}}$ es una cerradura algebraica de F). Existen n de tales elementos λ, a saber $\epsilon_n^i \lambda$, $0 \leq i \leq n-1$. Notemos que el campo $\mathrm{F}(\lambda)$ no depende de qué raíz n-ésima de a escojamos. Por ello denotaremos a este campo como $\mathrm{F}(\sqrt[n]{a})$. Denotemos por $(\mathrm{F}^*)^n$ al subgrupo de F^* que consiste de las n-ésimas potencias de elementos de F^*. Si H es un subgrupo de F^* que contiene a $(\mathrm{F}^*)^n$, denotaremos por F_H al compuesto de todos los campos $\mathrm{F}(\sqrt[n]{a})$ con $a \in \mathrm{H}$. F_H está unívocamente determinado por H como un subcampo de $\bar{\mathrm{F}}$. El siguiente resultado está demostrado en [8].

Lema A.8 (*i*) *Para cualquier subgrupo* H *de* F^* *que contenga a* $(\mathrm{F}^*)^n$, $\mathrm{F}_\mathrm{H}/\mathrm{F}$ *es una extensión de Kummer.*
(*ii*) *Si* E/F *es una extensión de Kummer de exponente* n, *entonces* $\mathrm{E} = \mathrm{F}_\mathrm{H}$ *con* $\mathrm{H} = (\mathrm{E}^*)^n \cap \mathrm{F}^*$.
(*iii*) E/F *es una extensión de Kummer de exponente* m *si y sólo si* F *contiene una raíz* m*-ésima primitiva de la unidad y* E *es el campo de descomposición de una familia de polinomios de la forma* $\mathrm{X}^m - a$, $a \in \mathrm{F}$.

Observación. Por el Teorema A.3 las extensiones cíclicas de Kummer de exponente n son de la forma $\mathrm{F}(\lambda)$ para algún $\lambda \in \mathrm{E}$ tal que $\lambda^n \in \mathrm{F}$.

Conclusiones

Sea F/K un campo de funciones para el cual su campo de constantes es algebraicamente cerrado de característica p positiva. Para las extensiones cíclicas F/K(x) de grado m (donde $(m, p) = 1$) con $m + 3$ lugares totalmente ramificados y de grado p^n ($n > 1$), existe una condición necesaria para que un lugar sea un punto de Weierstrass: un lugar totalmente ramificado es un punto de Weieratrass.

Bibliografía

[1] Accola, R.; *On Generalized Weierstrass Points on Riemann Surfaces.* Lecture Notes Math. Statist., Univ. Pittsburgh, Pittsburgh, PA. 5, 1-19, 1983.

[2] Bears, L.; *Riemann Surfaces.* New York University, 1957 – 1958.

[3] Boseck, H.; *Zur Theorie der Weierstrasspunkte.* Math. Nachr. 19, 29-63, 1958.

[4] Farkas, H.M. y Kra, I.; *Riemann Surfaces.* Springer-Verlag, 1980.

[5] Garcia, A.; *On Weierstrass Points on Artin-Schreier Extensions of* $k(x)$. Math. Nachr. 144, 233-239, 1989.

[6] Hasse, H.; *Theorie der relativ-zyklischen algebreischen Funktionenkörper.* Crelle's J. 172, 37-54, 1934.

[7] Hasse, H.; *Zur Theorie der Abstrakten elliptischen Funktionenkörper. I.* Crelle's J. 175, 55-92, 1936.

[8] Karpilovsky, G.; *Topics in Field Theory.* Nort-Holland, 1989.

[9] Lewittes, J.; *Automorphisms of compact Riemann Surfaces.* Amer. J. Math. 85, 734-752, 1963.

[10] Schmid, H.L.; *Zur Arithmetik der zyklischen p-Köper.* Crelle's J. 176, 1936.

[11] Schmidt, F.K.; *Zur Arithmetik Theorie der algebreischen Funktionen. II.* Math. Z. 45, 75-96, 1939.

[12] Springer, G.; *Riemann Surfaces.* Addison Wesley. 1957.

[13] Stichtenoth, H.; *Algebraic Function Fields and Codes.* Springer-Verlag, 1993.

[14] Valentini, R.C. y Madan, M.L.; *Weierstrass Points in Characteristic p.* Math. Ann. 247, 123-132, 1980.

[15] Villa, G.D.; *Introducción a la Teoría de las Funciones Agebraicas.* Fondo de Cultura Económica, 2003.

[16] Villa, G.D.; *Topics in the Theory of Algebraic Function Fields.* Birhäuser, Boston (Sometido).

[17] Witt, E.; *Zyklische Körper und Algebren der Charakteristik p vom Grade p^n. Struktur diskret bewerteter Körper mit vollkommenem Restklassenkörper der Charakteristik p.* Crelle's J. 176, 126-140, 1936

Índice alfabético