PUNTOS DE WEIERSTRASS Y CURVAS SOBRE CUERPOS FINITOS

ALEJANDRO SIMARRA CAÑATE

UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
PROGRAMA DE MAESTRÍA EN
CIENCIAS–MATEMÁTICAS
SANTIAGO DE CALI
2009

PUNTOS DE WEIERSTRASS Y CURVAS SOBRE CUERPOS FINITOS

ALEJANDRO SIMARRA CAÑATE

Trabajo de investigación presentado como requisito para optar al título de Magister en Matemáticas.

Director
Ph.D Álvaro Garzón Rojas

UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
PROGRAMA DE MAESTRÍA EN CIENCIAS–MATEMÁTICAS
SANTIAGO DE CALI
2009

FACULTAD DE CIENCIAS NATURALES Y EXACTAS

ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN DE MAESTRIA EN CIENCIAS-MATEMÁTICAS

Jurado conformado por los doctores:

1. CARLOS TRUJILLO, Universidad del Cauca

El día 18 de junio de 2009 a las 10:00 AM. se llevó a cabo la sustentación del Trabajo de Investigación **"PUNTOS DE WEIERSTRASS Y CURVAS SOBRE CUERPOS FINITOS"**, presentada por el estudiante ALEJANDRO SIMARRA CAÑATE, código 0605328, Plan 7179, candidato a grado para la próxima ceremonia.

RESULTADO DE LA EVALUACIÓN:

(X) APROBADA
( ) MERITORIA
( ) LAUREADA

Regístrese esta calificación.

( ) REPROBADA: El estudiante debe matricularse en esta actividad

( ) PENDIENTE: El estudiante debe acoger las recomendaciones del jurado y presentar nuevamente el documento ante el Director de Tesis. ( ) Requiere. ( ) No requiere nueva sustentación.

El plazo para nueva sustentación y/o presentación del documento es de: _____

OBSERVACIONES

Excelente presentación, se recomienda la publicación del trabajo. El estudiante contestó correctamente las preguntas del jurado.

Santiago de Cali, 18 de junio de 2009

GUILLERMO ORTIZ
JURADO

CARLOS TRUJILLO
JURADO

ALVARO SARZÓN
DIRECTOR

JHON JAIRO DUQUE
COORDINADOR DE LA SUSTENTACIÓN

Dedicatoria

A el, a usted y a mi.

RESUMEN

El estudio de puntos con coordenadas enteras o racionales en curvas y superficies, es decir definidas por ecuaciones del tipo $f(x, y) = 0$ ó $f(x, y, z) = 0$ data desde el siglo XII A.C. Sorprendentemente, el mismo problema en cuerpos finitos es de gran importancia para la teoría de números y códigos; pues este, es equivalente a la hipótesis de Riemann sobre cuerpos de funciones y los parametros de los códigos de Goppa dependen fuertemente del número de puntos racionales de la curva con la que se inducen.

Este trabajo tiene como finalidad, dar una prueba detallada de la hipótesis de Riemann sobre cuerpos finitos por medio de la teoría de puntos de Weierstrass. Dado un sistema lineal sin puntos básicos o un morfismo que va de la curva al espacio proyectivo enésimo, se obtiene una cota para el número de puntos racionales. Se llega a la cota por medio de una "aproximación lineal"; usando el plano osculador y los ordenes de Frobenius, que son invariantes de la curva respecto al sistema lineal (morfismo) y al cuerpo finito de base. Con dicha cota se prueba la hipótesis de Riemann para curvas sobre cuerpos finitos y se mejora la cota de Hasse–Weil en algunos casos particulares.

Palabras Claves: género, morfismo, sistema lineal, teorema de Bezout, teorema de Riemann-Roch, derivada de Hasse y laguna de Weierstrass.

Agradecimientos

- ***A la sociedad colombiana en la que vivo representada especialmente por los jueces de este trabajo.***
- ***A la Universidad del Valle, al Departamento de Matemáticas y a mis alumnos pues son el medio por el cual la sociedad me ha dado su educación.***
- ***Al profesor Álvaro Garzón por su colaboración y paciencia tanto en los aspectos académicos como espirituales.***
- ***A Gonzalo Garcia, Rocio Castillo, Alvaro Ortiz y Diana Narvaez que me han transmitido lo que significa vivir.***
- ***A todos mis compañeros del posgrado representados aquí por Horacio y Samin pues sin ellos no existiriamos.***
- ***A todos mis hermanos. En especial a Henry, Liliana–Helisto, Amalfy, Nicolas, Lorena y Liliana Posada. Ellos están en mi y yo en ellos.***
- ***A mis padres Nicolas Simarra y Noris Cañate por que me enseñan el camino para ser en Dios.***

INTRODUCCIÓN

El teorema de Fermat y la hipótesis de Riemann están entre los problemas más importantes de la Matemática. El primero afirma la no existencia de puntos racionales no triviales que satisfagan la ecuación diofántica $x^n+y^n = z^n$ $(n > 2)$ y el segundo que los ceros no triviales de la función zeta $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ viven en la linea $Re(s) = \frac{1}{2}$. Estos problemas estan relacionados con la geometría de las curvas algebraicas y la distribución de los números primos. Por tal razón, Gauss comienza un estudio detallado de las congruencias cuadraticas y cúbicas. Por ejemplo obtuvo el número de soluciones de la ecuación $ax^3-by^3 \equiv 1\ (mod\ p)$ para primos de la forma $p = 3n+1$. Luego, por medio de la geometría algebraica y con los trabajos de Riemann y Noether se obtuvieron serios avances. Ya en 1924 Artin, considero la congruencia $y^2 \equiv f(x)\ (mod\ p)$ y conjeturó que el número N de soluciones satisface que $N \leq p + 1 + 2p^{\frac{1}{2}}$ si el grado de f es 4 . Dicha conjetura fue probada pocos años despues por Hasse. Pero, fue con el uso de la teoría de la función zeta para curvas algebraicas proyectivas (cuerpos de funciones) que Weil probo en el año 1948 para una curva definida sobre un cuerpo finito $\mathbb{F}_q$, que $N \leq q+1+2q^{\frac{1}{2}}g$ donde g es el género de la curva y; además que dicha cota es equivalente a la hipótesis de Riemann sobre cuerpos finitos.

Más recientemente Stepanov, Schmidt y Bombieri dieron una prueba de forma más sencilla de la hipótesis de Riemann usando el método de Thue–Stepanov. De otro lado Serre, Stark, Drinfeld, Vladut e Ihara obtuvieron resultados que mejoran la cota de Hasse-Weil en algunos casos especiales.

El propósito de este trabajo es hacer una prueba autocontenida de la hipótesis de Riemann o de la cota de Hasse–Weil, usando teoría de puntos de Weierstrass; llenando los detalles del artículo *Weierstrass points and curves over finite fields* de Stohr y Voloch. Otra de nuestras contribuciones es una generalización tanto del método Stohr–Voloch como de algunos resultados subyacentes y la construcción de ejemplos que ilustran la teoría.

En el capítulo 1 se obtiene una cota para el número de puntos racionales N de una curva C usando el teorema de Bezout, se define el hiperplano osculador y el divisor de Ramificación de un sistema lineal $\mathfrak{D}$ con ayuda de sus invariantes y los invariantes hermitianos. Se generaliza también el concepto de punto de Weiestrass.

Seguidamente, en el capítulo 2, se demuestra el siguiente teorema:

TEOREMA PRINCIPAL

Sea C una curva algebraica proyectiva, no singular, de género g, definida sobre $\mathbb{F}_q$ y N el número de puntos racionales. Si existe un sistema lineal sin puntos básicos definido sobre $\mathbb{F}_q$ de grado d y dimensión n, con ordenes de Frobenius $v_0, \ldots, v_{n-1}$, entonces

$$N \leq \frac{\left(\sum_{i=0}^{n-1} v_i\right)(2g-2) + (q+n)d}{n}.$$

El teorema anterior es el resultado principal del trabajo y para su demostración es indispensable el divisor $\mathbb{F}_q$-Frobenius.

Por medio del teorema principal se demuestra la hipótesis de Riemann y se obtienen cotas mejores que esta para algunos casos particulares en el último capítulo.

Índice

1. SISTEMAS LINEALES Y PUNTOS DE WEIERSTRASS

El problema de acotar el número de *puntos racionales* de una curva definida sobre un cuerpo finito $\mathbb{F}_q$ es equivalente a la *hipótesis de Riemann sobre cuerpos de funciones*. Evidentemente una cota burda para dicho número es q^2+1. Pero si introducimos algunos *invariantes* de la curva podríamos obtener mejores cotas. Por ejemplo: si la curva es de grado d entonces otra cota es dq. Obsérvese que si $d<q$, entonces la segunda cota es mejor que la primera. El primer propósito de este capitulo es obtener una cota mejor que las anteriores usando el *teorema de Bezout*. Sin embargo, para poder refinar esta cota es necesario desarrollar por medio de *morfismos* una teoría geométrica algebraica que permita caracterizar la curva en términos locales y globales. Con este fin en mente, implementamos una teoría de morfismos, *sistemas lineales e invariantes hermitianos*. Seguidamente se estudian los *planos osculadores* de una curva en un punto genérico, pues esto permite obtener analiticamente los invariantes hermitianos. Luego complementamos nuestro estudio haciendo un análisis global. Esta es la causalidad para desarrollar una teoría de invariantes para sistemas lineales. Finalmente, al relacionar los invariantes hermitianos que son de carácter local, con los *invariantes de los sistemas lineales* (invariantes globales), resulta una generalización de los clásicos *puntos de Weierstrass*, que se convierten en el objeto de estudio del primer capitulo. Los puntos de Weierstrass se caracterizan por medio del *divisor de ramificación*.

1.1. Puntos racionales, su acotamiento y el teorema de Bezout

El teorema de Bezout es quizás el resultado más importante de la teoría de intersección desde el punto de vista de la geometría algebraica. Este tiene múltiples aplicaciones a problemas clásicos (véase Simarra [13]). A pesar de ser un resultado tan antiguo, nos permite obtener una cota del número de puntos racionales de una curva plana irreducible, que en algunos casos particulares es mejor que la cota de Hasse – Weil. Precisamente, tenemos el siguiente teorema:

Teorema 1.1.1. *Sea $f(X,Y)\in\mathbb{F}_q[X,Y]$ un polinomio absolutamente irreducible de grado d, donde la característica del cuerpo $\mathbb{F}_q$ es $\chi(\mathbb{F}_q)\neq 2$ y supongamos que f no divide a*

$$H\big(f(X,Y)\big)=f_{XX}f_Y^2-2f_{XY}f_Xf_Y+f_{YY}f_X^2.$$

Entonces, el número N de soluciones de la ecuación $f(X,Y)=0$ en $\mathbb{F}_q^2\cong\mathbb{A}^2(\mathbb{F}_q)$ satisface

$$N\leq\frac{1}{2}d(d+q-1)$$

Prueba.

Observe que $f_X \neq 0$ y $f_Y \neq 0$, pues en caso contrario $H\big(f(X,Y)\big) = 0$ y entonces $f(X,Y)$ divide a $H\big(f(X,Y)\big)$.

Sea $h(X,Y) = (X - X^q)f_X + (Y - Y^q)f_Y$. Claramente h se anula sobre todos los puntos racionales de f, más aún h puede verse como una función regular de

$$V(f) = \{(\alpha,\beta) \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} \text{ tales que } f(\alpha,\beta) = 0\},$$

esto es $h : V(f) \to k$ donde $k = \overline{\mathbb{F}_q}$, por lo tanto $h \in K(f) = k(x,y)$.

Veamos que la multiplicidad de los puntos $P = (x_0, y_0) \in \mathbb{A}^2(\mathbb{F}_q)$ en $h \in K(f) = k(x,y)$ es al menos 2. Para esto, probaremos que $dh(P) = 0$. En efecto (usando la regla de la cadena y del producto para la derivación d),

$$dh = (X - X^q)df_X + (Y - Y^q)df_Y + f_X dX + f_Y dY.$$

Ahora como $f(x,y) = 0$ entonces $df = f_X dX + f_Y dY = 0$, o equivalentemente

$$\frac{dY}{dX} = -\frac{f_X}{f_Y},$$

(pues d es una aplicación k-lineal). Así que $dh(P) = 0$. Por lo tanto la multiplicidad de P en h, $m_P(h) \geq 2$.

De manera que si suponemos que $h(Q) \neq 0$ para algún $Q \in V(f)$ entonces por el teorema de Bezout tenemos que $2N \leq \sum_{P \in V(f) \cap V(h)} m_P(f) m_P(h) \leq gr(f)gr(h) = d(d+q-1)$, pues $f(X,Y)$ es absolutamente irreducible. Se concluye finalmente que

$$N \leq \frac{1}{2} d(d+q-1).$$

De otro lado, si $h(X,Y) = (X - X^q)f_X + (Y - Y^q)f_Y = 0$ entonces dividiendo la ecuación anterior por $-f_Y$ tenemos que

$$(X - X^q)\frac{-f_X}{f_Y} - (Y - Y^q) = 0;$$

lo que es equivalente a

$$(X - X^q)\frac{dY}{dX} - (Y - Y^q) = 0,$$

y derivando respecto a X tenemos que

$$\frac{dY}{dX} + (X - X^q)\frac{d^2Y}{dX^2} - \frac{dY}{dX} = 0$$

si y sólo si

$$(X - X^q)\frac{d^2Y}{dX^2} = 0 \text{ si y sólo si } \frac{d^2Y}{dX^2} = 0.$$

Veamos ahora que $\dfrac{d^2Y}{dX^2} = 0$ implica que $f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2 = 0$; como función sobre $V(f)$, lo que es equivalente a la condición de divisibilidad de $f(X,Y)$ respecto a $H\big(f(X,Y)\big)$ por el teorema de Bezout o por la definición del cuerpo de funciones, $K\big(V(f)\big) = k(x,y)$.

Consecuentemente, $h(X,Y) = (X - X^q)f_X + (Y - Y^q)f_Y = 0$ si y sólo si,

$$\frac{f_X}{f_Y} = -\frac{Y - Y^q}{X - X^q} = -\frac{dY}{dX}.$$

Así

$$\begin{aligned} 0 \;=\; h_X \;&=\; f_X + (X - X^q)\big[f_{XX} + f_{XY}\tfrac{dY}{dX}\big] \\ &\quad + \tfrac{dY}{dX}f_Y + (Y - Y^q)\big[f_{YX} + f_{YY}\tfrac{dY}{dX}\big] \\ &= \; f_X + (X - X^q)\big[f_{XX} - f_{XY}\tfrac{f_X}{f_Y}\big] \\ &\quad - \tfrac{f_X}{f_Y}f_Y + (Y - Y^q)\big[f_{YX} - f_{YY}\tfrac{f_X}{f_Y}\big] \end{aligned}$$

Luego

$$f_{XX} - f_{XY}\frac{f_X}{f_Y} = -\frac{Y - Y^q}{X - X^q}\left(f_{XY} - f_{YY}\frac{f_X}{f_Y}\right)$$

si y sólo si,

$$f_{XX} - f_{XY}\frac{f_X}{f_Y} = \frac{f_X}{f_Y}\left(f_{XY} - f_{YY}\frac{f_X}{f_Y}\right)$$

y multiplicando por f_Y^2 obtenemos que

$$f_{XX}f_Y^2 - f_{XY}f_Xf_Y = f_X\big[f_{XY}f_Y - f_{YY}f_X\big]$$

y por lo tanto

$$f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2 = 0. \qquad \boxdot$$

Cabe decir que en la demostración del teorema anterior hemos hecho uso de las clausuras proyectivas de las curvas en cuestión, para poder usar de forma estricta el teorema de Bezout.

Observación 1.1.2. *La condición* $\dfrac{d^2Y}{dX^2} = 0$ *significa que al menos un punto de la curva* $V(f)$ *no es de inflexión, lo contrario sucede sólo cuando* f *es una linea o en su defecto cuando la característica del cuerpo* $\mathbb{F}_q$, $\chi(\mathbb{F}_q) \leq d$.

Esto se justificará plenamente en la siguiente sección. Sin embargo lo explicaremos ahora usando un método elemental, interesante y relevante por lo que epistemologicamente representa en este trabajo. Es decir, analizaremos de donde proviene la función $H\big(f(X,Y)\big)$ y la condición que se le impuso en la hipótesis.

Sea $A = (a_{ij}) \in M_n(k)$ donde $M_n(k)$ es el conjunto de matrices n por n con coeficientes en un cuerpo perfecto k. Denotaremos por A_i (A^j) a la i (j)-ésima fila (columna) de A. La transpuesta de A se denotará por ${}^tA$.

El grupo $GL_{n+1}(k)$ de matrices invertibles de dimensión $n+1$, actua transitivamente sobre $\mathbb{P}^n(k)$ en la forma usual, más precisamente, tenemos la acción $\phi : GL_{n+1}(k) \times \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ definida así:

$$\phi(A, P) = (A_0 \cdot {}^tP : \ldots : A_n \cdot {}^tP),$$

donde ${}^tP$ es el transpuesto de $P := (x_0 : \ldots : x_n) \in \mathbb{P}^n(k)$. De otro lado, si $A \in GL_{n+1}(k)$, la aplicación $T_{\phi_A} := \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ definida por $T_{\phi_A}(P) := \phi(A, P)$, es un cambio de coordenadas proyectivas (esto es, T_{ϕ_A} es un isomorfismo del espacio proyectivo $\mathbb{P}^n(k)$), luego para todo j, definimos

$$T^j_{\phi_A}(P) := {}^tA^j \cdot {}^tP = P \cdot A^j = \sum_{i=0}^{n} x_i a_{ij}.$$

Para cada $F \in k[X_0, \ldots, X_n]$ y todo cambio de coordenadas proyectivas T, usaremos el símbolo F^T para denotar la composición $F\big(T(X_0, \ldots, X_n)\big)$ y para cada n-úpla de polinomios $F_0, \ldots, F_n \in k[X_0, \ldots, X_n]$ definimos $(F_0, \ldots, F_n)^T$ como $(F_0^T, \ldots, F_n^T)$.

Como es usual, para cada $F \in k[X_0, \ldots, X_n]$ el *Hessiano* de F, $H(F)$ se define como

$$H(F) = \det\big(F_{ij}\big) = \det\big([\nabla F_i]\big).$$

donde F_i denota la derivada parcial de F con respecto a la variable X_i, esto es $F_i = \dfrac{\partial F}{\partial X_i}$.

Proposición 1.1.3. *Supongamos que $\chi(k) \neq 2$, $n = 2$, $P = (0 : 0 : 1)$, F es absolutamente irreducible, $p > d = gr(F) \geq 2$ y además, que Y es la linea tangente a F en P, entonces:*

1. $H(F^{T_{\phi_A}}) = \det(A)^2 H(F)^{T_{\phi_A}}$ *para toda* $A \in GL_{n+1}(k)$.
2. $I(P, F \cap H(F)) = I(P_*, f \cap g)$ *donde* $g = f_{XX} f_Y^2 - 2 f_{XY} f_X f_Y + f_{YY} f_X^2$ *y* $f = F_*$.
3. $P \in F \cap H(F)$, *si y sólo si,* P *es un punto múltiple o un flex.*
4. *La función inducida por* g *o* $H(f) = H(F)_*$ *en* $K(F)$ *es no nula, si y sólo si, existen puntos simples de* F *que no son de inflexión.*

Prueba.
Usando la regla del producto y de la cadena para derivadas tenemos que

$$\begin{array}{rclcl}(F^{T_{\phi_A}})_i & = & \nabla F\big(T_{\phi_A}(X_0,\ldots,X_n)\big)\frac{\partial T_{\phi_A}}{\partial X_i} & = & (F_0^{T_{\phi_A}},\ldots,F_n^{T_{\phi_A}})\cdot(a_{0,i},a_{1,i},\ldots,a_{n,i}) \\ & = & \sum_{m=0}^n a_{m,i}F_m^{T_{\phi_A}} & = & \Big(\sum_{m=0}^n a_{m,i}F_m\Big)^{T_{\phi_A}} \\ & = & T^i_{\phi_A}(F_0,\ldots,F_n)^{T_{\phi_A}} & = & T^i_{\phi_A}(\nabla F)^{T_{\phi_A}}\end{array} \tag{1}$$

De otro lado

$$\begin{aligned}\big[T^i_{\phi_A}(\nabla F)\big]_j &= \big[T^i_{\phi_A}(F_0,\ldots,F_n)\big]_j \\ &= \nabla T^i_{\phi_A}(F_0,\ldots,F_n)\cdot(F_{0,j},\ldots,F_{n,j}) \\ &= (a_{0,i},\ldots,a_{n,i})\cdot(F_{0,j},\ldots,F_{n,j}) \\ &= \textstyle\sum_{m=0}^n a_{m,i}F_{j,m} \\ &= T^i_{\phi_A}(F_{j,0},\ldots,F_{j,n}) \\ &= T^i_{\phi_A}(\nabla F_j)\end{aligned}$$

Luego aplicando convenientemente la ecuación (1) obtenemos que

$$\begin{aligned}(F^{T_{\phi_A}})_{ij} &= [T^i_{\phi_A}(\nabla F)^{T_{\phi_A}}]_j \\ &= T^j_{\phi_A}\Big(\nabla\big(T^i_{\phi_A}(\nabla F)\big)\Big)^{T_{\phi_A}} \\ &= T^j_{\phi_A}\Big(\big([T^i_{\phi_A}(\nabla F)]_0,\ldots,[T^i_{\phi_A}(\nabla F)]_n\big)\Big)^{T_{\phi_A}} \\ &= T^j_{\phi_A}\Big(\big(T^i_{\phi_A}(\nabla F_0),\ldots,T^i_{\phi_A}(\nabla F_n)\big)\Big)^{T_{\phi_A}}\end{aligned}$$

Así,

$$\begin{aligned}H(F^{T_{\phi_A}}) &= \det\Big(\big[(F^{T_{\phi_A}})_{ij}\big]\Big) \\ &= \det\left(\left[T^j_{\phi_A}\Big(\big(T^i_{\phi_A}(\nabla F_0),\ldots,T^i_{\phi_A}(\nabla F_n)\big)\Big)^{T_{\phi_A}}\right]\right) \\ &= \det\left(\Big[T^i_{\phi_A}\big((\nabla F_0)^{T_{\phi_A}}\big),\ldots,T^i_{\phi_A}\big((\nabla F_n)^{T_{\phi_A}}\big)\Big]\cdot A\right)\end{aligned}$$

y

$$\begin{aligned} H(F^{T_{\phi_A}}) &= \det\left(\left[T^i_{\phi_A}\big((\nabla F_0)^{T_{\phi_A}}\big),\ldots,T^i_{\phi_A}\big((\nabla F_n)^{T_{\phi_A}}\big)\right]\cdot A\right) \\ &= \det\left({}^tA\cdot\left[(\nabla F_j)^{T_{\phi_A}}\right]\cdot A\right) \\ &= \det(A)^2\det\left(\left[(\nabla F_j)^{T_{\phi_A}}\right]\right) \\ &= \det(A)^2 H(F)^{T_{\phi_A}}. \end{aligned}$$

Luego, $V\big(H(F^{T_{\phi_A}})\big) = V\big(H(F)^{T_{\phi_A}}\big)$.

Para demostrar 2, consideramos las variables usuales $X = X_0,\ Y = X_1$ y $Z = X_2$. Así

$$\begin{aligned} H(F) &= \det\begin{pmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{pmatrix} \\ &= \tfrac{1}{Z}\det\begin{pmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ ZF_{ZX} & ZF_{ZY} & ZF_{ZZ} \end{pmatrix} \\ &= \tfrac{1}{Z}\det\begin{pmatrix} F_{XX} & F_{XY} & \cdots \\ F_{YX} & F_{YY} & \cdots \\ XF_{XX}+YF_{XY}+ZF_{XZ} & XF_{YX}+YF_{YY}+ZF_{YZ} & \cdots \end{pmatrix} \\ &= \tfrac{1}{Z}\det\begin{pmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ (d-1)F_X & (d-1)F_Y & (d-1)F_Z \end{pmatrix} \\ &= \tfrac{1}{Z^2}\det\begin{pmatrix} F_{XX} & F_{XY} & (d-1)F_X \\ F_{YX} & F_{YY} & (d-1)F_Y \\ (d-1)F_X & (d-1)F_Y & d(d-1)F \end{pmatrix} \\ &= (d-1)\tfrac{1}{Z^2}\det\begin{pmatrix} F_{XX} & F_{XY} & F_X \\ F_{XY} & F_{YY} & F_Y \\ (d-1)F_X & (d-1)F_Y & dF \end{pmatrix} \end{aligned}$$

y

$$\begin{aligned} H(F) &= (d-1)\tfrac{1}{Z^2}\Big[F_{XX}\big(-(d-1)F_Y^2+dF_{YY}F\big)\\ &\quad -F_{XY}\big(-(d-1)F_XF_Y+dF_{XY}F\big)\\ &\quad +F_X\big((d-1)F_YF_{XY}-(d-1)F_{YY}F_Z\big)\Big]\\ &= -(d-1)^2\tfrac{1}{Z^2}(F_{XX}F_Y^2-2F_{XY}F_XF_Y+F_{YY}F_X^2)\\ &\quad +d(d-1)\tfrac{1}{Z^2}(F_{XX}F_{YY}-F_{XY}^2)F, \end{aligned}$$

donde la primera igualdad se obtiene usando la estructura de álgebra de $k[X,Y,Z]$; la tercera igualdad multiplicando la primera fila por X, la segunda fila por Y y sumando ambas a la tercera fila. La cuarta igualdad se tiene en virtud del teorema de *Euler* (véase [13], Teo. 2.2.1). Las siguientes igualdades se obtienen de forma análoga pero operando por columnas y expandiendo el determinante por cofactores (véase Lang [9]). Por lo tanto, $I\big(P, F\cap H(F)\big) = I\big(P_*, F_*\cap H(F)_*\big) = I(P_*, f\cap g)$ usando las propiedades del número de intersección (Simarra [13], Sec. 4.3).

Ahora $P\in F\cap H(F)$ si y sólo si, $P_*\in F_*\cap H(F)_* = f\cap g$. Si P es un punto simple entonces podemos suponer que Y es tangente a F en P ([13], Teo. 3.5.2) y $f = F_* = F(X,Y,1) = Y+aX^2+bXY+cY^2+dX^3+r(X,Y)$ donde cada término de $r(X,Y)$ tiene grado ≥ 3. De otro lado F es absolutamente irreducible, si y sólo si, f es absolutamente irreducible ([13], Lema 5.3.1) y F tiene un número finito de puntos múltiples por [13], Prop 6.1.4.

Por lo tanto, $g = 2a+Xr_1(X,Y)+Yr_2(X,Y)$ cuando $P=(0:0:1)$ es simple ($r_s(X,Y)\in \mathbb{F}_q[X,Y]$) y entonces, $P\in F\cap H(F)$ si y sólo si, P es un punto múltiple ($F_X(P)=F_Y(P)=F_Z(P)=0$. Vease [13], Prop. 6.1.1) o un punto de inflexión ($2a=0$ si y sólo si, $a=0$ en característica impar) y se obtiene el numeral 3. El item 4 se obtiene por el teorema de Bezout pues $0\neq g\in K\big(V(f)\big)$ y debido a que todo punto simple $P\in V(F)$ es de inflexión, si y sólo si, $\dfrac{d^2Y}{dX^2}(P)=0$.

Por lo tanto usando la forma de la ecuación (1) tenemos que $f = Y\big(1+J(X,Y)\big)+X^m\big(a+XG(X)\big)$ donde $m\geq 2$, $a\neq 0$ y $0\neq a+XG(X)\in\mathbb{F}_q[X]$ pues f es absolutamente irreducible. Claramente con las consideraciones anteriores, si $gr(F)<p=\chi(k)$ entonces $\dfrac{d^2Y}{dX^2}\neq 0$. Luego, $\dfrac{d^2Y}{dX^2}=0$ sólo si F es una linea o cuando $\chi(k)\leq gr(F)$. ⊡

Adicionalmente la afirmación del párrafo anterior implica que si F es cúbica (elíptica) e irreducible entonces F tiene al menos un punto de inflexión. También $H(F)=0$ como función cuando p divide a $d-1$.

Ejemplo 1.1.4. *Considérese a* $f(x,y) = y^3 + y - x^4$ *y* $k = \overline{\mathbb{F}_9}$. *La primera cota de acuerdo a lo comentado al inicio del capitulo es* $4 \times 9 = 36$. *Por el teorema tendríamos que* $N \leq 24$. *Sin embargo este resultado no es aplicable pues no se cumplen las hipótesis del Teorema 1.1.1. Por supuesto, esta curva es la famosa* hermitiana *y tiene propiedades muy interesantes (véase Stichtenoth [16], Ej VI.3.6, pág. 198 y el Capitulo 2 de este trabajo).* ⊡

Ejemplo 1.1.5. *Sea* $f(x,y) = y^5 + y - x^3$ *en* $\mathbb{F}_5$. *Aquí se satisfacen claramente las condiciones del teorema 1.1.1 y* $N \leq 22$. *Esta es mejor que las cotas triviales ya mencionadas y en este caso da un estimativo mejor que la cota de Hasse – Weil.* ⊡

La dificultad de obtener un resultado análogo al teorema 1.1.1 en característica 2 es que las derivadas de orden 2 se anulan. Obsérvese que en general, las derivadas de orden p se anulan cuando la característica de $\mathbb{F}_q$ es p. Esto nos dice que si existe alguna forma de generalizar el resultado, entonces debemos modificar o redefinir el concepto de derivada de orden superior.

1.2. Morfismos vs sistemas lineales. Invariantes hermitianos

Sean C una curva irreducible, no singular, algebraica y proyectiva de género $g(C) = g$, definida sobre un cuerpo algebraicamente cerrado k de característica p, denotaremos por $k(C)$ el cuerpo de funciones racionales de C y por $\nu_P : k(C) \to \mathbb{Z} \cup \{\infty\}$ la valuación localizada en un punto k-racional P de C. Un morfismo $f : C \to \mathbb{P}^n(k)$ es una aplicación de la forma $f = (f_0 : \ldots : f_n)$ donde $f_i \in k(C)$ $(i = 0, 1, \ldots, n)$, ó $f \in \mathbb{P}^n\big(k(C)\big)$.

Proposición 1.2.1. *Si* $f : C \to \mathbb{P}^n(k)$ *es un morfismo, entonces las* f_i *son únicas salvo un factor de proporcionalidad* $h \in k(C)^*$.

Prueba:
Supongamos que $f = (f_0 : \ldots : f_n) = (g_0 : \ldots : g_n)$, entonces $f_i(P) = h(P)g_i(P)$ para algún $h(P) \in k^*$ y todo i. Así que $f_i g_j = g_i f_j$ para $0 \leq i, j \leq n$,

Ahora, puesto que $0 \neq f_j \in k(C)$ para algún j entonces $g_j \neq 0$, luego si definimos $h = \dfrac{g_j}{f_j} \in k(C)^*$ tenemos que $hf_i = \dfrac{g_j}{f_j} f_i = g_i$ para todo i. Concluimos entonces que $f = (hf_0 : \ldots : hf_n)$ para algún $h \in k(C)$. ⊡

Sean $P \in C$ y t un parámetro P-uniformizante. Si denotamos por $e_P = -\min\{\nu_P(f_0), \ldots, \nu_P(f_n)\}$ entonces por la proposición (1.2.1)

$$f(P) = \big([t^{e_P} f_0](P) : \ldots : [t^{e_P} f_n](P)\big).$$

Supondremos de ahora en adelante que $f(C)$ no está contenida en ningún hiperplano

$H \subset \mathbb{P}^n(k)$, (esto nos asegura que $f_i \neq 0$ para todo i), luego asociamos a f el divisor

$$E = \sum_{P \in C} e_P P \in \mathcal{D}_C. \tag{2}$$

Observe que el divisor E está bien definido pues cada $f_i \in k(C)$ tiene un número finito de ceros y polos (Véase Stichtenoth [16], Cor I.3.4).

Dado un hiperplano $H = \sum_{i=0}^n a_i X_i$ de $\mathbb{P}^n(k)$ entonces $P \in f^{-1}(H) \iff f(P) \in H \iff H\big(f(P)\big) = 0$. Esto tiene como implicación que

$$\begin{array}{rclcl} \nu_P\big(f^{-1}(H)\big) & = & \nu_P\big(H(f)\big) & = & \nu_P\big(\sum_{i=0}^n a_i t^{e_P} f_i\big) \\ & = & \nu_P\big(t^{e_P}\sum_{i=0}^n a_i f_i\big) & = & \nu_P\big(\sum_{i=0}^n a_i f_i\big) + e_P. \end{array}$$

El hecho anterior nos permite definir el divisor de intersección correspondiente a H.

Definición 1.2.2 (*Divisor de Intersección y Sistema Lineal de Secciones Hiperplanas*)**.** *El* divisor de intersección *de la curva parametrizada f correspondiente a un hiperplano H es*

$$f^{-1}(H) = div\left(\sum_{i=0}^n a_i f_i\right) + E.$$

Al sistema lineal

$$\mathfrak{D} = \{f^{-1}(H) \in \mathcal{D}_C : H \subset \mathbb{P}^n(k) \text{ es un hiperplano}\}.$$

se le llama sistema lineal de secciones hiperplanas*.*

La notación escogida para el divisor de intersección de H se debe a que en el caso en que $C \subseteq \mathbb{P}^n(k)$ y $f = id_C$ entonces $f^{-1}(H) = C \cap H$ y dicha intersección es preferible concebirla como un divisor de intersección $\operatorname{div}(H) = \sum_{P \in C} I(P, C \cap H)P$ para tener más información. Además, si suponemos que f es birracional entonces f conserva multiplicidades y

$$gr\big(\operatorname{div}(C \cap H)\big) = \sum_{P \in C} I(P, C \cap H) = gr(C)gr(H) = gr(C)$$

por el teorema de Bezout (véase Hartshorne [5], Teo I.7.7).

Proposición 1.2.3. *El divisor de intersección $f^{-1}(H)$ es invariante bajo equivalencias. Además, si T es un cambio de coordenadas inducido por la matriz $A = (a_{ij}) \in GL_{n+1}(k)$ y $g = T \circ f$, entonces f y g inducen el mismo divisor E y el mismo sistema lineal $\mathfrak{D}$.*

Prueba.
Supongamos que representamos a f por $hf = (hf_0 : \ldots : hf_n)$ con $h \in k(C)^*$, entonces

$$\begin{array}{rcl} e'_P & = & -\min\{\nu_P(hf_0), \ldots, \nu_P(hf_n)\} \\ & = & -\min\{\nu_P(h) + \nu_P(f_0), \ldots, \nu_P(h) + \nu_P(f_n)\} \\ & = & -\big(\min\{\nu_P(f_0), \ldots, \nu_P(f_n)\} + \nu_P(h)\big) \\ & = & e_P - \nu_P(h) \end{array}$$

Luego

$$E' = \sum_{P \in X} e'_P P = E - \operatorname{div}(h). \tag{3}$$

y $E \sim E'$. Así,

$$\begin{aligned} [hf]^{-1}(H) &= \operatorname{div}\big(\textstyle\sum_{i=0}^{n} a_i h f_i\big) + E' \\ &= \operatorname{div}\big(\textstyle\sum_{i=0}^{n} a_i f_i\big) + \operatorname{div}(h) + E - \operatorname{div}(h) \\ &= f^{-1}(H). \end{aligned}$$

De otro lado, si T es un cambio de coordenadas proyectivas, entonces $T \circ f = g = (g_0 : \ldots : g_n)$ con $g_i = \sum_{j=0}^{n} a_{ij} f_j$.

Supongamos que $A^{-1} = (b_{ij})$ y que m y r son enteros tales que $\nu_P(f_m) = \min\{\nu_P(f_0), \ldots, \nu_P(f_n)\}$ y $\nu_P(g_r) = \min\{\nu_P(g_0), \ldots, \nu_P(g_n)\}$. Claramente $f_i = \sum_{j=0}^{n} b_{ij} g_j$. Luego, existen s y u enteros tales que $a_{rs},\ b_{mu} \neq 0$ porque en caso contrario concluimos que $\det(A) = 0$ y/o $\det(A^{-1}) = 0$ que no puede ser. Así, por las propiedades de la P-valuación tenemos que

$$\begin{array}{lllll} \nu_P(g_r) & \geq & \min\{\nu_P(a_{r0} f_0), \ldots, \nu_P(a_{rn} f_n)\} & \geq & \nu_P(f_s) \\ & \geq & \nu_P(f_m) & \geq & \min\{\nu_P(b_{m0} g_0), \ldots, \nu_P(b_{mn} g_n)\} \\ & \geq & \nu_P(g_u) & \geq & \nu_P(g_r) \end{array}$$

Luego, $\nu_P(f_m) = \nu_P(g_r)$ y los morfismos inducen el mismo divisor E. Puesto que $f^{-1}(H) = g^{-1}\big(T(H)\big)$ donde H es un hiperplano de $\mathbb{P}^n(k)$ entonces f y g inducen el mismo sistema lineal de secciones hiperplanas. ⊡

Proposición 1.2.4. *El sistema lineal de secciones hiperplanas $\mathfrak{D}$ no tiene puntos básicos (s.p.b). Es decir, no existe P tal que $D \geq P$ para todo divisor $D \in \mathfrak{D}$.*

Prueba.

En efecto, supongamos que $D \geq P$ para todo $D \in \mathfrak{D}$ y algún $P \in C$. Luego $f(P) = \big(f_0(P) : \ldots : f_n(P)\big) \in H$ para todo hiperplano $H \subset \mathbb{P}^n(k)$. En particular, si $H = X_j$ entonces $f_j(P) = 0$ para todo j, lo cual es absurdo. ⊡

De acuerdo con la proposición anterior concluimos que cada morfismo f determina un sistema lineal s.p.b. El recíproco también es cierto como lo establece el siguiente resultado. Antes de enunciarlo estableceremos algo de notación.

Denotaremos por $SL(C)$ al conjunto de sistemas lineales *sin puntos básicos* contenidos en $\mathcal{D}_C$, por $Hom(C)$ al conjunto de morfismos de C en $\mathbb{P}^m(k)$ donde m es un entero positivo y para cada divisor $A \in \mathcal{D}_C$ asociamos el k-espacio vectorial

$$L(A) = \{f \in K(C); (f) + A \geq 0\},$$

cuya dimensión denotaremos por $l(A)$.

Proposición 1.2.5. *Cada sistema lineal s.p.b.* $\mathfrak{D} \subset |E| = \{div(f)+E \in \mathcal{D}_C : f \in L(E)\}$[1] *induce un único morfismo (salvo equivalencias).*

Prueba.

Primero, observemos que es posible dotar a $|E|$ de una estructura de espacio proyectivo $\mathbb{P}\big(L(E)\big)$.

En efecto, si $B = \{g_0, \ldots, g_{l(E)-1}\}$ es una base para $L(E)$, todo elemento $\mathrm{div}(f) + E \in |E|$ puede escribirse de manera única como $\mathrm{div}(\lambda_0 g_0 + \cdots + \lambda_{l(E)-1} g_{l(E)-1}) + E$, con $\lambda_0, \ldots, \lambda_{l(E)-1} \in k$. Luego tenemos una biyección

$$\begin{array}{ccc} |E| & \longrightarrow & \mathbb{P}\big(L(E)\big) \cong \mathbb{P}\big(\mathbb{A}^{l(E)}(k)\big) = \mathbb{P}^{l(E)-1}(k) \\ \mathrm{div}(\lambda_0 g_0 + \cdots + \lambda_{l(E)-1} g_{l(E)-1}) + E & \longrightarrow & (\lambda_0 : \cdots : \lambda_{l(E)-1})_B \end{array}$$

De otro lado, no es dificil probar que $\mathfrak{D}$ es un subespacio proyectivo de $|E|$, (generado por el conjunto $\{z \in L(E); (z) + E \in \mathfrak{D}\}$).
Supongamos que $B' = \{f_0, \ldots, f_n\}$ es una base para $\mathfrak{D}$. Por lo tanto, tenemos una aplicación

$$\begin{array}{ccc} SL(C) & \longrightarrow & Hom(C) \\ \mathfrak{D} = \Big\{\mathrm{div}\big(\sum_{i=0}^{n} \lambda_i f_i\big) + E : \lambda_i \in k\Big\} & \longrightarrow & f(P) = \big(f_0(P) : \cdots : f_n(P)\big) \end{array}$$

El morfismo f es único salvo equivalencias puesto que éste depende completamente de la base B'. ⊡

Definición 1.2.6 (Dimensión y grado de un sistema lineal)**.** *Para un sistema lineal s.p.b.* $\mathfrak{D} \subset |E|$ *definimos el grado y la dimensión proyectiva de* $\mathfrak{D}$ *como*

$$grad(\mathfrak{D}) := grad(E) \ y \ \dim(\mathfrak{D}) := \dim(E) - 1$$

Definición 1.2.7 (Invariantes hermitianos)**.** *Sea* P *un punto de* C*. Un entero positivo* j *se llama* P*-invariante hermitiano o simplemente* $(\mathfrak{D}, P)$*-orden, si existe un divisor* $D \in \mathfrak{D}$ *tal que* $\nu_P(D) = j$*.*

El siguiente resultado nos proporciona una relación entre los $(\mathfrak{D}, P)$-órdenes y las *lagunas de Weierstrass* en P.

Lema 1.2.8 (Noether)**.** *Sean* D *y* $E \in \mathcal{D}_C$*. Si* E *es un divisor canónico, entonces*

$$l\big(E - (D + P)\big) < l(E - D) \iff l(D + P) = l(D). \tag{4}$$

[1] Un sistema lineal $|E|$ de este tipo se llama completo.

Prueba.

Por el Teorema de Riemann-Roch

$$l(D+P) = gr(D+P) + 1 - g + l\big(E-(D+P)\big) = gr(D) + 1 - g + 1 + l\big(E-(D+P)\big)$$

y

$$l(D) = gr(D) + 1 - g + l\big(E-D\big).$$

Luego,

$$\begin{aligned} l(D+P) &= l(D) \quad \text{si y sólo si,} \\ l(E-D) &= 1 + l(E-(D+P)) \text{ si y sólo si,} \\ lE-(D+P)) &< l(E-D). \end{aligned}$$

⊡

Ahora consideramos el caso en que $\mathfrak{D}$ es un *sistema lineal canónico*, es decir cuando cada $E \in \mathfrak{D}$ es un divisor canónico.

Proposición 1.2.9. *Un entero j es un $(\mathfrak{D}, P)$-orden, si y sólo si, $j+1$ es una laguna de Weierstrass. Es decir, no existe una función racional en C, regular fuera de P que tenga un polo de orden $j+1$.*

Prueba. Sea E un divisor canónico en $\mathfrak{D}$. Puesto que $\mathfrak{D}$ es s.p.b. consideremos un elemento $D \in \mathfrak{D}$ tal que $D \ngeq P$, (esto es $\nu_P(D) = 0$) y $l(D) \geq 1$.

Ahora $E \sim D$ si y sólo si, $E = D + \operatorname{div}(g)$ para algún $g \in L(D)$. Entonces, $\nu_P(E) = j$ si y sólo si, $\nu_P(g) = j$ si y sólo si, $l(D-jP) > l\big(D-(j+1)P\big)$ si y sólo si, $l(jP) = l\big((j+1)P\big)$ si y sólo si, $j+1$ es una laguna de Weierstrass. ⊡

Ahora procedemos a hacer una caracterización de los $(\mathfrak{D}, P)$-ordenes en el caso general.

Definición 1.2.10 (Subespacios hermitianos)**.** *Sea P un punto de C y $\mathfrak{D}$ un sistema lineal s.p.b. Definimos para cada $i \in \mathbb{Z}_0^+$ el subespacio $\mathfrak{D}_i(P) = \{D \in \mathfrak{D} : D \geq iP\}$ que denotaremos sin hacer referencia al punto P por $\mathfrak{D}_i$ y que se llama subespacio hermitiano i–ésimo.*

Observe que $\mathfrak{D} = \mathfrak{D}_0 \supseteq \mathfrak{D}_1 \supseteq \mathfrak{D}_2 \supseteq \cdots$, además si $D = E + \operatorname{div}(g)$ y $D' = E + \operatorname{div}(g')$ son elementos de $\mathfrak{D}_i$, entonces $D + \lambda D' \in \mathfrak{D}_i$ pues $\nu_P(D + \lambda D') \geq \min\{\nu_P(D), \nu_P(\lambda D')\} \geq i$ para todo $\lambda \in k$, luego $\mathfrak{D}_i \subseteq \mathfrak{D}$ es un subespacio.

Más aún, $D \in \mathfrak{D}_i \subset |E|$, si y sólo si, existe $g \in k(C)$ tal que

$$D = \operatorname{div}(g) + E \geq iP$$

equivalentemente,

$$\operatorname{div}(g) + E - iP \geq 0$$

esto es,

$$g \in L(E - iP).$$

En consecuencia, $\mathfrak{D}_i \subseteq |E|_i = \mathbb{P}\big(L(E - iP)\big)$ donde

$$|E|_i = \{\mathrm{div}(g) + E \in \mathcal{D}_C : g \in L(E - iP)\}.$$

Observe además que de acuerdo con la demostración de la proposición 1.2.5, $\dim\big(|E|_i\big) = l(E - iP) - 1$. Luego

$$\begin{aligned} \dim\big(|E|_j\big) - \dim\big(|E|_{j+1}\big) &= l(E - jP) - l\big(E - (j+1)P\big) \\ &\leq gr(E - jP) - gr\big(E - (j+1)P\big) \\ &\leq 1. \end{aligned}$$

Ahora puesto que $\mathfrak{D}_j = \mathfrak{D} \cap |E|_j$ entonces

$$\dim\big(\mathfrak{D}_j\big) - \dim(\mathfrak{D}_{j+1}) \leq \dim\big(|E|_j\big) - \dim\big(|E|_{j+1}\big) \leq 1.$$

En resumen, tenemos:

Proposición 1.2.11. *Un entero j es un $(\mathfrak{D}, P)$-orden si y sólo si, $\mathfrak{D}_j \neq \mathfrak{D}_{j+1}$.* ⊡

Además, puesto que el grado de un divisor principal es cero, entonces $\mathfrak{D}_i = \emptyset$ si $i > d = gr(\mathfrak{D})$. Como $\dim(\mathfrak{D}) = n$ entonces tenemos exactamente $n + 1$ invariantes hermitianos. Denotamos al invariante i-ésimo por j_{i-1}. Luego tenemos que $j_0 < j_1 < \cdots < j_n \leq d$. Ahora como $\mathfrak{D}$ es s.p.b., entonces $j_0 = 0$.

Ejemplo 1.2.12. Sea $C = \mathbb{P}^1(k)$ con k es algebraicamente cerrado. Obsérvese que C puede considerarse como la recta $Y = 0$ en $\mathbb{P}^2(k)$ y $k(C) = k(x)$ donde x es la función coordenada.

El sistema lineal $\mathfrak{D} = |nP_\infty|$ no tiene puntos básicos $\big($el punto $P_\infty = (0 : 1)$ y $n \in \mathbb{Z}^+\big)$. Por el Teorema de Riemann-Roch, una base de $L(nP_\infty)$ es $\{1, x, x^2, \ldots, x^n\}$. Luego, el morfismo correspondiente a $|nP_\infty|$ es $f = (1 : x : \ldots : x^n)$.

Sea $P = (1 : 0) \in C$. Puesto que $\mathrm{div}(x^i) = iP - iP_\infty$ y $\nu_P\big(\mathrm{div}(x^i) + nP_\infty\big) = i$, entonces $j_i = i$ es el $i + 1$-ésimo $(|nP_\infty|, P)$-orden. ⊡

Consideremos el sistema lineal $\mathfrak{D}$ contenido en $|E|$ de una curva C. Luego, si $gr(E) = d > 2g - 2$ entonces por el Teorema de Riemann-Roch

$$n = \dim\big(\mathfrak{D}\big) \leq \dim\big(|E|\big) = l(E) - 1 = gr(E) + 1 - g - 1 = d - g.$$

Mas aún, si $gr(E - iP) = d - i > 2g - 2$ entonces

$$\dim\big(\mathfrak{D}_i\big) \leq \dim\big(|E|_i\big) = l(E - iP) - 1 = gr(E) - i - g.$$

Observación 1.2.13. *Si $\mathfrak{D} = |E|$, es un sistema lineal completo y $d - i > 2g - 1$ ($i < d - 2g + 1$), entonces $j_i = i$.*

Nótese que $d - i > d - (i + 1) > 2g - 2$. Luego

$$\dim\big(|E|_i\big) = d - i - g > d - (i + 1) - g = \dim\big(|E|_{i+1}\big).$$

y $|E|_i \supset |E|_{i+1}$. De manera que $j_i \leq i$ e $i = j_i$. ⊡

1.3. Planos osculadores

Estudiaremos ahora el comportamiento local de las curvas. Para esto se usa geometricamente el concepto de plano osculador emulando la geometría diferencial. Para precisar ideas y trasladar nuestro análisis al punto origen del espacio proyectivo es conveniente el siguiente lema:

Lema 1.3.1. *Sea S un k-subespacio vectorial de hiperplanos de $\mathbb{P}^n(k)$. Entonces, dada una base $\{H_0, \ldots, H_m\}$ de S, existe un isomorfismo $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ tal que*

$$T(H_j) = H_j^T = X_{n-j}.$$

Más aún,

$$T\Big(\bigcap_{H \in S} H\Big) = T\big(V(H_0, H_1, \ldots, H_m)\big) = V(X_{n-m}, X_{n-m+1}, \ldots, X_n).$$

El lema anterior nos afirma que es suficiente intersecar un conjunto finito de hiperplanos de una colección arbitraria de los mismos debido a su dependencia lineal. Una prueba del Lema se puede ver en Simarra [13], Sec. 3.5 teo 3.5.1.

Sea $Hyp^{(i)}(P) = \{H \subset \mathbb{P}^n(k) : H$ es un hiperplano y $\nu_P\big(f^{-1}(H)\big) \geq i\}$ donde f es el morfismo inducido por el sistema lineal $\mathfrak{D}$. Tenemos entonces la siguiente biyección denotada consecuentemente por f:

$$\begin{array}{rcl} f : \mathfrak{D}_i & \to & Hyp^{(i)}(P) \\ D = f^{-1}(H) & \to & f(D) = H \end{array} \tag{5}$$

Definición 1.3.2 (Planos osculadores)**.** *Sea C una curva, P un punto de C e i un entero entre 0 y $n-1$. Al conjunto*

$$L_i = \bigcap_{f^{-1}(H)\in\mathfrak{D}_{j_{i+1}}} H$$

se le llama i-ésimo plano osculador en P. En particular a L_{n-1} se le llama hiperplano osculador.

Debido al Lema 1.2.8 y a la biyección obtenida en la ecuación (5) entonces

$$L_i = \bigcap_{H\in Hyp^{(i+1)}(P)} H \text{ y } \dim(L_i) = i,$$

pues $\dim\big(Hyp^{(i+1)}(P)\big) = n-(i+1)$. Por lo anterior queda justificado el nombre de L_{n-1}. También, $L_0 = f(P)$ y L_1 es la recta tangente a $f(X)$ en $f(P)$ porque $I\big(P, X\cap f^{-1}(L_1)\big) \geq j_2 \geq 2$. Además, obsérvese la similitud de la serie $L_0 \subset \cdots \subset L_{n-1}$ con el marco de Frenet. También, P es una rama no singular de $f(C)$ si y sólo si, $j_1 = 1$, pues L^* es una recta que interseca a $f(C)$ transversalmente en $f(P)$ si y sólo si, $I\big(P, C\cap f^{-1}(L^*)\big) = m_P(C)m_P\big(f^{-1}(L^*)\big) = 1$.

Hasta ahora se ha hecho una descripción puramente general de los planos osculadores. Sin embargo es deseable tener una descripción algebraica y analítica de los mismos, en términos de las componentes del morfismo f. Esto se hace usando derivadas de orden superior. En característica cero las derivadas usuales son suficientes. Pero en característica p las derivadas de orden mayor o igual a p se anulan. Esto nos dice que se requiere otro tipo de derivación de orden superior (véase W. M. Schmidt [14], Sec. I.6, pág. 27).

Definición 1.3.3 (Derivada de Hasse)**.** *Sea $k[t]$ el anillo de polinomios en una indeterminada e i un entero no negativo. Al operador k-lineal $D_t^{(i)} : k[t] \to k[t]$ definido por*

$$D_t^{(i)}\Big(\sum_j c_j t^j\Big) = \sum_j \binom{j}{i} c_j t^{j-i}$$

se le llama hiperderivada *o* derivada de Hasse *i-ésima.*

En la definición se supone que $\binom{j}{i} = 0$ si y sólo si, $i > j$.

La definición anterior se puede extender a $k(t)$ y a cualquier extensión finita separable del mismo (véase W. Schmidt [14], Cap. III, Sec. 8, pág. 125).

Observación 1.3.4. *Observe que la derivada usual se relaciona con la derivada de Hasse mediante la siguiente fórmula. Si $g(t)$ es un polinomio de $k[t]$ entonces*

$$g^{(i)}(t) = i!D_t^{(i)}\big(g(t)\big)$$

Definición 1.3.5 (Derivadas vectoriales proyectivas)**.** *Sea* $f = (f_0 : \cdots : f_n) \in \mathbb{P}^n\big(k(C)\big)$ *un morfismo. La* hiperderivada vectorial *es la función* $D_t^{(i)} : \mathbb{P}^n\big(k(C)\big) \to \mathbb{A}^{n+1}\big(k(C)\big)$ *definida por*

$$D_t^{(i)} f = \big(D_t^{(i)} f_0, \cdots, D_t^{(i)} f_n\big)$$

La definición anterior depende de la representación en coordenadas del morfismo f. Sin embargo esto no afectará los dividendos de la misma. Además, denotaremos por $D_t^{(i)} f(P)$ al vector $\big(D_t^{(i)} f_0(P), \cdots, D_t^{(i)} f_n(P)\big)$.

Teorema 1.3.6. *Sea* t *un parámetro* P*-primo. Supongamos que la componente* P*-ésima del divisor* E *(véase la ecuación (2)),* e_P *es nula y que los* $(\mathfrak{D}, P)$*-órdenes* $j_0, j_1, \ldots, j_{i-1}$ *son conocidos. Entonces el* P*-invariante hermitiano* j_i *es el menor entero tal que* $\big\{D_t^{(j_0)} f(P), \ldots, D_t^{(j_{i-1})} f(P), D_t^{(j_i)} f(P)\big\}$ *es un conjunto linealmente independiente sobre* k*. Más aún, el* i*-ésimo plano osculador es generado por el conjunto de vectores* $\big\{D_t^{(j_0)} f(P), \ldots, D_t^{(j_{i-1})} f(P), D_t^{(j_i)} f(P)\big\}$.

Observe que la condición $e_P = 0$ siempre se puede obtener multiplicando por $h = t^{-e_P}$ al morfismo f.

Prueba.

Puesto que

$$L_i = \bigcap_{H \in Hyp^{(i+1)}(P)} H = \bigcap_{j=0}^{n-(i+1)} H_j$$

donde $H_0, \ldots, H_{n-(i+1)}$ son hiperplanos linealmente independientes de $Hyp^{(i+1)}(P)$ (Observe que en realidad los hiperplanos no dependen de i, excepto su cantidad por la dimensión de L_i).

Por el Lema 1.3.1 existe un isomorfismo $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ tal que $T(H_j) = X_{n-j}$ donde $X_0, X_1, \ldots, X_n$ son los hiperplanos coordenados. Luego por la Proposición 1.2.3

$$L_i = \big\{(x_0 : \cdots : x_n) | x_s = 0 \text{ siempre que } s > i\big\}.$$

Ahora, si $H \subset \mathbb{P}^n(k)$ es un hiperplano que intersecta a X en P con multiplicidad $m_P(H) \geq j_{i+1}$, entonces $L_i \subset H$ y como $H = \sum_{m=0}^{n} a_m X_m$ para algún $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$ entonces

$$H(x_0 : x_1 \cdots : x_i : 0 : \cdots : 0) = \sum_{m=0}^{i} a_m x_m = 0.$$

Por lo tanto, si $x_s = 1$ y $x_m = 0$ para todo $m \neq s$ entonces $a_s = 0$. Así, $a_0 = \cdots = a_i = 0$ y $H = \sum_{m=i+1}^{n} a_m X_m$.

De manera que

$$j_{i+1} = \text{mín}\left\{\nu_P\Big(\sum_{m=i+1}^{n} a_m f_m\Big) : a_{i+1}, \ldots, a_n \in k\right\},$$

y en consecuencia

$$j_n = \nu_P(a_n f_n) = \nu_P(f_n), j_{n-1} = \nu_P(f_{n-1}), \ldots, j_0 = \nu_P(f_0),$$

pues si x y y están en un anillo de valuación y $\nu(y) > \nu(x+y)$ entonces $\nu(x) = \nu(x+y-y) = \nu(x+y)$. Así, $f_i = c_i t^{j_i} + \sum_{m>j_i} b_{im} t^m \in k(C)$ donde $c_i \in k^*$.
Adicionalmente, $D_t^{(j_i)} f_i(P) = c_i$ y $D_t^{(j_i)} f_r(P) = 0$ si $i < r$. Luego la matriz

$$\begin{bmatrix} D_t^{(j_0)} f(P) \\ D_t^{(j_1)} f(P) \\ \vdots \\ D_t^{(j_i)} f(P) \end{bmatrix} = \begin{pmatrix} c_0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ D_t^{(j_1)} f_0(P) & c_1 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ D_t^{(j_i)} f_0(P) & D_t^{(j_i)} f_1(P) & \cdots & c_i & 0 & \cdots & 0 \end{pmatrix}$$

tiene filas linealmente independientes y por su forma generan a L_i. Es decir,

$$L_i = \text{span}\big\{D_t^{(j_0)} f(P), \ldots, D_t^{(j_i)} f(P)\big\}.$$

⊡

Observación 1.3.7. *Note que en la demostración del teorema 1.3.6 hemos probado que para cada punto $P \in C$ y para cada morfismo f podemos suponer que:*

1. $\nu_P(E) = e_P = 0$.
2. $f = (f_0 : \cdots : f_n)$ *es tal que* $f_i = c_i t^{j_i} + h_i(t)$ *donde* $\nu_P(h_i) > j_i$.
3. $f(P) = (1 : 0 : \cdots : 0)$.
4. $L_i = \cap_{j=i+1}^{n} X_j$.

⊡

De otro lado los invariantes hermitianos satisfacen una condición general especial de minimalidad.

Proposición 1.3.8. *Sean $m_0, m_1, \ldots, m_r$ enteros no negativos tales que $m_0 < m_1 < \cdots < m_r$. Si $D_t^{(m_0)} f(P), \ldots, D_t^{(m_r)} f(P)$ son vectores linealmente independientes entonces $j_i \leq m_i$ para $i = 0, 1, \ldots, r$.*

Prueba.

Los vectores $D_t^{(0)}f(P), D_t^{(1)}f(P), \ldots, D_t^{(j_i-1)}f(P)$ generan un espacio de dimensión i encajado en $\mathbb{A}^{n+1}(k)$. Por lo tanto $j_i - 1 < m_i$ y $j_i \leq m_i$. ⊡

Corolario 1.3.9. *El hiperplano osculador en $P \in X$ está dado por la ecuación*

$$\det \begin{pmatrix} X_0 & X_1 & \cdots & X_n \\ D_t^{(j_0)}f_0(P) & D_t^{(j_0)}f_1(P) & \cdots & D_t^{(j_0)}f_n(P) \\ \vdots & \vdots & \ddots & \vdots \\ D_t^{(j_{n-1})}f_0(P) & D_t^{(j_{n-1})}f_1(P) & \cdots & D_t^{(j_{n-1})}f_n(P) \end{pmatrix} = 0$$

⊡

Observe que de acuerdo con los resultados y caracterizaciones obtenidas hasta ahora, es razonable analizar bajo que circunstancias la sucesión de $(\mathfrak{D}, P)$-órdenes es distinta de la sucesión clásica $(0, 1, \ldots, n)$. Más precisamente queremos poder responder las siguientes preguntas:

1. ¿Existe un número finito de puntos cuya sucesión de invariantes hermitianos es clásica?
2. ¿Cual es la razón de cambio entre los puntos de la curva y sus invariantes hermitianos?
3. ¿Existen condiciones geométricas o algebraicas generales que permitan conocer explicitamente los invariantes hermitianos del morfismo respecto a ciertos puntos?

Definición 1.3.10 (Punto de osculación)**.** *Un punto $P \in C$ se llama punto de osculación de $\mathfrak{D}$ o punto de $\mathfrak{D}$-osculación si el último invariante hermitiano en P, $j_n > n$.*

La definición anterior permite clasificar los puntos donde el hiperplano osculador L_{n-1} intersecta a C con multiplicidad mayor que la dimensión del sistema lineal asociado a la curva. Estos son exactamente los puntos donde la sucesión de invariantes hermitianos no es clásica.

1.4. Invariantes de los morfismos

Para conocer el comportamiento de los invariantes hermitianos respecto a la variación de los puntos de una curva C, se hace un estudio de los *wronskianos* generalizados en $k(C)$

$$\det\left(D_t^{(m_i)}f_j\right) = \det \begin{pmatrix} D_t^{(m_0)}f_0 & D_t^{(m_0)}f_1 & \cdots & D_t^{(m_0)}f_n \\ \vdots & \vdots & \ddots & \vdots \\ D_t^{(m_n)}f_0 & D_t^{(m_n)}f_1 & \cdots & D_t^{(m_n)}f_n \end{pmatrix}$$

donde $m_i \in \mathbb{Z}_0^+$ y $f = (f_0 : \cdots : f_n) : C \to \mathbb{P}^n(k)$ es el morfismo correspondiente a un sistema lineal $\mathfrak{D}$. Se desarrollará un estudio similar al de las secciones 1.2 y 1.3 pero más general.

Sea t una variable separante de $k(C)/k$; es decir, $k(C)/k(t)$ es una extensión finita y separable. La existencia de variables separantes de un cuerpo de funciones algebraicas se justifica en Stichtenoth [16], Prop. III.9.2.

Observación 1.4.1 (Regla del producto y de la cadena de Hasse)**.** *La derivada de Hasse satisface:*

1. $D_t^{(m_i)}(hg) = \sum_{s=0}^{m_i} D_t^{(s)} h D_t^{(m_i-s)} g = h D_t^{(m_i)} g + \sum_{s=1}^{m_i} D_t^{(s)} h D_t^{(m_i-s)} g$ *para* $g, h \in k(C)$.
2. $D_u^{(m_i)} g = (\frac{dt}{du})^{m_i} D_t^{(m_i)} g + \sum_{s=0}^{m_i-1} A_{is} D_t^{(s)} g$ *para algunos* $A_{is} \in k(C)$.
3. $D_t^{(m)}\big(D_t^{(n)} g\big) = \binom{m+n}{m} D_t^{(m+n)} g$.
4. $D_t^{(m)} g^q = 0$ *si* m *no es múltiplo de* $q = p^n$*, donde* p *es la característica de* k.

La derivada de Hasse satisface propiedades adicionales las cuales están consignadas en Komiya [8], págs. 373 – 374 y W. Schmidt [14], Cap. I, Sec 6, pág. 27 – 31.

Proposición 1.4.2. *Sean* $m_0, \ldots, m_n$ *enteros no negativos.*

i) Si $g_i = \sum_{j=0}^n a_{ij} f_j$ *donde la matriz* $(a_{ij}) \in GL_{n+1}(k)$ *entonces*

$$\det\big(D_t^{(m_i)} g_j\big) = \det(a_{ij}) \det\big(D_t^{(m_i)} f_j\big).$$

Además, cuando

$$m_0 < m_1 < \cdots < m_n \text{ y } \langle D_t^{(m_0)} f, \ldots, D_t^{(m_{i-1})} f\rangle = \langle D_t^{(0)} f, D_t^{(1)} f, \ldots, D_t^{(m_i-1)} f\rangle$$

para $i = 1, 2, \ldots, n$*, se tienen los siguientes resultados:*

ii) Si $h \in k(C)$ *entonces*

$$\det\big(D_t^{(m_i)}(h f_j)\big) = (\epsilon + h) h^n \det\big(D_t^{(m_i)} f_j\big),$$

para algún $\epsilon \in k(C)$*. Ahora si* $m_0 = 0$ *entonces* $\epsilon = 0$ *y*

$$\det\big(D_t^{(m_i)}(h f_j)\big) = h^{n+1} \det\big(D_t^{(m_i)} f_j\big).$$

iii) Si $u \in k(C)$ *es otra variable separante de* $k(C)/k$ *entonces*

$$\det\big(D_u^{(m_i)} f_j\big) = \left(\Big(\frac{dt}{du}\Big)^{m_0} + \epsilon\right)\Big(\frac{dt}{du}\Big)^{\sum_{i=1}^n m_i} \det\Big(D_t^{(m_i)} f_j\Big),$$

para algún $\epsilon \in k(C)$*. Además, si* $m_0 = 0$ *entonces*

$$\det\big(D_u^{(m_i)} f_j\big) = \Big(\frac{dt}{du}\Big)^{\sum_{i=0}^n m_i} \det\big(D_t^{(m_i)} f_j\big)$$

Prueba.

Por la linealidad del operador $D_t^{(m_r)}$

$$D_t^{(m_r)} g_i = D_t^{(m_r)} \left(\sum_{j=0}^{n} a_{ij} f_j \right) = \sum_{j=0}^{n} a_{ij} D_t^{(m_r)} f_j.$$

Luego por la multiplicación de matrices tenemos

$$\begin{aligned}
\det\left(D_t^{(m_i)} g_j\right) &= \det \begin{pmatrix} \sum_{j=0}^{n} a_{0j} D_t^{(m_0)} f_j & \cdots & \sum_{j=0}^{n} a_{nj} D_t^{(m_0)} f_j \\ \vdots & \ddots & \vdots \\ \sum_{j=0}^{n} a_{0j} D_t^{(m_n)} f_j & \cdots & \sum_{j=0}^{n} a_{nj} D_t^{(m_n)} f_j \end{pmatrix} \\
&= \det \left(\begin{bmatrix} D_t^{(m_0)} f_0 & \cdots & D_t^{(m_0)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_n)} f_0 & \cdots & D_t^{(m_n)} f_n \end{bmatrix} \begin{bmatrix} a_{00} & \cdots & a_{n0} \\ \vdots & \ddots & \vdots \\ a_{0n} & \cdots & a_{nn} \end{bmatrix} \right) \\
&= \det \begin{pmatrix} a_{00} & \cdots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{n0} & \cdots & a_{nn} \end{pmatrix} \det \begin{pmatrix} D_t^{(m_0)} f_0 & \cdots & D_t^{(m_0)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_n)} f_0 & \cdots & D_t^{(m_n)} f_n \end{pmatrix} \\
&= \det(a_{ij}) \det\left(D_t^{(m_i)} f_j\right).
\end{aligned}$$

Por lo tanto se tiene $i)$

Para $ii)$ usamos fuertemente la Observación 1.4.1 y la hipótesis sobre los espacios generados. Claramente $D_t^{(m_0)}(hf_j) = hD_t^{(m_0)} f_0 + \sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_0$ y

$$\begin{aligned}
&\left(\textstyle\sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_0, \ldots, \sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_n \right) \\
&= \textstyle\sum_{s=1}^{m_0} \left(D_t^{(s)} h D_t^{(m_0-s)} f_0, \ldots, D_t^{(s)} h D_t^{(m_0-s)} f_n \right) = \epsilon\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big),
\end{aligned}$$

para algún $\epsilon \in k(C)$. De manera que $\epsilon = 0$ si $m_0 = 0$. Así, la primera fila de $\left(D_t^{(m_i)}(hf_j)\right)$ satisface que

$$\begin{aligned}
&\big(D_t^{(m_0)}(hf_0), \ldots, D_t^{(m_0)}(hf_n)\big) \\
&\quad = \big(hD_t^{(m_0)} f_0 + \textstyle\sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_0, \ldots, hD_t^{(m_0)} f_n + \sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_n\big) \\
&\quad = h\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big) + \left(\textstyle\sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_0, \ldots, \sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_n \right) \\
&\quad = h\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big) + \epsilon\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big) \\
&\quad = (\epsilon + h)\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big).
\end{aligned}$$

Luego por la Observación 1.4.1 y la linealidad del determinante

$$\det\left(D_t^{(m_i)}(hf_j)\right)$$

$$= \det\begin{pmatrix} (h+\epsilon)D_t^{(m_0)}f_0 & \cdots & (h+\epsilon)D_t^{(m_0)}f_n \\ hD_t^{(m_1)}f_0 + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_0 & \cdots & hD_t^{(m_1)}f_n + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_n \\ \vdots & \ddots & \vdots \\ hD_t^{(m_n)}f_0 + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_0 & \cdots & hD_t^{(m_n)}f_n + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_n \end{pmatrix}$$

$$= (h+\epsilon)\det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots & D_t^{(m_0)}f_n \\ hD_t^{(m_1)}f_0 + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_0 & \cdots & hD_t^{(m_1)}f_n + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_n \\ \vdots & \ddots & \vdots \\ hD_t^{(m_n)}f_0 + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_0 & \cdots & hD_t^{(m_n)}f_n + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_n \end{pmatrix}$$

Similarmente,

$$\left(\sum_{s=1}^{m_i} D_t^{(s)}hD_t^{(m_i-s)}f_0, \ldots, \sum_{s=1}^{m_i} D_t^{(s)}hD_t^{(m_i-s)}f_n\right) = \sum_{s=1}^{m_i}\left(D_t^{(s)}hD_t^{(m_i-s)}f_0, \ldots, D_t^{(s)}hD_t^{(m_i-s)}f_n\right)$$

pertenece al espacio (generado) $\langle D_t^{(m_0)}f, \ldots, D_t^{(m_{i-1})}f\rangle$ para $i = 1, 2, \ldots, n$. Por lo tanto, usando las propiedades del determinante tenemos que

$$\det\left(D_t^{(m_i)}(hf_j)\right)$$

$$= (h+\epsilon)\det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots & D_t^{(m_0)}f_n \\ hD_t^{(m_1)}f_0 + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_0 & \cdots & hD_t^{(m_1)}f_n + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_n \\ \vdots & \ddots & \vdots \\ hD_t^{(m_n)}f_0 + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_0 & \cdots & hD_t^{(m_n)}f_n + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_n \end{pmatrix}$$

$$= (h+\epsilon)\det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots & D_t^{(m_0)}f_n \\ hD_t^{(m_1)}f_0 & \cdots & hD_t^{(m_1)}f_n \\ \vdots & \ddots & \vdots \\ hD_t^{(m_n)}f_0 + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_0 & \cdots & hD_t^{(m_n)}f_n + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_n \end{pmatrix}$$

$$= (h+\epsilon)h\det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots & D_t^{(m_0)}f_n \\ D_t^{(m_1)}f_0 & \cdots & D_t^{(m_1)}f_n \\ \vdots & \ddots & \vdots \\ hD_t^{(m_n)}f_0 + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_0 & \cdots & hD_t^{(m_n)}f_n + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_n \end{pmatrix}$$

Reaplicando argumentos similares tenemos que

$$\det\left(D_t^{(m_i)}(hf_j)\right) = = (h+\epsilon)h^n \det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots & D_t^{(m_0)}f_n \\ D_t^{(m_1)}f_0 & \cdots & D_t^{(m_1)}f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_n)}f_0 & \cdots & D_t^{(m_n)}f_n \end{pmatrix}$$

y se tiene el resultado. Además, recuérdese que si $m_0 = 0$ entonces $\epsilon = 0$ y

$$\det\left(D_t^{(m_i)}(hf_j)\right) = h^{n+1}\det\left(D_t^{(m_i)}f_j\right).$$

El inciso *iii*) se obtiene de forma análoga al ii) pero usando la regla de la cadena para la derivada de Hasse (Observación 1.4.1, 2). Véase que el escalar h que sale repetidamente del determinante podría ser variable de fila a fila, pues det es una función multilineal. Es decir,

$$\begin{aligned}\det\left(D_u^{(m_i)}f_j\right) &= \left(\left(\tfrac{dt}{du}\right)^{m_0}+\epsilon\right)\det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots \\ \left(\frac{dt}{du}\right)^{m_0}D_t^{(m_1)}f_0 + \sum_{s=1}^{m_1} D_t^{(s)}hD_t^{(m_1-s)}f_0 & \cdots \\ \vdots & \ddots \\ \left(\frac{dt}{du}\right)^{m_n}D_t^{(m_n)}f_0 + \sum_{s=1}^{m_n} D_t^{(s)}hD_t^{(m_n-s)}f_0 & \cdots \end{pmatrix} \\ &= \left(\left(\tfrac{dt}{du}\right)^{m_0}+\epsilon\right)\left(\tfrac{dt}{du}\right)^{\sum_{i=1}^n m_i}\det\begin{pmatrix} D_t^{(m_0)}f_0 & \cdots & D_t^{(m_0)}f_n \\ D_t^{(m_1)}f_0 & \cdots & D_t^{(m_1)}f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_n)}f_0 & \cdots & D_t^{(m_n)}f_n \end{pmatrix}\end{aligned}$$

y si $m_0 = 0$ entonces

$$\det\left(D_u^{(m_i)}f_j\right) = \left(\frac{dt}{du}\right)^{\sum_{i=0}^n m_i}\det\left(D_t^{(m_i)}f_j\right).$$

⊡

En el caso en que $m_0 = 0$, la proposición nos asegura que la condición $\det\left(D_t^{(m_i)}f_j\right) \neq 0$ (los vectores filas $D_t^{(m_0)}f, \ldots, D_t^{(m_n)}f$ son linealmente independientes) no depende de la representación proyectiva del morfismo f. De manera que la condición de estudio de los wronskianos generalizados depende unicamente del sistema lineal $\mathfrak{D}$.

Teorema 1.4.3. *Sea C una curva y $f = (f_0 : \cdots : f_n) : C \to \mathbb{P}^n(k)$ un morfismo correspondiente a un sistema lineal $\mathfrak{D}$. Existen $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$ escogidos en el* orden lexicográfico *tales que*

$$\det\left(D_t^{(\varepsilon_i)} f_j\right) \neq 0.$$

Es decir, $\varepsilon_0 = 0$ y si $\varepsilon_0, \ldots, \varepsilon_{i-1}$ son conocidos entonces ε_i es el entero más pequeo tal que los vectores $D_t^{(\varepsilon_0)} f, \ldots, D_t^{(\varepsilon_i)} f$ son linealmente independientes sobre $k(C)$.

Prueba.

Obsérvese que es suficiente mostrar que existen $m_0 = 0 < m_1 < \cdots < m_n$ tales que $\det\left(D_t^{(m_i)} f_j\right) \neq 0$. Por el Teorema 1.3.6 y la Proposición 1.4.2 podemos considerar los invariantes hermitianos $j_0, \ldots, j_n$ y $\det\left(D_t^{(j_i)} f_j(P)\right) = \det\left(D_t^{(j_i)} f_j\right)(P) \neq 0$. Así,

$$\det\left(D_t^{(j_i)} f_j\right) \neq 0.$$

$\boxdot$.

Definición 1.4.4 (Ordenes de los sistemas lineales)**.** *Sea C una curva y $\mathfrak{D}$ un sistema lineal s.p.b. A los enteros $\varepsilon_0, \ldots, \varepsilon_n$ del Teorema 1.4.3 se les llama $\mathfrak{D}$-ordenes u ordenes (invariantes) del morfismo $\mathfrak{D}$.*

Sobra decir que los enteros $\varepsilon_0, \ldots, \varepsilon_n$ dependen unicamente del sistema lineal $\mathfrak{D}$ en concordancia con sus nombres.

Observación 1.4.5. *Si $j_0, \ldots, j_n$ son $(\mathfrak{D}, P)$-ordenes entonces $\varepsilon_i \leq j_i$ para todo i. Además los ε_i son mínimos en un sentido aún más general:*

Si $m_0, m_1, \ldots, m_r$ son enteros no negativos tales que $m_0 < m_1 < \cdots < m_r$ y $D_t^{(m_0)} f, \ldots, D_t^{(m_r)} f$ son vectores linealmente independientes sobre $k(C)$ entonces $\varepsilon_i \leq m_i$ para $i = 0, 1, \ldots, r$.

La observación anterior es una analogía de la Proposición 1.3.8.

Ejemplo 1.4.6. Sean C la curva sobre $k = \overline{\mathbb{F}_4}$ definida por la extensión de *Kummer* $y^3 = x^4 + x + 1$ y f el morfismo definido por $f = (1 : x : y^2)$.
Denotemos por $g_{(m)}$ a $D_x^{(m)} g$. Entonces,

$$(y^3)_{(1)} = 3y^2 y_{(1)} = \binom{4}{1} x^3 + 1 = 1.$$

Así,

$$y_{(1)} = \frac{1}{y^2} \qquad \text{y} \qquad (y^2)_{(1)} = 0.$$

Luego, usando las propiedades de la derivada de Hasse vistas en la Observación 1.4.1 tenemos:

$$(y^2)_{(2)} = y_{(2)} y + y_{(1)} y_{(1)} + y y_{(2)} = \frac{1}{y^4}.$$

De manera que

$$D_x^{(1)}f = (0,1,0) \quad \text{y} \quad D_x^{(2)}f = (0,0,\frac{1}{y^4}).$$

Por lo tanto $\varepsilon_i = i$.

Ahora si cambiamos el morfismo f por $g = (1, x^4, y)$ entonces cambian los órdenes. Por la Observación 1.4.1 $(y^p)_{(n)} = 0$ si $n \not\equiv 0 \pmod{p}$ donde p es la característica de $k(C)$. Así,

$$(y^3)_{(2)} = y_{(2)}y^2 + y(y^2)_{(2)} = 0 \quad \text{y} \quad y_{(2)} = \frac{1}{y^5}.$$

Analogamente,

$$y_{(3)} = \frac{1}{y^8} \quad \text{y} \quad y_{(4)} = \frac{1}{y^2}.$$

Luego,

$$D_x^{(1)}g = (0,0,\tfrac{1}{y^2}), \quad D_x^{(2)}g = (0,0,\tfrac{1}{y^5}),$$
$$D_x^{(3)}g = (0,0,\tfrac{1}{y^8}), \quad D_x^{(4)}g = \left(0,1,\tfrac{1}{y^2}\right)$$

y $\varepsilon_0 = 0$, $\varepsilon_1 = 1$ y $\varepsilon_2 = 4$.

Ejemplo 1.4.7. Sea C la curva hermitiana $y^3 + y = x^4$, $k = \overline{\mathbb{F}_9}$ y $f = (1 : x : y)$. Luego, $y' = y_{(1)} = x^3$ y $y_{(2)} = 0$. En consecuencia

$$(y^2)_{(2)} = (y')^2, \ (y^2)_{(3)} = 2yy_{(3)} \text{ y } y_{(3)} = x - x^9.$$

Así, $D_x^{(1)}f = (0,1,x^3)$, $D_x^{(2)}f = (0,0,0)$ y $D_x^{(3)}f = (0,0,x-x^9)$. Por lo tanto $\varepsilon_0 = 0$, $\varepsilon_1 = 1$ y $\varepsilon_2 = 3$. Obsérvese que el punto $P = (1:0:0) \in C$ y entonces C tiene 28 puntos racionales. Además, $j_0 = 0$ y $j_1 = 1$ son P-invariantes hermitianos. Sin embargo $\varepsilon_2 = 3$ no lo es. Pero, $D_x^{(4)}f = (0:0:1)$ y por lo tanto $j_2 = 4$. Este mismo fenómeno sucede con los otros 27 puntos racionales de C. En el Ejemplo 1.4.6, no sucede como en este caso.

1.5. El divisor de ramificación y puntos de Weierstrass

Para saber de que manera varían los invariantes hermitianos de un sistema lineal $\mathfrak{D}$ s.p.b., de una curva C respecto a un punto P, es necesario hacer un estudio del divisor de ramificación. Este nos permite concluir que los $(\mathfrak{D}, P)$-ordenes son los ordenes del morfismo inducido para casi todo P. Esto nos dice que existen un número finito de puntos donde el comportamiento geométrico de la curva es distinto. Estos son los famosos puntos de Weierstrass. Desde luego contarlos y localizarlos es un tema de interés.

Definición 1.5.1 (Divisor de ramificación.)**.** *Sea C una curva, $\mathfrak{D}$ un sistema lineal s.p.b. y $\varepsilon_0, \ldots, \varepsilon_n$ los $\mathfrak{D}$-ordenes. Al divisor*

$$R(\mathfrak{D}, f, t) = div\Big(\det\big(D_t^{(\varepsilon_i)} f_j\big)\Big) + \Big(\sum_{i=0}^{n} \varepsilon_i\Big) div(dt) + (n+1)E$$

se le llama divisor de ramificación *de $\mathfrak{D}$.*

En la definición anterior f es el morfismo inducido por $\mathfrak{D}$, $t \in k(C)$ es un parámetro separante de $k(C)/k$ y E es el divisor correspondiente a f de la ecuación (2).

Se denota al divisor de ramificación por R, cuando se conocen sus objetos definidores. Sin embargo:

Observación 1.5.2. *El divisor de ramificación R depende unicamente del sistema lineal.*

1) *El divisor R no depende de la representación del morfismo inducido.*

Sea $f = (f_0 : \ldots : f_n) : C \to \mathbb{P}^n(k)$ y $hf = (hf_0 : \ldots : hf_n)$ donde $h \in k(C)^*$. Sean E y E' los divisores asociados a los morfismos f y hf $\big($Véase la ecuación (2)$\big)$. Luego, por la Proposición 1.2.3, pág. 19,

$$\begin{aligned}
R(\mathfrak{D}, hf, t) &= \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)}(hf_j)\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)E' \\
&= \operatorname{div}\Big(h^{n+1}\det\big(D_t^{(\varepsilon_i)} f_j\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)\big(E - \operatorname{div}(h)\big) \\
&= (n+1)\operatorname{div}(h) + \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)} f_j\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) \\
&\quad +(n+1)\big(E - \operatorname{div}(h)\big) \\
&= \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)} f_j\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)E \\
&= R(\mathfrak{D}, f, t)
\end{aligned}$$

2) *El divisor de ramificación no depende del morfismo inducido.*

Si f y g son dos morfismos inducidos por el sistema lineal $\mathfrak{D}$, entonces $g = T \circ f$ donde $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ es un isomorfismo (vease las Proposiciones 1.2.3, 1.2.5 y sus comentarios). Luego, $g_i = \sum_{j=0}^n a_{ij} f_j$ donde $(a_{ij}) \in GL_{n+1}(k)$. Así que

$$\begin{aligned}
R(\mathfrak{D}, g, t) &= \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)} g\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)E \\
&= \operatorname{div}\Big(\det\big(a_{ij}\big)\det\big(D_t^{(\varepsilon_i)} f_j\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)E \\
&= \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)} f\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)E
\end{aligned}$$

3) *El divisor R no depende del parámetro separante.*

Sea u un parámetro separante de $k(C)/k$. Entonces por la Proposición 1.4.2

$$\begin{aligned} R(\mathfrak{D},f,u) &= \operatorname{div}\Big(\det\big(D_u^{(\varepsilon_i)}f\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(du) + (n+1)E \\ &= \operatorname{div}\left(\left(\tfrac{dt}{du}\right)^{\sum_{i=0}^n \varepsilon_i}\det\big(D_t^{(\varepsilon_i)}f_j\big)\right) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(du) + (n+1)E \\ &= \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)}f_j\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}\left(\tfrac{dt}{du}\right) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(du) \\ &\quad +(n+1)E \\ &= \operatorname{div}\Big(\det\big(D_t^{(\varepsilon_i)}f_j\big)\Big) + \big(\textstyle\sum_{i=0}^n \varepsilon_i\big)\operatorname{div}(dt) + (n+1)E \\ &= R(\mathfrak{D},f,t) \end{aligned}$$

⊡

La observación nos permite concluir que dada una curva C podemos referirnos funcionalmente al divisor de ramificación de $\mathfrak{D}$ por $R(\mathfrak{D})$.

Observación 1.5.3. *Si $A, B \in M_n(F)$ (F un cuerpo y $M_n(F)$ es el conjunto de matrices $n\times n$) entonces* $\det(A+tB) = \det(A)+tb(t)$ *donde b es un polinomio de $F[t]$ que depende de A y B.*

La observación puede verificarse facilmente por inducción matemática.

Proposición 1.5.4. *Sean $j_0,\dots,j_n$ los $(\mathfrak{D},P)$-ordenes de $P\in X$ y t un parámetro separante de $k(C)/k$. Si $m_0,\dots,m_n$ son enteros no negativos entonces*

$$\det\big(D_t^{(m_i)}f_j\big) = ct^{\sum_{i=0}^n j_i-m_i}\left[\det\left(\binom{j_r}{m_i}\right)+tb\right],$$

donde $c\in k^*$, $b\in k(C)$ y $\nu_P(b)\geq 0$. Además, si $m_0<m_1<\cdots<m_n$ y

$$\det\left(\binom{j_r}{m_i}\right) = \det\begin{pmatrix}\binom{j_0}{m_0} & \cdots & \binom{j_n}{m_0}\\ \vdots & \ddots & \vdots\\ \binom{j_0}{m_n} & \cdots & \binom{j_n}{m_n}\end{pmatrix} \not\equiv 0 \ (mod\ p)$$

donde p es la característica de $k(C)$, entonces $\varepsilon_i\leq m_i$ donde $\varepsilon_0,\dots,\varepsilon_n$ son los $\mathfrak{D}$-ordenes.

Prueba.

Podemos asumir que $f_r = c_r t^{j_r}+h_r$ con $c_r\in k^*$ por un argumento igual al de la demostración del teorema 1.3.6 (Ver también la Observación 1.3.7 y el Lema 1.3.1). En adición $\nu_P(h_r)>j_r$. Luego $D_t^{(m_i)}f_r = \binom{j_r}{m_i}c_r t^{j_r-m_i}+D_t^{(m_i)}h_r$ donde $\nu_P(D_t^{(m_i)}h_r)>\nu_P(t^{j_r-m_i}) = j_r-m_i$ y $\nu_P(t^{m_i-j_r-1}D_t^{(m_i)}h_r)\geq 0$. Así, usando las propiedades del determinante y la

Observación 1.5.3

$$\det\left(D_t^{(m_i)}f_j\right) =$$
$$\det\begin{pmatrix} \binom{j_0}{m_0}c_0t^{j_0-m_0}+D_t^{(m_0)}h_0 & \cdots & \binom{j_n}{m_0}c_nt^{j_n-m_0}+D_t^{(m_0)}h_n \\ \cdots & \ddots & \cdots \\ \binom{j_0}{m_n}c_0t^{j_0-m_n}+D_t^{(m_n)}h_0 & \cdots & \binom{j_n}{m_n}c_nt^{j_n-m_n}+D_t^{(m_n)}h_n \end{pmatrix}$$
$$= \prod_{i=0}^n c_i t^{-\sum_{i=0}^n m_i}\det\begin{pmatrix} \binom{j_0}{m_0}t^{j_0}+c_0^{-1}t^{m_0}D_t^{(m_0)}h_0 & \cdots & \binom{j_n}{m_0}t^{j_n}+c_n^{-1}t^{m_0}D_t^{(m_0)}h_n \\ \cdots & \ddots & \cdots \\ \binom{j_0}{m_n}t^{j_0}+c_0^{-1}t^{m_n}D_t^{(m_n)}h_0 & \cdots & \binom{j_n}{m_n}t^{j_n}+c_n^{-1}t^{m_n}D_t^{(m_n)}h_n \end{pmatrix}$$
$$= \prod_{i=0}^n c_i t^{\sum_{i=0}^n j_i-\sum_{i=0}^n m_i}\det\begin{pmatrix} \binom{j_0}{m_0}+c_0^{-1}t^{m_0-j_0}D_t^{(m_0)}h_0 & \cdots & \binom{j_n}{m_0}+c_n^{-1}t^{m_0-j_n}D_t^{(m_0)}h_n \\ \cdots & \ddots & \cdots \\ \binom{j_0}{m_n}+c_0^{-1}t^{m_n-j_0}D_t^{(m_n)}h_0 & \cdots & \binom{j_n}{m_n}+c_n^{-1}t^{m_n-j_n}D_t^{(m_n)}h_n \end{pmatrix}$$

y

$$\begin{aligned}\det\left(D_t^{(m_i)}f_j\right) &= \textstyle\prod_{i=0}^n c_i t^{\sum_{i=0}^n j_i-m_i}\det\left(\begin{bmatrix} \binom{j_0}{m_0} & \cdots & \binom{j_n}{m_0} \\ \cdots & \ddots & \cdots \\ \binom{j_0}{m_n} & \cdots & \binom{j_n}{m_n}\end{bmatrix}+t\begin{bmatrix} c_0^{-1}t^{m_0-j_0-1}D_t^{(m_0)}h_0 & \cdots \\ \cdots & \ddots \\ c_0^{-1}t^{m_n-j_0-1}D_t^{(m_n)}h_0 & \cdots\end{bmatrix}\right) \\ &= ct^{\sum_{i=0}^n j_i-m_i}\Big(\det\left(\tbinom{j_r}{m_i}\right)+tb\Big).\end{aligned}$$

donde $c=\prod_{i=0}^n c_i\in k^*$, $b\in k(C)$ y $\nu_P(b)\geq 0$.

Ahora, si $\det\left(\binom{j_r}{m_i}\right)\not\equiv 0 \pmod p$, entonces $\det\left(D_t^{(m_i)}f_j\right)\neq 0$ y por la Observación 1.4.5 se tiene que $\varepsilon_i\leq m_i$. ⊡

Observación 1.5.5. *La mejor escogencia en el orden lexicográfico de los m_i en la Proposición 1.5.4 son los ordenes del morfismo $g:\mathbb{P}^1(k)\to\mathbb{P}^n(k)$ donde $g(1:x)=(x^{j_0}:\cdots:x^{j_n})$.*

Claramente $D_x^{(m)}g=\left(\binom{j_0}{m}x^{j_0-m},\ldots,\binom{j_n}{m}x^{j_n-m}\right)$ y, puesto que

$$\begin{aligned}\det\left(D_x^{(m_i)}x^{j_r}\right) &= \det\begin{pmatrix} \binom{j_0}{m_0}x^{j_0-m_0} & \cdots & \binom{j_n}{m_0}x^{j_n-m_0} \\ \cdots & \ddots & \cdots \\ \binom{j_0}{m_n}x^{j_0-m_n} & \cdots & \binom{j_n}{m_n}x^{j_0-m_n}\end{pmatrix} \\ &= \det\left(\tbinom{j_r}{m_i}\right)x^{\sum_{i=0}^n j_i-m_i}\neq 0,\end{aligned}$$

si y solo si, $\det\left(\binom{j_r}{m_i}\right)\not\equiv 0\ (mod\ p)$, si y solo si, dados $m_0,\ldots,m_{i-1}$ y $\left(\binom{j_0}{m_0},\ldots,\binom{j_n}{m_0}\right),\ldots,\left(\binom{j_0}{m_{i-1}},\ldots,\binom{j_n}{m_{i-1}}\right)$ son linealmente independientes sobre $\mathbb{F}_p$, entonces m_i es el entero positivo mas pequeño (mínimo) tal que $\left(\binom{j_0}{m_0},\ldots,\binom{j_n}{m_0}\right),\ldots,\left(\binom{j_0}{m_{i-1}},\ldots,\binom{j_n}{m_{i-1}}\right),\left(\binom{j_0}{m_i},\ldots,\binom{j_n}{m_i}\right)$ son linealmente independientes sobre $\mathbb{F}_p$ (Mírese la Observación 1.4.5. Además, recuerde que $K\big(\mathbb{P}^1(k)\big)\cong k(x)$)

Teorema 1.5.6. *Sean R el divisor de ramificación de $\mathfrak{D}$, P un punto de la curva C y $j_0,\ldots,j_n$ sus correspondientes $(\mathfrak{D},P)$-ordenes. Entonces $\nu_P(R)\geq\sum_{i=0}^n(j_i-\varepsilon_i)$; donde la*

igualdad se tiene si y solo si,

$$\det\left(\binom{j_r}{\varepsilon_i}\right) \ncong 0 \ (mod\ p)$$

donde p es la característica de $k(C)$.

Prueba.

Por la Observación 1.5.2, podemos suponer que t es un parámetro P-uniformizante. Además, podemos asumir que $e_P = \nu_P(E) = \nu_P\big(\mathrm{div}(dt)\big) = \nu_P(1) = 0$ (hemos usado la Observación 1.3.7). Luego, por la Proposición 1.5.4

$$\det\left(D_t^{(\varepsilon_i)} f_j\right) = ct^{\sum_{i=0}^n j_i - \varepsilon_i}\left(\det\left(\binom{j_r}{\varepsilon_i}\right) + tb\right)$$

Por lo tanto $\nu_P(R) \geq \sum_{i=0}^n j_i - \varepsilon_i \geq 0$. Ahora, $\nu_P(R) = \sum_{i=0}^n j_i - \varepsilon_i \iff \det\left(\binom{j_r}{\varepsilon_i}\right) \neq 0$ en $k \iff \det\left(\binom{j_r}{\varepsilon_i}\right) \ncong 0 \ (mod\ p)$. ⊡

El teorema nos dice que $R(\mathfrak{D})$ es un divisor positivo. Más aún, $\nu_P(R) = 0$ si y solo si, $j_i = \varepsilon_i$ para todo i. De manera que los $\mathfrak{D}$-ordenes $\varepsilon_0, \ldots, \varepsilon_n$ son los invariantes hermitianos para casi todo P, por que el soporte del divisor de ramificación R, $Sopp(R) = \{P \in X : \nu_P(R) \neq 0\}$ es un conjunto finito. Es decir, hay un conjunto finito de puntos para los cuales los invariantes hermitianos no son los $\mathfrak{D}$-ordenes.

Definición 1.5.7 (Punto de Weierstrass)**.** *Sean C una curva, $\mathfrak{D}$ un sistema lineal s.p.b., P un punto de C y $\varepsilon_0, \ldots, \varepsilon_n$ los $\mathfrak{D}$-ordenes. Decimos que P es $\mathfrak{D}$-ordinario si $j_i = \varepsilon_i$ para todo $i \in \{0, 1, \ldots, n\}$. De lo contrario a P se le llama punto de Weierstrass de $\mathfrak{D}$. A la valuación $\nu_P(R)$ se le llama* peso *de P en $\mathfrak{D}$.*

El número de puntos de Weierstrass de $\mathfrak{D}$ contando sus pesos es

$$gr(R) = \sum_{i=0}^{n} \varepsilon_i(2g-2) + (n+1)d,$$

donde d es el grado de $\mathfrak{D}$.

Cuando el sistema lineal $\mathfrak{D}$ es canónico entonces la definición anterior de punto de Weierstrass coincide con la clásica.

Definición 1.5.8 (Sistemas lineales no clásicos)**.** *Sea $(\varepsilon_0, \ldots, \varepsilon_n)$ la sucesión de $\mathfrak{D}$-ordenes. Decimos que $\mathfrak{D}$ es clásico si $(\varepsilon_0, \ldots, \varepsilon_n) = (0, 1, \ldots, n)$. De lo contrario se dice que $\mathfrak{D}$ es no clásico.*

Bajo la hipótesis de clasicismo de $\mathfrak{D}$ los puntos de Weierstrass son los mismos puntos de $\mathfrak{D}$-osculación. De otro lado si $\mathfrak{D}$ es no clásico, entonces todos los puntos de C son de osculación pues $j_n \geq \varepsilon_n > n$.

La existencia de sistemas lineales no clásicos es realmente rara debido a las condiciones geométricas que la curva debe satisfacer. Esto nos dice que es importante estudiar las condiciones para que un sistema lineal sea clásico. Teniendo en mente este fin, es importante la siguiente observación:

Observación 1.5.9. *Si $j_r > i$ ($j_r, i \in \mathbb{Z}_0^+$) entonces*

$$\binom{j_r}{i} = \frac{j_r^i}{i!} + \sum_{s=0}^{i-1} a_{is} \frac{j_r^i}{s!}$$

donde $a_{is} \in \mathbb{Q}$

La afirmación anterior se obtiene expandiendo polinomialmente (respecto a j_r) a $\binom{j_r}{i}$.

Corolario 1.5.10. *Si $j_0, \ldots, j_n$ son $(\mathfrak{D}, P)$-ordenes entonces*

$$\det\left(\binom{j_r}{i}\right) = \prod_{i>s}^{n} \frac{j_i - j_s}{i - s}.$$

Además, si p no divide a $\det\left(\binom{j_r}{i}\right)$ entonces $\mathfrak{D}$ es clásico y el peso de P es $\sum_{i=0}^{n}(j_i - i)$.

Prueba.

Por la Observación 1.5.9

$$\begin{aligned}
\det\left(\binom{j_r}{i}\right) &= \det\begin{pmatrix} \binom{j_0}{0} & \cdots & \binom{j_n}{0} \\ \binom{j_0}{1} & \cdots & \binom{j_n}{1} \\ \vdots & \ddots & \vdots \\ \binom{j_0}{n} & \cdots & \binom{j_n}{n} \end{pmatrix} \\
&= \det\begin{pmatrix} \frac{j_0^0}{0!} & \cdots & \frac{j_n^0}{0!} \\ \frac{j_0^1}{1!} + a_{10}\frac{j_0^0}{0!} & \cdots & \frac{j_n^1}{1!} + a_{10}\frac{j_n^0}{0!} \\ \vdots & \ddots & \vdots \\ \frac{j_0^n}{n!} + \sum_{s=0}^{n-1} a_{ns}\frac{j_0^s}{s!} & \cdots & \frac{j_n^n}{n!} + \sum_{s=0}^{n-1} a_{ns}\frac{j_n^s}{s!} \end{pmatrix}.
\end{aligned}$$

Luego,

$$\det\left(\binom{j_r}{i}\right) = \det\begin{pmatrix} \frac{j_0^0}{0!} & \cdots & \frac{j_n^0}{0!} \\ \frac{j_0^1}{1!} & \cdots & \frac{j_n^1}{1!} \\ \vdots & \ddots & \vdots \\ \frac{j_0^n}{n!} & \cdots & \frac{j_n^n}{n!} \end{pmatrix} = \prod_{r=0}^{n} \frac{1}{r!} \det\begin{pmatrix} j_0^0 & \cdots & j_n^0 \\ j_0^1 & \cdots & j_n^1 \\ \vdots & \ddots & \vdots \\ j_0^n & \cdots & j_n^n \end{pmatrix}.$$

Así que

$$\det\left(\binom{j_r}{i}\right) = \prod_{i>s\geq 0}^{n} (j_i - j_s) \prod_{r=0}^{n} \frac{1}{r!} = \prod_{i>s}^{n} \frac{j_i - j_s}{i - s}.$$

Obsérvese que se ha usado el determinante de Vandermonde y un argumento similar al de la Proposición 1.4.2. De otro lado si $p = \chi(k)$ no divide a $\det\left(\binom{j_r}{i}\right)$ entonces $\varepsilon_i = i$ por la Proposición 1.5.4 y, $\nu_P(R) = \sum_{i=0}^{n}(j_i - i)$. ⊡

El criterio del corolario se satisface si $j_i - j_r$ $(i > r)$ no es divisible por p. En particular, como $j_n \leq d = gr(\mathfrak{D})$ entonces se tiene el siguiente resultado:

Corolario 1.5.11. *Si $p > d$ ó $p = 0$ entonces $\mathfrak{D}$ es clásico y*

$$\nu_P(R) = \sum_{i=0}^{n}(j_i - i).$$

Obsérvese que si d es par entonces la hipótesis del corolario se puede cambiar por $p+1 > d$. Es decir, para que un sistema lineal de grado impar sea no clásico se requiere que $p+1 \leq d$. En el caso $p = 2$ el resultado se tiene salvo en el caso extremo $n = 1$ y $d = 2$, porque $n \leq d$ donde n es la dimensión del sistema lineal y d es el grado. Este resultado generaliza el teorema de F. K. Schmidt citado en Komiya [8], Teo. C.

Corolario 1.5.12. *Sea ε_r un $\mathfrak{D}$-orden y ε un entero tal que $\binom{\varepsilon_r}{\varepsilon} \not\equiv 0 \ (mod\ p)$. Entonces ε es también un $\mathfrak{D}$-orden. En particular si $\varepsilon_r < p$ entonces, $0, 1, \ldots, \varepsilon_r - 1$ son $\mathfrak{D}$-ordenes.*

Prueba.

Debemos suponer que $\varepsilon < \varepsilon_r$, pues de lo contrario $\binom{\varepsilon_r}{\varepsilon} = 0$ ó $\varepsilon = \varepsilon_r$. Sea i el mayor entero tal que $\varepsilon_{i-1} < \varepsilon$. Es decir, $\varepsilon \leq \varepsilon_i$. Luego por la Proposición 1.5.4 (podemos suponer que el punto P de la proposición es $\mathfrak{D}$-ordinario) y la Observación 1.5.5, definiendo

$$m = \operatorname{ran}\begin{pmatrix} \binom{\varepsilon_0}{\varepsilon_0} & \binom{\varepsilon_1}{\varepsilon_0} & \cdots & \binom{\varepsilon_{i-1}}{\varepsilon_0} & \cdots & \binom{\varepsilon_r}{\varepsilon_0} & \cdots & \binom{\varepsilon_n}{\varepsilon_0} \\ \binom{\varepsilon_0}{\varepsilon_1} & \binom{\varepsilon_1}{\varepsilon_1} & \cdots & \binom{\varepsilon_{i-1}}{\varepsilon_1} & \cdots & \binom{\varepsilon_r}{\varepsilon_1} & \cdots & \binom{\varepsilon_n}{\varepsilon_1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \binom{\varepsilon_0}{\varepsilon_{i-1}} & \binom{\varepsilon_1}{\varepsilon_{i-1}} & \cdots & \binom{\varepsilon_{i-1}}{\varepsilon_{i-1}} & \cdots & \binom{\varepsilon_r}{\varepsilon_{i-1}} & \cdots & \binom{\varepsilon_n}{\varepsilon_{i-1}} \\ \binom{\varepsilon_0}{\varepsilon} & \binom{\varepsilon_1}{\varepsilon} & \cdots & \binom{\varepsilon_{i-1}}{\varepsilon} & \cdots & \binom{\varepsilon_r}{\varepsilon} & \cdots & \binom{\varepsilon_n}{\varepsilon_1} \end{pmatrix}$$

tenemos que

$$\begin{aligned} m &= \operatorname{ran}\begin{pmatrix} 1 & \binom{\varepsilon_1}{\varepsilon_0} & \cdots & \binom{\varepsilon_{i-1}}{\varepsilon_0} & \cdots & \binom{\varepsilon_r}{\varepsilon_0} & \cdots & \binom{\varepsilon_n}{\varepsilon_0} \\ 0 & 1 & \cdots & \binom{\varepsilon_{i-1}}{\varepsilon_1} & \cdots & \binom{\varepsilon_r}{\varepsilon_1} & \cdots & \binom{\varepsilon_n}{\varepsilon_1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & \binom{\varepsilon_r}{\varepsilon_{i-1}} & \cdots & \binom{\varepsilon_n}{\varepsilon_{i-1}} \\ 0 & 0 & \cdots & 0 & \cdots & \binom{\varepsilon_r}{\varepsilon} & \cdots & \binom{\varepsilon_n}{\varepsilon} \end{pmatrix} \\ &= i + 1. \end{aligned}$$

Por lo tanto $\varepsilon_i \leq \varepsilon$ y $\varepsilon = \varepsilon_i$. ⊡

Observación 1.5.13. *La condición* $\binom{\varepsilon_r}{\varepsilon} \not\equiv 0 \ (mod\ p)$ *se tiene si y solo si,* ε_r *es p-adicamente menor que* ε*; es decir, si y solo si, cada coeficiente en la expansión p-ádica de* ε *es más pequeño que el correspondiente de* ε_r*.*

Pueden verse las justificaciones de la observación y algunos casos particulares de los resultados obtenidos aquí en Komiya [8], Sec. 1, Teo. A, Lema B y en sus citadas referencias.

El Corolario 1.5.11 no se puede mejorar en el caso en que d es impar como lo muestra la linea proyectiva $\mathbb{P}^1(k)$ y el morfismo $f = (1 : x : x^p)$ donde p es la característica de k.

2. EL METODO STÖHR–VOLOCH

El método usado para obtener la cota para el número de puntos $\mathbb{F}_q$-racionales de una curva C inducida por un polinomio $f(X,Y) \in \overline{\mathbb{F}_q}[X,Y]$ del Capítulo 1 se fundamentó en la construcción de una curva (función) auxiliar $h(f,q,P)$ donde $P \in C$. Esta satisface las siguientes propiedades:

1. Si P es $\mathbb{F}_q$-racional de C entonces $h(f,q,P) = 0$ (h se anula en los puntos racionales de C).
2. El número de puntos $P \in C$ tales que $h(f,q,P) = 0$, que no son $\mathbb{F}_q$-racionales están controlados (son pocos).

Por supuesto se requiere que la función h sea no nula y esto implica imponer condiciones a f o C. Obsérvese que esto se hace en el teorema 1.1.1 y además, $h : C \to \overline{\mathbb{F}_q}$ cuenta el número de puntos de $(x_0, y_0) = P \in C$ tales que $P^q = (x_0^q, y_0^q)$ está en la recta tangente a C en P.

El proposito de este capítulo es generalizar el método presentado en la sección 1.1 utilizando el hiperplano osculador en vez de la recta tangente. Luego, con ayuda de los ordenes y divisor $\mathbb{F}_q$-Frobenius en lugar del teorema de Bezout, se obtiene el teorema y método de K–O Stöhr y F. Voloch.

2.1. Divisor de Frobenius y puntos racionales

Sea $\mathbb{F}_q$ el cuerpo de Galois con q elementos de característica p y $k = \overline{\mathbb{F}_q}$ su clausura algebraica. Sea C una curva algebraica irreducible, no singular definida sobre k de género g y F_q el morfismo $\mathbb{F}_q$-Frobenius en C. Un punto $P \in C$ es $\mathbb{F}_q$-racional si y sólo si, P es un punto fijo de la aplicación de Frobenius ($F_q(P) = P$).

Dado un subcuerpo $L \subseteq k$, la curva $C(L)$ es la curva C, pero definida sobre L.

Sea $f : C \to \mathbb{P}^n(k)$ un $\mathbb{F}_q$-morfismo. Es decir, $f = (f_0, \ldots, f_n)$ donde $f_i \in \mathbb{F}_q(C) \subset k(C)$ (la función f_i es $\mathbb{F}_q$-racional).

Supongamos además que $f(C)$ no está contenido en ningún hiperplano H de $\mathbb{P}^n(k)$. Luego, el morfismo f induce un sistema lineal $\mathfrak{D}(f) = \mathfrak{D}$ sin puntos básicos (s.p.b) (Véase la Proposición 1.2.5 y sus comentarios precedentes); es decir, para cada $P \in C$ existe $D \in \mathfrak{D}$ tal que P no pertenece al soporte de D ($P \notin Sopp(D)$ o $P \not\leq D$). De otro lado, definimos el divisor $E = \sum_{P \in C(\mathbb{F}_q)} e_P \in \mathcal{D}_C$, donde $e_P = -\min\{\nu_P(f_0), \ldots, \nu_P(f_n)\}$ (Véase el Capítulo 1, ecuación (2), pág. 19). Obsérvese que E y $\mathfrak{D}$ quedan definidos sobre $\mathbb{F}_q$.

Sea N_q el número de puntos $\mathbb{F}_q$-racionales. Cuando se sobreentienda el q entonces denotaremos por N al número de puntos racionales. Dado un entero a, denotaremos al vector $(f_0^a, \ldots, f_n^a) \in k(C)^{n+1}$ $\Big(\big(f_0^a(P), \ldots, f_n^a(P)\big) \in k^{n+1}\Big)$ por f^a $\big(f^a(P)$, donde $P \in C\big)$. Analogamente, si $h \in k(C)$ entonces $hf = (hf_0 : \cdots : hf_n)$. Para obtener una cota para N, contamos el número máximo de puntos de $P \in C$ tales que $f(P)^q := \big(f_0^q(P) : \ldots : f_n^q(P)\big)$ esté en el plano osculador en P (Véase la Sección 1.3, pág. 25). Es decir, contamos los puntos P de C tales que $f(P)$ bajo la aplicación de Frobenius de $\mathbb{P}^n(k)$, esté en el plano osculador $L_{n-1}(P)$. De manera que si $e_P = 0$ (Véase la Observación 1.3.7) y $j_0, \ldots, j_n$ son los $(\mathfrak{D}, P)$-ordenes, entonces $f(P)^q$ está en el plano osculador, si y sólo si,

$$\det \begin{pmatrix} f^q(P) \\ D_t^{(j_0)} f \\ \vdots \\ D_t^{(j_{n-1})} f \end{pmatrix} = \det \begin{pmatrix} f_0^q(P) & f_1^q(P) & \cdots & f_n^q(P) \\ D_t^{(j_0)} f_0(P) & D_t^{(j_0)} f_1(P) & \cdots & D_t^{(j_0)} f_n(P) \\ \vdots & \vdots & \ddots & \vdots \\ D_t^{(j_{n-1})} f_0(P) & D_t^{(j_{n-1})} f_1(P) & \cdots & D_t^{(j_{n-1})} f_n(P) \end{pmatrix} = 0,$$

donde t es un parametro P-uniformizante. Lo anterior motiva el estudio del wronskiano

$$W_t^{(m_0,\ldots,m_{n-1})}(f) := \det \begin{pmatrix} f^q \\ D_t^{(m_0)} f \\ \vdots \\ D_t^{(m_{n-1})} f \end{pmatrix}$$

donde $m_i \in \mathbb{Z}_0^+$ y t es un parametro separante de $\mathbb{F}_q(C)/\mathbb{F}_q$. Cuando se sobreentienda la sucesión $(m_0, \ldots, m_{n-1})$ denotaremos a $W_t^{(m_0,\ldots,m_{n-1})}$ por W_t.

Proposición 2.1.1. *Sea $f = (f_0 : \cdots : f_n) : C \to \mathbb{P}^n(k)$ el morfismo inducido por el sistema lineal s.p.b $\mathfrak{D}$ y $(m_0, \ldots, m_{n-1})$ una sucesión de enteros no negativos.*

a) Si $g_i = \sum_{j=0}^n a_{ij} f_j$ con $(a_{ij}) \in GL_{n+1}(\mathbb{F}_q)$, entonces

$$W_t(g) = \det(a_{ij}) W_t(f).$$

Además, si $m_0 < m_1 < \cdots < m_{n-1}$ y $\langle D_t^{(m_0)} f, \ldots, D_t^{(m_{i-1})} f\rangle = \langle D_t^{(0)} f, D_t^{(1)} f, \ldots, D_t^{(m_i-1)} f\rangle$ para $i = 1, 2, \ldots, n$, se tienen los siguientes resultados:

b) Si $h \in \mathbb{F}_q(C)$, entonces $W_t(hf) = (\epsilon + h) h^{q+n-1} W_t(f)$ para algún $\epsilon \in \mathbb{F}_q(C)$. También, si $m_0 = 0$ entonces $\epsilon = 0$ y

$$W_t(hf) = h^{q+n} W_t(f)$$

c) Si $u \in k(C)$ es otra variable separante de $\mathbb{F}_q(C)/\mathbb{F}_q$ entonces

$$W_u(f) = \left(\left(\frac{dt}{du}\right)^{m_0} + \epsilon\right)\left(\frac{dt}{du}\right)^{\sum_{i=1}^{n-1} m_i} W_t(f),$$

para algún $\epsilon \in k(C)$. En el caso $m_0 = 0$, entonces

$$W_u(f) = \Big(\frac{dt}{du}\Big)^{\sum_{i=0}^{n-1} m_i} W_t(f).$$

La demostración de esta proposición es análoga a la de la proposición 1.5.4.

Prueba.

a) Obsérvese, que $a_{ij} \in \mathbb{F}_q$ si y solo si, $a_{ij}^q = a_{ij}$. Luego, $g_i^q = \big(\sum_{j=0}^n a_{ij} f_j\big)^q = \sum_{j=0}^n a_{ij} f_j^q$. De otro lado, por la linealidad del operador $D_t^{(m_r)}$

$$D_t^{(m_r)} g_i = D_t^{(m_r)} \left(\sum_{j=0}^n a_{ij} f_j \right) = \sum_{j=0}^n a_{ij} D_t^{(m_r)} f_j.$$

Luego, por la multiplicación de matrices tenemos

$$\begin{aligned} W_t(g) &= \det \begin{pmatrix} \sum_{j=0}^n a_{0j} f_j^q & \cdots & \sum_{j=0}^n a_{nj} f_j^q \\ \sum_{j=0}^n a_{0j} D_t^{(m_0)} f_j & \cdots & \sum_{j=0}^n a_{nj} D_t^{(m_0)} f_j \\ \vdots & \ddots & \vdots \\ \sum_{j=0}^n a_{0j} D_t^{(m_{n-1})} f_j & \cdots & \sum_{j=0}^n a_{nj} D_t^{(m_{n-1})} f_j \end{pmatrix} \\ &= \det \begin{pmatrix} a_{00} & \cdots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{n0} & \cdots & a_{nn} \end{pmatrix} \det \begin{pmatrix} f_j^q & \cdots & f_j^q \\ D_t^{(m_0)} f_0 & \cdots & D_t^{(m_0)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_{n-1})} f_0 & \cdots & D_t^{(m_{n-1})} f_n \end{pmatrix} \\ &= \det(a_{ij}) W_t(f). \end{aligned}$$

b) Claramente $(hf)^q = h^q f^q$. De otro lado, usando la Observación 1.4.1 y la hipótesis sobre los espacios generados tenemos que $D_t^{(m_0)}(hf_j) = hD_t^{(m_0)} f_j + \sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_j$ y

$$\begin{aligned} &\Big(\textstyle\sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_0, \ldots, \sum_{s=1}^{m_0} D_t^{(s)} h D_t^{(m_0-s)} f_n\Big) \\ &= \textstyle\sum_{s=1}^{m_0} \Big(D_t^{(s)} h D_t^{(m_0-s)} f_0, \ldots, D_t^{(s)} h D_t^{(m_0-s)} f_n\Big) = \epsilon\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big), \end{aligned}$$

para algún $\epsilon \in \mathbb{F}_q(C)$. De manera que $\epsilon = 0$ si $m_0 = 0$. Así,

$$\big(D_t^{(m_0)}(hf_0), \ldots, D_t^{(m_0)}(hf_n)\big) = (\epsilon + h)\big(D_t^{(m_0)} f_0, \ldots, D_t^{(m_0)} f_n\big).$$

Luego, por la Observación 1.4.1 y la linealidad del determinante

$$\begin{aligned} W_t(hf) &= \det \begin{pmatrix} h^q f_0^q & \cdots \\ (h+\epsilon) D_t^{(m_0)} f_0 & \cdots \\ hD_t^{(m_1)} f_0 + \sum_{s=1}^{m_1} D_t^{(s)} h D_t^{(m_1-s)} f_0 & \cdots \\ \vdots & \ddots \\ hD_t^{(m_{n-1})} f_0 + \sum_{s=1}^{m_{n-1}} D_t^{(s)} h D_t^{(m_{n-1}-s)} f_0 & \cdots \end{pmatrix} \\ &= (h+\epsilon) h^{q+n-1} W_t(f). \end{aligned}$$

Además, si $m_0 = 0$ entonces $\epsilon = 0$ y

$$W_t(hf) = h^{q+n} W_t(f).$$

c) Análogamente a b) pero usando la regla de la cadena para la derivada de Hasse (Observación 1.4.1, 2) tenemos que

$$\begin{aligned} W_u(f) &= \Big(\big(\tfrac{dt}{du}\big)^{m_0} + \epsilon\Big) \det \begin{pmatrix} f_0^q & \cdots \\ D_t^{(m_0)} f_0 & \cdots \\ \big(\tfrac{dt}{du}\big)^{m_0} D_t^{(m_1)} f_0 + \sum_{s=1}^{m_1} D_t^{(s)} h D_t^{(m_1-s)} f_0 & \cdots \\ \vdots & \ddots \\ \big(\tfrac{dt}{du}\big)^{m_{n-1}} D_t^{(m_{n-1})} f_0 + \sum_{s=1}^{m_{n-1}} D_t^{(s)} h D_t^{(m_{n-1}-s)} f_0 & \cdots \end{pmatrix} \\ &= \Big(\big(\tfrac{dt}{du}\big)^{m_0} + \epsilon\Big) \big(\tfrac{dt}{du}\big)^{\sum_{i=1}^{n-1} m_i} W_t(f) \end{aligned}$$

y si $m_0 = 0$ entonces

$$W_u(f) = \Big(\frac{dt}{du}\Big)^{\sum_{i=0}^{n-1} m_i} W_t(f).$$

⊡

Lema 2.1.2. *Sea X un L-espacio vectorial y $\{V_1, \ldots, V_n\}$ una base de X. Sea $V \in X$. Si $V = \sum_{i=1}^{m} \alpha_i V_i$ para algunos $\alpha_i \in L$ y $\alpha_m \neq 0$ entonces $\{V_1, \ldots, V_{m-1}, V, V_{m+1}, \ldots, V_n\}$ es una base de X.*

Este lema no es más que una propiedad de las relaciones de dependencia.

Proposición 2.1.3. *Sean $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$ los respectivos ordenes del sistema lineal s.p.b. $\mathfrak{D}$ y f el morfismo inducido por $\mathfrak{D}$. Existen $v_0, \ldots, v_{n-1}$ enteros no negativos tales que $W_t^{(v_0,\ldots,v_{n-1})}(f) \neq 0$. Además, si la sucesión $(v_0, \ldots, v_{n-1})$ es escogida en el orden lexicográfico (es decir, $v_0 = 0$ y si $f^q, D_t^{(v_0)} f, \ldots, D_t^{(v_{i-1})} f$ son linealmente independientes entonces v_i es el entero más pequeño tal que $f^q, D_t^{(v_0)} f, \ldots, D_t^{(v_{i-1})} f, D_t^{(v_i)} f$ son linealmente independientes) entonces existe $s \in \mathbb{Z}$ tal que*

$$v_i = \begin{cases} \varepsilon_i & si\ i < s \\ \varepsilon_{i+1} & si\ i \geq s \end{cases}$$

Prueba.

Sea s el menor entero tal que $f^q = \sum_{i=0}^{s} \lambda_i D_t^{(\varepsilon_i)} f$. Claramente $s \neq 0$ porque f no es constante ($\mathfrak{D} \neq 0$ pues es s.p.b). Por la minimalidad de s entonces $\lambda_s \neq 0$. Luego, por el Lema 2.1.2 $f^q, D_t^{(\varepsilon_0)} f, \ldots, D_t^{(\varepsilon_{s-1})} f, D_t^{(\varepsilon_{s+1})} f, \ldots, D_t^{(\varepsilon_n)} f$ es un conjunto linealmente independiente. Por lo tanto,

$$v_i = \begin{cases} \varepsilon_i & \text{si } i < s \\ \varepsilon_{i+1} & \text{si } i \geq s \end{cases} \Rightarrow W_t^{(v_0,\ldots,v_{n-1})}(f) \neq 0.$$

Supongamos ahora que tenemos la sucesión de enteros $(w_0, \ldots, w_{n-1})$ escogida en el orden lexicográfico tal que $0 = w_0 < \cdots < w_{n-1}$ y $W_t^{(w_0,\ldots,w_{n-1})}(f) \neq 0$. Luego, $w_i \leq v_i$ para $i = 0, 1, \ldots, n-1$. De otro lado, como $f^q, D_t^{(w_0)}f, \ldots, D_t^{(w_{n-1})}f$ son linealmente independientes, entonces $\{D_t^{(w_0)}f, D_t^{(w_1)}f, \ldots, D_t^{(w_{n-1})}f\}$ es linealmente independiente. Así, por la minimalidad de los $\mathfrak{D}$-ordenes (Observación 1.4.5) tenemos que $\varepsilon_i \leq w_i$ para $i = 0, 1, \ldots, n-1$. Luego, $w_i = v_i = \varepsilon_i$ para $i < s$. Concluimos entonces que $f^q, D_t^{(\varepsilon_0)}f, D_t^{(\varepsilon_1)}f, \ldots, D_t^{(\varepsilon_{s-1})}f, D_t^{(w_s)}f, \ldots, D_t^{(w_{n-1})}f$ son linealmente independientes y por el Lema 2.1.2, $D_t^{(\varepsilon_0)}f, D_t^{(\varepsilon_1)}f, \ldots, D_t^{(\varepsilon_{s-1})}f, D_t^{(\varepsilon_s)}f, D_t^{(ws)}f, \ldots, D_t^{(w_{n-1})}f$ son linealmente independientes. Luego, $\varepsilon_{i+1} = v_i \leq w_i$ para $i > s$ por la minimalidad de los $\mathfrak{D}$-ordenes. Por lo tanto, $w_i = v_i$ para $i = 0, 1, \ldots, n-1$ y se tiene el resultado. ⊡

Observación 2.1.4. *Los v_i son mínimos en un sentido aún más general: Si $m_0, m_1, \ldots, m_r$ son enteros no negativos tales que $m_0 < m_1 < \cdots < m_r$ y $f^q, D_t^{(m_0)}f, \ldots, D_t^{(m_r)}f$ son vectores linealmente independientes sobre $k(C)$ entonces $v_i \leq m_i$ para $i = 0, 1, \ldots, r$.*

En efecto

$$\operatorname{ran}\begin{pmatrix} f_0^q(P) & \cdots & f_n^q(P) \\ D_t^{(0)}f_0(P) & \cdots & D_t^{(0)}f_n(P) \\ D_t^{(1)}f_0(P) & \cdots & D_t^{(1)}f_n(P) \\ \vdots & \ddots & \vdots \\ D_t^{(v_r-1)}f_0(P) & \cdots & D_t^{(v_r-1)}f_n(P) \end{pmatrix} = \operatorname{ran}\begin{pmatrix} f_0^q(P) & \cdots & f_n^q(P) \\ D_t^{(v_0)}f_0(P) & \cdots & D_t^{(v_0)}f_n(P) \\ D_t^{(v_1)}f_0(P) & \cdots & D_t^{(v_1)}f_n(P) \\ \vdots & \ddots & \vdots \\ D_t^{(v_r-1)}f_0(P) & \cdots & D_t^{(v_r-1)}f_n(P) \end{pmatrix} = r+1.$$

Luego, $v_r - 1 < m_r$ pues

$$\operatorname{ran}\begin{pmatrix} f_0^q(P) & \cdots & f_n^q(P) \\ D_t^{(m_0)}f_0(P) & \cdots & D_t^{(m_0)}f_n(P) \\ D_t^{(m_1)}f_0(P) & \cdots & D_t^{(m_1)}f_n(P) \\ \vdots & \ddots & \vdots \\ D_t^{(m_r)}f_0(P) & \cdots & D_t^{(m_r)}f_n(P) \end{pmatrix} = r+2.$$

y $v_r \leq m_r$. ⊡

Debido a los resultados anteriores es natural tener la siguiente definición:

Definición 2.1.5 (Ordenes y Divisor $\mathbb{F}_q$-Frobenius)**.** *Sea C una curva y $\mathfrak{D}$ un sistema lineal s.p.b. A los enteros $v_0, \ldots, v_{n-1}$ de la Proposición 2.1.3 se les llama ordenes $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$ o $(\mathfrak{D}, \mathbb{F}_q)$-ordenes de Frobenius. Al divisor*

$$S(\mathfrak{D}) = div\big(W_t(f)\big) + \left(\sum_{i=0}^{n-1} v_i\right) div(dt) + (q+n)E,$$

lo llamamos divisor $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$ (Aquí se entiende que t es un parametro separante de $\mathbb{F}_q(C)/\mathbb{F}_q$ y E es el divisor de la Sección 1.2, Ecuación (2), pág. 19) .

Cuando se sobreentiende el sistema lineal $\mathfrak{D}$ denotaremos al divisor $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$ por S. Claramente, $gr(S) = \big(\sum_{i=0}^{n-1} v_i\big)(2g-2) + (q+n)d$, donde $d = gr(\mathfrak{D})$.

Ejemplo 2.1.6. Sea $C = \mathbb{P}^1(k)$ donde $k = \overline{\mathbb{F}_q}$ es algebraicamente cerrado. Obsérvese que $k(C) = k(x)$ donde x es la función coordenada, la cual es trascendente sobre k. El sistema lineal $\mathfrak{D} = |nP_\infty|$ no tiene puntos básicos $\big($el punto $P_\infty = (0:1)$ y $n \in \mathbb{Z}^+\big)$. Por el Teorema de Riemann-Roch, una base de $L(nP_\infty)$ es $\{1, x, x^2, \ldots, x^n\}$. Luego, el morfismo correspondiente a $|nP_\infty|$ es $f = (1 : x : \ldots : x^n)$. Sabemos que $\varepsilon_i = j_i = i$ para todo i (Véase el ejemplo 1.2.12 y la observación 1.4.5). Así, $D_x^{(m)} g = \Big(0, \binom{1}{m}x^{1-m}, \ldots, \binom{m}{m}x^{m-m}, \binom{m+1}{m}x, \ldots, \binom{n}{m}x^{n-m}\Big) = \Big(0, 0, \ldots, 1, \binom{m+1}{m}x, \ldots, \binom{n}{m}x^{n-m}\Big)$. Véamos que la sucesión de ordenes de Frobenius es $(v_0, \ldots, v_{n-1}) = (0, \ldots, n-1)$. Obsérvese que

$$\begin{aligned} W_x(g) &= \det \begin{pmatrix} 1 & x^q & \cdots & x^{(n-1)q} & x^{nq} \\ 1 & x & \cdots & x^{n-1} & x^n \\ 0 & \binom{1}{1}x^{1-1} & \cdots & \binom{n-1}{1}x^{(n-1)-1} & \binom{n}{1}x^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \binom{1}{n-1}x^{1-(n-1)} & \cdots & \binom{n-1}{n-1}x^{(n-1)-(n-1)} & \binom{n}{n-1}x^{n-(n-1)} \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & x^q & \cdots & x^{(n-1)q} & x^{nq} \\ 0 & x - x^q & \cdots & x^{n-1} - x^{(n-1)q} & x^n - x^{nq} \\ 0 & \binom{1}{1}x^{1-1} & \cdots & \binom{n-1}{1}x^{(n-1)-1} & \binom{n}{1}x^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \binom{1}{n-1}x^{1-(n-1)} & \cdots & \binom{n-1}{n-1}x^{(n-1)-(n-1)} & \binom{n}{n-1}x^{n-(n-1)} \end{pmatrix}, \end{aligned}$$

donde la segunda igualdad se obtuvo restando la fila uno (1) a la fila dos (2). Luego, usando la Observación 1.5.3 y el Corolario 1.5.10

$$\begin{aligned} W_x(g) &= \det \begin{pmatrix} \binom{1}{0}x - x^q & \binom{2}{0}x^2 - x^{2q} & \cdots & \binom{n}{0}x^n - x^{nq} \\ \binom{1}{1}x^{1-1} + 0 & \binom{2}{1}x^{2-1} + 0 & \cdots & \binom{n}{1}x^{n-1} + 0 \\ \vdots & \vdots & \ddots & \vdots \\ \binom{1}{n-1}x^{1-(n-1)} + 0 & \binom{2}{n-1}x^{2-(n-1)} + 0 & \cdots & \binom{n}{n-1}x^{n-(n-1)} + 0 \end{pmatrix} \\ &= \det \begin{pmatrix} \binom{1}{0}x^{1-0} & \binom{2}{0}x^{2-0} & \cdots & \binom{n}{0}x^{n-0} \\ \binom{1}{1}x^{1-1} & \binom{2}{1}x^{2-1} & \cdots & \binom{n}{1}x^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{1}{n-1}x^{1-(n-1)} & \binom{2}{n-1}x^{2-(n-1)} & \cdots & \binom{n}{n-1}x^{n-(n-1)} \end{pmatrix} + xb \\ &= \det\Big(\binom{r+1}{i}\Big)\, x^n + xb \\ &= \prod_{i>s\geq 0}^{n} \frac{i+1-(s+1)}{i-s} x^n + xb \\ &= x^n + xb \neq 0, \end{aligned}$$

pues $\nu_P(b) \geq n$. Por lo tanto $v_i = i$. ⊡

En el ejemplo anterior el divisor de Frobenius es

$$S = \operatorname{div}\big(W_x(g)\big) + \left(\sum_{i=0}^{n-1} i\right)\operatorname{div}(dx) + (q+n)E = \operatorname{div}\big(W_x(g)\big) + \frac{(n-1)n}{2}\operatorname{div}(dx) + (q+n)nP_\infty$$

y $gr(S) = (q+1)n$, pues $gr\big(\operatorname{div}(dx)\big) = 2g-2 = -2$ ($g = 0$ pues C es racional).

Ejemplo 2.1.7. *Sea C la hermitiana $y^3 + y = x^4$, $k = \overline{\mathbb{F}_9}$ y $f = (1 : x : y)$. Luego, $y_{(1)} = D_x^{(1)}y = x^3$, $y_{(2)} = 0$ y $y_{(3)} = x - x^9$. Así, $\varepsilon_0 = 0$, $\varepsilon_1 = 1$ y $\varepsilon_2 = 3$. Además, $D_x^{(1)}f = (0, 1, x^3)$, $D_x^{(2)}f = (0, 0, 0)$ y $D_x^{(3)}f = (0, 0, x - x^9)$ por el Ejemplo 1.4.7. Veamos que $v_0 = 0$ y $v_1 = 3$. Con un razonamiento análogo al del ejemplo 2.1.6 tenemos que*

$$\begin{aligned}
\det\begin{pmatrix} 1 & x^9 & y^9 \\ 1 & x & y \\ 0 & 1 & x^3 \end{pmatrix} &= \det\begin{pmatrix} x - x^9 & y - y^9 \\ 1 & x^3 \end{pmatrix} \\
&= (x - x^9)x^3 - (y - y^9) \\
&= x^4 - x^{12} + y^9 - y \\
&= y + y^3 - x^{12} + y^9 - y \\
&= (y^3 + y - x^4)^3 = 0.
\end{aligned}$$

Luego, $f^q, f, D_x^{(\varepsilon_1)}f$ son linealmente dependientes y se tiene que $v_0 = 0$ y $v_1 = \varepsilon_2 = 3$.

Así que en el caso de la curva hermitiana tenemos que

$$W_x(f) = \det\begin{pmatrix} 1 & x^9 & y^9 \\ 1 & x & y \\ 0 & 0 & x - x^9 \end{pmatrix} = \det\begin{pmatrix} x - x^9 & y - y^9 \\ 0 & x - x^9 \end{pmatrix} = (x - x^9)^2$$

y $S = 2\operatorname{div}(x - x^9) + 3\operatorname{div}(dx) + 11E$. Ahora, como $d = gr(E) = gr(C) = 4$ y el género de C es $g = \frac{d-1)(d-2)}{2} = 3$, entonces $gr(S) = 3(2g-2) + 11 \cdot 4 = 56$.

Definición 2.1.8 (Sistema lineal clásico y ordinario)**.** *Diremos que un sistema lineal $\mathfrak{D}$ definido sobre una curva $C(\mathbb{F}_q)$ es $\mathbb{F}_q$-clásico ($\mathbb{F}_q$-ordinario) si la sucesión de ordenes $\mathbb{F}_q$-Frobenius es clásica (ordinaria). Es decir, si*

$$(v_0, \ldots, v_{n-1}) = (0, \ldots, n-1) \quad \big((v_0, \ldots, v_{n-1}) = (\varepsilon_0, \ldots, \varepsilon_{n-1})\big).$$

Observación 2.1.9. *El divisor $\mathbb{F}_q$-Frobenius, depende unicamente del sistema lineal $\mathfrak{D}$.*

1) *Independencia de la representación del morfismo inducido.*

Sea $f = (f_0 : \ldots : f_n) : C \to \mathbb{P}^n(k)$ y $hf = (hf_0 : \ldots : hf_n)$ donde $h \in k(C)^*$. Sean E y E' los divisores asociados a los morfismos f y hf (Véase la ecuación (2), pág. 19). Luego,

por la Proposición 1.2.3, pág. 19,

$$\begin{aligned} S(hf) &= \operatorname{div}\big(W_t(hf)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)E' \\ &= (q+n)\operatorname{div}(h) + \operatorname{div}\big(W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)\big(E - \operatorname{div}(h)\big) \\ &= \operatorname{div}\big(W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)E \\ &= S(\mathfrak{D}). \end{aligned}$$

2) *Independencia del morfismo inducido por* $\mathfrak{D}$.

Si f y g son dos morfismos inducidos por el sistema lineal $\mathfrak{D}$, entonces $g = T \circ f$ donde $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ es un isomorfismo (Véase las Proposiciones 1.2.3, 1.2.5 y sus comentarios). Luego, $g_i = \sum_{j=0}^{n} a_{ij} f_j$ donde $(a_{ij}) \in GL_{n+1}(k)$. Así que

$$\begin{aligned} S(g) &= \operatorname{div}\big(W_t(g)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)E \\ &= \operatorname{div}\big(\det(a_{ij})W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)E \\ &= S(\mathfrak{D}) \end{aligned}$$

3) *Independencia del parámetro separante.*

Sea u un parámetro separante de $\mathbb{F}_q(C)/\mathbb{F}_q$. Entonces, por la Proposición 1.4.2

$$\begin{aligned} S(u) &= \operatorname{div}\big(W_u(f)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(du) + (q+n)E \\ &= \operatorname{div}\left(\left(\tfrac{dt}{du}\right)^{\sum_{i=0}^{n-1} v_i} W_t(f)\right) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(du) + (q+n)E \\ &= \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}\left(\tfrac{dt}{du}\right) + \operatorname{div}\big(W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(du) + (q+n)E \\ &= \operatorname{div}\big(W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)E \\ &= S(\mathfrak{D}). \end{aligned}$$

⊡

En realidad podemos suponer que el morfismo f es $(1 : f_1 : \cdots : f_n)$ (dividiendo por $f_0 \in \mathbb{F}_q(C)^*$). Luego,

$$W_t^{(m_0,\ldots,m_{n-1})}(f) = \det \begin{pmatrix} 1 & f_1^q & \cdots & f_n^q \\ 1 & f_1 & \cdots & f_n \\ 0 & D_t^{(m_1)} f_1 & \cdots & D_t^{(m_1)} f_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & D_t^{(m_{n-1})} f_1 & \cdots & D_t^{(m_{n-1})} f_n \end{pmatrix}$$

y

$$\begin{aligned} W_t^{(m_0,\ldots,m_{n-1})}(f) &= \det\begin{pmatrix} 1 & f_1^q & \cdots & f_n^q \\ 0 & f_1 - f_1^q & \cdots & f_n - f_n^q \\ 0 & D_t^{(m_1)} f_1 & \cdots & D_t^{(m_1)} f_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & D_t^{(m_{n-1})} f_1 & \cdots & D_t^{(m_{n-1})} f_n \end{pmatrix} \\ &= \det\begin{pmatrix} f_1 - f_1^q & \cdots & f_n - f_n^q \\ D_t^{(m_1)} f_1 & \cdots & D_t^{(m_1)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_{n-1})} f_1 & \cdots & D_t^{(m_{n-1})} f_n \end{pmatrix}, \end{aligned}$$

donde en la segunda igualdad se resto la fila uno a la dos. Lo anterior nos permite resaltar algunos fenómenos cuando $m_i = v_i$.

Observación 2.1.10. *Si $v_i < q$, entonces $v_0, \ldots, v_i$ son los primeros $i+1$ ordenes del morfismo $g = (f_1 - f_1^q : \cdots : f_n - f_n^q) : C \to \mathbb{P}^{n-1}(\mathbb{F}_q)$.*

Podemos suponer que existe $P \in C$ tal que $0 < \nu_P(f_i) < \nu_P(f_j) < \infty$ si $i < j$, por los comentarios posteriores al teorema 1.3.6. Luego, $f_1 - f_1^q, \ldots, f_n - f_n^q$ es linealmente independiente sobre k, pues de lo contrario $\sum_{i=m}^n \big[\alpha_i(f_i - f_i^q)\big] = 0$ donde $\alpha_m \neq 0$ y $\alpha_i \in k$. Luego, $\nu_P\Big(\sum_{i=m}^n \big[\alpha_i(f_i - f_i^q)\big]\Big) = \nu_P(\alpha_m f_m) = \infty < \infty$ que no puede ser. Así que g es un morfismo tal que $g(C)$ no está contenido en ningún hiperplano H de $\mathbb{P}^{n-1}(k)$ y, por lo tanto, induce un sistema lineal s.p.b. (Proposición 1.2.5 y sus comentarios predecesores).

De otro lado, como la hiperderivada de Hasse es lineal y $D_t^{(v_j)}(f_i^q) = 0$ si v_j no es múltiplo de q (Observación 1.4.1), entonces los primeros $i+1$ ordenes de g son ordenes de Frobenius de $\mathfrak{D}$ (Observación 2.1.4). ⊡

De forma similar usando el corolario 1.5.12 tenemos la siguiente proposición:

Proposición 2.1.11. *Si $v_r < q$ es un orden $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$, entonces cada entero v tal que $\binom{v_r}{v} \not\equiv 0 \pmod p$ (v es p-adicamente más pequeño que v_r), es también un orden de Frobenius. En particular si $v_r < p$, entonces $(v_0, \ldots, v_r) = (0, \ldots, r)$.* ⊡

Ahora haremos un análisis local del divisor $S(\mathfrak{D})$ y/o del wronskiano $W_t^{(m_0,\ldots,m_{n-1})}(f)$. Obsérvese que todo punto $\mathbb{F}_q$-racional satisface que $\nu_P\big(W_t(f)\big) > 0$. De otro lado podemos suponer que la componente P-ésima del divisor E es cero y que t es un parametro P-uniformizante. Así, $\nu_P\big(S(\mathfrak{D})\big) = \nu_P\big(W_t^{(v_0,\ldots,v_{n-1})}(f)\big)$ pues $\nu_P\big(\mathrm{div}(dt)\big) = \nu_P(E) = e_P = 0$. Por lo tanto, si $v_i = j_i$ para todo i, entonces $P \in Sopp(S)$ si y sólo si, la imagen bajo el morfismo de Frobenius de $f(P)$, está en el hiperplano osculador L_{n-1}. De otro lado, si $v_i < j_i$ para algún i, entonces P está en el soporte de S.

Proposición 2.1.12. *Sea P un punto de C con invariantes hermitianos $j_0, \ldots, j_n$ y $v_0, \ldots, v_{n-1}$ los ordenes $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$. Entonces:*

a) $\nu_P\big(W_t^{(m_0,\ldots,m_{n-1})}(f)\big) \geq \sum_{i=1}^{n-1}(j_i - m_i)$ *con igualdad si y solo si,*

$$\det\left(\binom{j_r}{m_i}\right) \not\equiv 0 \pmod{p}.$$

En particular, $\nu_P\big(S(\mathfrak{D})\big) \geq \sum_{i=1}^{n-1}(j_i - v_i)$ *con desigualdad si,* $\det\left(\binom{j_r}{v_i}\right) \cong 0 \pmod{p}$

b) Si P es $\mathbb{F}_q$-racional, entonces $\nu_P\big(W_t^{(m_0,\ldots,m_{n-1})}(f))\big) \geq \sum_{i=0}^{n-1}(j_{i+1} - m_i)$. *La igualdad se da si y sólo si,* $\det\left(\binom{j_r}{m_i}\right) \not\equiv 0 \pmod{p}$. *En particular,* $\nu_P(S) \geq \sum_{i=0}^{n-1}(j_{i+1} - v_i)$.

c) El divisor $S(\mathfrak{D})$ es positivo (efectivo).

Prueba.

a) Aplicando una transformación proyectiva T inducida por $(a_{ij}) \in GL_{n+1}(k)$ podemos suponer que $e_P = 0$ y $g = (g_0 : \cdots : g_n) = T \circ f$ satisface que $g_i = \sum_{j=0}^{n} a_{ij} f_j = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$ y $c_i \in k^*$ (Véase los comentarios posteriores al teorema 1.3.6). Así que $\nu_P(g_i) \geq 0$ y $\nu_P(f_i) \geq 0$ $\big($si suponemos que $(b_{ij}) = (a_{ij})^{-1} \in GL_{n+1}(k)$, entonces $f_i = \sum_{j=0}^{n} b_{ij} g_j$ y $\nu_P(f_i) \geq \min\{\nu_P(g_0), \ldots, \nu_P(g_n)\} \geq 0\big)$. Sea $l_i = \sum_{j=0}^{n} a_{ij} f_j^q$. Luego, $\nu_P(l_i) \geq 0$ y

$$\det\begin{pmatrix} l_0 & \cdots & l_n \\ D_t^{(m_0)} g_0 & \cdots & D_t^{(m_0)} g_n \\ D_t^{(m_1)} g_0 & \cdots & D_t^{(m_1)} g_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_{n-1})} g_0 & \cdots & D_t^{(m_{n-1})} g_n \end{pmatrix} = \det(a_{ij}) W_t^{(m_0,\ldots,m_{n-1})}(f) = \sum_{i=0}^{n} (-1)^i l_i y_i$$

donde

$$\begin{aligned} y_s &= \det\begin{pmatrix} D_t^{(m_0)} g_0 & \cdots & D_t^{(m_0)} g_{s-1} & D_t^{(m_0)} g_{s+1} & \cdots & D_t^{(m_0)} g_n \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ D_t^{(m_{n-1})} g_0 & \cdots & D_t^{(m_{n-1})} g_{s-1} & D_t^{(m_{n-1})} g_{s+1} & \cdots & D_t^{(m_{n-1})} g_n \end{pmatrix} \\ &= c \det\left(\binom{j_r}{m_i} t^{j_r - m_i} + D_t^{(m_i)} h_r\right) \\ &= c \det\left(\binom{j_r}{m_i}\right) t^{\sum_{r=1}^{n}(j_r - m_{r-1}) - j_s} + t b_s \end{aligned}$$

y (adicionalemente) $r \neq s$ $(1 \leq r \leq n)$, $\nu_P\big(D_t^{(m_i)} h_r\big) > j_r - m_i$ y $\nu_P(b_i) \geq \sum_{r=1}^{n}(j_r - m_{r-1}) - j_i$ por la Proposición 1.5.4 (Ver también el Teorema 1.5.6). Así,

$$\nu_P(y_s) = \sum_{r=1}^{n}(j_r - m_{r-1}) - j_s \geq \sum_{r=1}^{n}(j_r - m_{r-1}) - j_n = \nu_P(y_n).$$

Por lo tanto,

$$\nu_P(W_t^{(m_0,\dots,m_{n-1})}(f)) \geq \sum_{i=1}^{n-1}(j_i - m_i)$$

con desigualdad si, $\det\left(\binom{j_r}{m_i}\right) \cong 0 \pmod p$.

b) Como $P \in C$ es racional, entonces los hiperplanos osculadores quedan definidos sobre $\mathbb{F}_q$ (Véase el Capítulo 1 y en particular la Sección 1.3). Así que podemos suponer despues de un cambio de coordenadas que $f_i = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$ y $c_i \in \mathbb{F}_q^*$. Podemos suponer además que $f_0 = 1$ (dividiendo por f_0 al morfismo f). Luego,

$$\begin{aligned} W_t^{(m_0,\dots,m_{n-1})}(f) &= \det\begin{pmatrix} f_1 - f_1^q & \cdots & f_n - f_n^q \\ D_t^{(m_1)} f_1 & \cdots & D_t^{(m_1)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_{n-1})} f_1 & \cdots & D_t^{(m_{n-1})} f_n \end{pmatrix} \\ &= c\det\left(\binom{j_r}{m_i} t^{j_r - m_i} + D_t^{(m_i)} l_r\right) \\ &= c\det\left(\binom{j_r}{m_i}\right) t^{\sum_{s=1}^n (j_s - m_{s-1})} + tb \end{aligned}$$

donde, $\nu_P(b) \geq \sum_{s=1}^n (j_s - m_{s-1})$ y $c \in \mathbb{F}_q^*$. Así, $\nu_P\big(W_t^{(m_0,\dots,m_{n-1})}(f)\big) \geq \sum_{i=0}^{n-1}(j_{i+1} - m_i)$, con igualdad si y sólo si, $\det\left(\binom{j_r}{m_i}\right) \not\cong 0 \ (mod\ p)$. En particular, si consideramos el divisor $\mathbb{F}_q$-Frobenius, entonces $v_i = m_i$, $e_P = 0$ y $\nu_P(S) \geq \sum_{i=0}^{n-1}(j_{i+1} - v_i)$.

c) Sea $P \in C$. Podemos suponer que $f_i = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$ y $c_i \in k^*$ y $j_0, \dots, j_n$ son los invariantes hermitianos de P. Así, $\nu_P(f_i) \geq 0$ y $\nu_P\big(D_t^{(m)} f\big) \geq 0$ para todo m. Luego, $\nu_P\big(S(\mathfrak{D})\big) = \nu_P\big(W_t^{(v_0,\dots,v_{n-1})}(f)\big) \geq 0$. ⊡

Por la Proposición 2.1.3, los mejores resultados de la proposición 2.1.12 se presentan cuando uno considera los ordenes $\mathbb{F}_q$-Frobenius.

Proposición 2.1.13. *Sea P un punto $\mathbb{F}_q$-racional de C con $(\mathfrak{D}, P)$-ordenes $j_0, \dots, j_n$ y $v_0, \dots, v_{n-1}$ los ordenes $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$. Si la sucesión de enteros $(m_0, \dots, m_{n-1})$ son tales que $0 \leq m_0 < \cdots < m_{n-1}$ y $\det\left(\binom{j_r - j_1}{m_i}\right) \not\cong 0 \pmod p$ para $r = 1, \dots, n$ e $i = 0, \dots, n-1$, entonces $v_i \leq m_i$.*

Prueba.

La mejor escogencia de los m_i son los ordenes del morfismo $g : \mathbb{P}^1(k) \to \mathbb{P}^{n-1}(k)$ dado por $g(1 : x) = (1 : x^{j_2 - j_1} : \cdots : x^{j_n - j_1})$ (El cuerpo de funciones racionales de la linea proyectiva es $k(x)$, donde x es trascendente sobre k), pues g es equivalente a $(x^{j_1} : x^{j_2} : \cdots : x^{j_n})$; y por lo tanto,

$$\begin{aligned} \det(D_x^{m_i} g_r) &= \det\left(\binom{j_r - j_1}{m_i} x^{j_r - j_1 - m_i}\right) &&= \det\left(\binom{j_r - j_1}{m_i}\right) x^{\sum_{s=0}^{n-1}(j_{s+1} - j_1 - m_s)} \\ &= x^{-nj_1}\det\left(\binom{j_r}{m_i} x^{j_r - m_i}\right) &&= x^{\sum_{s=0}^{n-1}(j_{s+1} - m_s) - nj_1}\det\left(\binom{j_r}{m_i}\right) \end{aligned}$$

De manera que podemos suponer que los m_i son los ordenes de g. Además, $\det\left(\binom{j_r-j_1}{m_i}\right) \neq 0 \iff det\left(\binom{j_r}{m_i}\right) \neq 0$. Luego, con un proceso análogo al de la Proposición 2.1.12 b) podemos asumir que $f_0 = 1$ y $f_i = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$, $c_i \in k^*$ y $W_t^{(m_0,\ldots,m_{n-1})}(f) = c \det\left(\binom{j_r}{m_i}\right) t^{\sum_{s=0}^{n-1}(j_{s+1}-m_s)} + tb \neq 0$; donde $\nu_P(b) \geq \sum_{s=0}^{n-1}(j_{s+1}-m_s)$ y $c \in \mathbb{F}_q^*$. Luego, $v_i \leq m_i$ por la Observación 2.1.4. ⊡

Como consecuencia inmediata de las proposiciones 2.1.12 y 2.1.13 se tiene el siguiente resultado:

Corolario 2.1.14. *Sea $P \in C$ es un punto $\mathbb{F}_q$-racional, y $j_0, \ldots, j_n$ sus correspondientes $(\mathfrak{D}, P)$-ordenes. Si $det\left(\binom{j_r}{m_i}\right) \not\equiv 0$ $(modp)$ entonces $m_i \leq j_{i+1} - j_1$ y $\nu_P\left(W_t^{(m_0,\ldots,m_{n-1})}(f)\right) \geq nj_1 \geq n\varepsilon_1$ donde ε_1 es el primer $\mathfrak{D}$-orden distinto de cero. En particular, si S es el divisor $\mathbb{F}_q$-Frobenius entonces $v_i \leq j_{i+1} - j_1$ y $\nu_P(S) \geq n$.*

El caso $v_i = i$ o $v_i = \varepsilon_i$ (donde $\varepsilon_0, \ldots, \varepsilon_{n-1}, \varepsilon_n$ son los $\mathfrak{D}$-ordenes) en la proposición 2.1.13, nos produce el siguiente resultado:

Corolario 2.1.15. *Si $\prod_{r>i\geq 1}^{n} \frac{j_r - j_i}{r-i}$ no es divisible por p $\Big(\det\left(\binom{j_r}{\varepsilon_i}\right) \not\equiv 0$ $pmodp\Big)$, entonces $v_i = i$ $(v_i = \varepsilon_i)$ y $\nu_P(S) = n + \sum_{i=1}^{n}(j_i - i)$ $\left(\nu_P(S) = \varepsilon_n + \sum_{i=1}^{n}(j_i - \varepsilon_i)\right)$.*

El siguiente corolario nos dice que es geometricamente "raro" encontrar sistemas lineales que no sean $\mathbb{F}_q$-clasicos o $\mathbb{F}_q$-ordinarios.

Corolario 2.1.16. *Si la sucesión de ordenes $\mathbb{F}_q$-Frobenius $(v_0, \ldots, v_{n-1})$ de $\mathfrak{D}$ difiere de $(0, 1, \ldots, n-1)$ $\left((\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})\right)$, entonces cada punto $\mathbb{F}_q$-racional es $\mathfrak{D}$-osculador ($\mathfrak{D}$-Weierstrass).*

Prueba.

Argumentemos por contradicción suponiendo que existe un punto racional clásico (ordinario). Luego, por el Corolario 2.1.14 $v_i \leq i + 1 - 1 = i$ $(v_i \leq \varepsilon_{i+1} - \varepsilon_1 < \varepsilon_{i+1})$ y por la Proposición 2.1.3 $v_i = i$ $(v_i = \varepsilon_i)$. ⊡

Ejemplo 2.1.17. Sea C la curva proyectiva inducida por la extensión de *Kummer* $y^3 = x^4 + x + 1$ donde $k = \overline{\mathbb{F}_4}$ y $f = (1 : x : y^2)$ y $\mathfrak{D}$ su respectivo sistema lineal. Por el Ejemplo 1.4.6 la sucesión de $\mathfrak{D}$-ordenes es clásica $(\varepsilon_i = i,\ i = 0, 1, 2)$ y el punto $(1 : 0 : 1) \in C$. Luego, por el Corolario 2.1.15 $v_0 = 0$ y $v_1 = 1$. Es decir, C es una curva $\mathbb{F}_q$-clásica respecto a $\mathfrak{D}$.

El resultado del ejemplo anterior puede verificarse por un cálculo directo. Observe que el resultado del ejemplo 2.1.6 es también un caso particular del corolario 2.1.15.

2.2. El Teorema de Stöhr–Voloch

Recordemos que venimos trabajando en un cuerpo finito $\mathbb{F}_q$ de característica p el cual tiene una clausura algebraica $k = \overline{\mathbb{F}_q}$ y una curva C algebraica, proyectiva, no singular, definida sobre k de género g. Un sistema lineal sin puntos básicos $\mathfrak{D}$ definido sobre $C(\mathbb{F}_q)$ tiene asociado un morfismo $f = (f_0, \ldots, f_n) : C \to \mathbb{P}^n(k)$ y un divisor $\mathbb{F}_q$-Frobenius $S(\mathfrak{D}) = \operatorname{div}\big(W_t^{(v_0,\ldots,v_{n-1})}(f)\big) + \big(\sum_{i=0}^{n-1} v_i\big)\operatorname{div}(dt) + (q+n)E$, donde t es un parametro separante de $\mathbb{F}_q(C)/\mathbb{F}_q$,

$$W_t^{(v_0,\ldots,v_{n-1})}(f) = \det \begin{pmatrix} f^q \\ D_t^{(v_0)} f \\ \vdots \\ D_t^{(v_{n-1})} f \end{pmatrix} \neq 0,$$

$\nu_P(E) = -\min\big\{\nu_P(f_0), \ldots, \nu_P(f_n)\big\}$, $\dim(\mathfrak{D}) = l(E) - 1 = n$ y $gr(\mathfrak{D}) = gr(E) = d$.

Hasta aquí, el lector debe haberse dado cuenta que el corolario 2.1.14, nos permite obtener una cota para N_q (el número de puntos $\mathbb{F}_q$-racionales de la curva C). Es decir, tenemos el siguiente resultado:

Proposición 2.2.1. *Si C es una curva definida sobre k y $m_0, \ldots, m_{n-1}$ son enteros positivos tales que $W_t^{(m_0,\ldots,m_{n-1})}(f) \neq 0$ y $\mathfrak{D}$ es un sistema lineal s.p.b inducido por f, con ordenes $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$, entonces*

$$N_q \leq \frac{\big(\sum_{i=0}^{n-1} m_i\big)(2g-2) + (q+n)d}{\varepsilon_1 n}$$

Prueba.

Por el Corolario 2.1.14

$$N_q \leq \sum_{P \in C(\mathbb{F}_q)} \frac{\nu_P\big(W_t^{(m_0,\ldots,m_{n-1})}(f)\big)}{\varepsilon_1 n}$$

y como

$$\sum_{P \in C(\mathbb{F}_q)} \nu_P\big(W_t^{(m_0,\ldots,m_{n-1})}(f)\big) \leq \big(\sum_{i=0}^{n-1} m_i\big)(2g-2) + (q+n)d,$$

entonces

$$N_q \leq \frac{\big(\sum_{i=0}^{n-1} m_i\big)(2g-2) + (q+n)d}{\varepsilon_1 n}.$$

⊡

Como consecuencia inmediata se tiene el teorema de Stöhr–Voloch.

Teorema 2.2.2 (Stöhr–Voloch)**.** *Sea C una curva algebraica proyectiva, no singular, de género g, definida sobre $\mathbb{F}_q$ y N el número de puntos racionales. Si existe un sistema lineal sin puntos básicos definido sobre $\mathbb{F}_q$ de grado d y dimensión n, con ordenes de Frobenius $v_0, \ldots, v_{n-1}$, entonces*

$$N \leq \frac{\left(\sum_{i=0}^{n-1} v_i\right)(2g-2) + (q+n)d}{n}.$$

Este tipo de acotamiento del número de lugares racionales de un cuerpo de funciones, se conoce como el *Método Stöhr–Voloch*. Este implica la *hipótesis de Riemann sobre cuerpos de funciones* y tiene muchas aplicaciones. Por ejemplo, permite obtener cotas mejores que la de Hasse–Weil en algunos casos particulares, como se verá en el siguiente capítulo.

Ejemplo 2.2.3. Sea $C = \mathbb{P}^1(k)$ donde $k = \overline{\mathbb{F}_q}$. Obsérvese que $k(C) = k(x)$ donde x es la función coordenada. El sistema lineal $\mathfrak{D} = |nP_\infty|$ no tiene puntos básicos y el morfismo correspondiente es $f = (1 : x : \ldots : x^n)$. Por el Ejemplo 2.1.6 y el Teorema 2.2.2, $q+1 \leq N_q \leq \frac{gr(S)}{n} = q+1$. Es decir, $N_q = q+1$ y la cota del Teorema de Stöhr–Voloch se alcanza en el caso trivial que es un caso clásico.

Analogamente para la curva hermitiana del Ejemplo 2.1.7 tenemos que $N \leq \frac{gr(S)}{2} = 28$. Pero por el Ejemplo 1.4.7, $N = 28$. Es decir, la cota es alcanzada en un caso no clásico. Esto nos asegura que el método Stöhr–Voloch no se puede mejorar en el sentido de escoger invariantes más pequeños que los ordenes de Frobenius.

En el caso en que la sucesión de ordenes de Frobenius es clásica, entonces por el Teorema 2.2.2

$$N \leq \frac{(\sum_{i=0}^{n-1} i)(2g-2) + (q+n)d}{n} \leq \frac{n(n-1)(g-1) + (q+n)d}{n}.$$

Es decir,

$$N \leq (n-1)(g-1) + \frac{(q+n)d}{n}. \tag{6}$$

Luego, tenemos los siguientes corolarios:

Corolario 2.2.4. *Si $N > (n-1)(g-1) + \frac{(q+n)d}{n}$ $\left(N > \frac{2\left(\sum_{i=0}^{n-1} \varepsilon_i\right)(g-1)+(q+n)d}{n}\right)$, entonces cada punto racional es un punto $\mathfrak{D}$-osculador ($\mathfrak{D}$-Weierstrass).*

Prueba.

Por el Teorema 2.2.2 $v_i \neq i$ ($v_i \neq \varepsilon_i$) para algún i. Luego, por el Corolario 2.1.16 cada punto racional es $\mathfrak{D}$-osculador ($\mathfrak{D}$-Weierstrass). ⊡

Corolario 2.2.5. *Si $p < n+1$ y $N > \frac{(n^2+n-2p+2)(g-1)+(q+n)d}{n}$ ó, $p > n$ y*

$$N > (n-1)(g-1) + \frac{(q+n)d}{n},$$

entonces $\mathfrak{D}$ no es clásico. Es decir, cada punto $P \in C$ es $\mathfrak{D}$-osculador.

Prueba.

Suponga que $\mathfrak{D}$ es clásico ($\varepsilon_i = i$). Luego, $v_i \leq i+1$ (Proposición 2.1.3) y por la Proposición 2.1.11 $v_i = i$ si $i+1 < p$ ($i \leq p-2$). Así,

$$\begin{array}{rcl} N & \leq & \frac{2\left(\sum_{i=0}^{p-2} i+\sum_{i=p-1}^{n-1}(i+1)\right)(g-1)+(q+n)d}{n} \quad = \quad \frac{2\left(\sum_{i=0}^{n-1} i+\sum_{i=p-1}^{n-1} 1\right)(g-1)+(q+n)d}{n} \\ & \leq & \frac{2\left(\frac{n(n-1)}{2}+n-p+1\right)(g-1)+(q+n)d}{n} \quad = \quad \frac{(n^2+n-2p+2)(g-1)+(q+n)d}{n} \end{array}$$

que contradice. De otro lado, si $p > n$ entonces $(v_0, \ldots, v_{n-1}) = (0, \ldots, n-1)$ (obsérvese que $v_{n-1} \leq \varepsilon_n = n < p$ y el uso de las Proposiciones 2.1.3 y 2.1.11). Luego,

$$N \leq (n-1)(g-1) + \frac{(q+n)d}{n}$$

que es una contradicción. ⊡

Se concluye del método Stöhr–Voloch que si una curva tiene muchos puntos racionales, entonces su geometría es extraña.

2.3. Generalización del método Stöhr–Voloch

Sea $\mathbb{F}_{q_0}$ el cuerpo de Galois con q_0 elementos de característica p y $k = \overline{\mathbb{F}_{q_0}}$ su clausura algebraica. Sea C una curva algebraica irreducible y no singular definida sobre $\mathbb{F}_{q_0}$ de género g.

Sea $f : C \to \mathbb{P}^n(k)$ un $\mathbb{F}_{q_0}$-morfismo. Es decir, $f = (f_0, \ldots, f_n)$ donde $f_i \in \mathbb{F}_{q_0}(C) \subset k(C)$ (la función f_i es $\mathbb{F}_{q_0}$-racional).

Supongamos además que $f(C)$ no está contenido en ningún hiperplano H de $\mathbb{P}^n(k)$. Luego, el morfismo f induce un sistema lineal $\mathfrak{D}(f) = \mathfrak{D}$ sin puntos básicos (s.p.b) (Véase la Proposición 1.2.5 y sus comentarios precedentes); es decir, para cada $P \in C$ existe $D \in \mathfrak{D}$ tal que P no pertenece al soporte de D ($P \notin Sopp(D)$ o $P \not\leq D$). De otro lado, definimos el divisor $E = \sum_{P \in C(\mathbb{F}_{q_0})} e_P \in \mathcal{D}_C$, donde $e_P = -\min\{\nu_P(f_0), \ldots, \nu_P(f_n)\}$ (Véase el Capítulo 1, ecuación 2, pág. 19). Obsérvese que E y $\mathfrak{D}$ quedan definidos sobre $\mathbb{F}_{q_0}$.

Sea $q_1, q_2, \ldots, q_m$ enteros tales que tales que $\mathbb{F}_{q_0} \subset \mathbb{F}_{q_1}$, $q_i = q_1^{a_i}$, $q_i \neq q_j$ si $i \neq j$ y N_q el número de puntos $\mathbb{F}_q$-racionales. Cuando se sobreentienda el q entonces denotaremos por N al número de puntos racionales. Para obtener una cota para N, estudiamos el

wronskiano

$$W_t^{(w_0,\ldots,w_{n-m})}(f) := \det \begin{pmatrix} f^{q_1} \\ \vdots \\ f^{q_m} \\ D_t^{(w_0)} f \\ \vdots \\ D_t^{(w_{n-m})} f \end{pmatrix}$$

donde $w_i \in \mathbb{Z}_0^+$, $\mathbb{F}_q \subset \mathbb{F}_{q_r}$ para algún $r \in \{1,\ldots,m\}$ y t es un parametro separante de $\mathbb{F}_{q_0}(C)/\mathbb{F}_{q_0}$. Cuando se sobreentienda la sucesión $(w_0,\ldots,w_{n-m})$ denotaremos a $W_t^{(w_0,\ldots,w_{n-m})}$ por W_t.

Obsérvese que si permutamos los q_i entonces el wronskiano se altera unicamente en signo por la antisimetría del determinante.

Proposición 2.3.1. *Sea $f = (f_0 : \cdots : f_n) : C \to \mathbb{P}^n(k)$ el morfismo inducido por el sistema lineal s.p.b $\mathfrak{D}$ y $(w_0,\ldots,w_{n-m})$ una sucesión de enteros no negativos.*

a) Si $g_i = \sum_{j=0}^n a_{ij} f_j$ con $(a_{ij}) \in GL_{n+1}(\mathbb{F}_{q_0})$, entonces

$$W_t(g) = \det(a_{ij}) W_t(f).$$

Además, si $w_0 < w_1 < \cdots < w_{n-m}$ y $\langle D_t^{(w_0)} f,\ldots,D_t^{(w_{i-1})} f\rangle = \langle D_t^{(0)} f, D_t^{(1)} f,\ldots,D_t^{(w_i-1)} f\rangle$ para $i = 1,2,\ldots,n-m+1$, se tienen los siguientes resultados:

b) Si $h \in k(C)$, entonces $W_t(hf) = (\epsilon + h) h^{\sum_{i=1}^m q_i + n - m} W_t(f)$ para algún $\epsilon \in k(C)$. También, si $w_0 = 0$ entonces $\epsilon = 0$ y

$$W_t(hf) = h^{\sum_{i=1}^m q_i + n - m + 1} W_t(f)$$

c) Si $u \in k(C)$ es otra variable separante de $\mathbb{F}_{q_0}(C)/\mathbb{F}_{q_0}$ entonces

$$W_u(f) = \left(\left(\frac{dt}{du} \right)^{w_0} + \epsilon \right) \left(\frac{dt}{du} \right)^{\sum_{i=1}^{n-m} w_i} W_t(f)$$

, para algún $\epsilon \in k(C)$. En el caso $w_0 = 0$, entonces $W_u(f) = \left(\frac{dt}{du}\right)^{\sum_{i=0}^{n-m} w_i} W_t(f)$.

La demostración de esta proposición es análoga a la de la proposición 2.1.1.

Prueba.

a) Obsérvese, que $a_{ij} \in \mathbb{F}_{q_0}$ si y solo si, $a_{ij}^{q_0} = a_{ij}$. Luego, $g_i^{q_0} = \left(\sum_{j=0}^n a_{ij} f_j\right)^{q_0} = \sum_{j=0}^n a_{ij} f_j^{q_0}$. De otro lado, por la linealidad del operador $D_t^{(w_r)}$

$$D_t^{(w_r)} g_i = \sum_{j=0}^n a_{ij} D_t^{(w_r)} f_j.$$

Luego, por la multiplicación de matrices tenemos

$$\begin{aligned} W_t(g) &= \det \begin{pmatrix} \sum_{j=0}^n a_{0j} f_j^{q_1} & \cdots & \sum_{j=0}^n a_{nj} f_j^{q_1} \\ \vdots & \ddots & \vdots \\ \sum_{j=0}^n a_{0j} f_j^{q_m} & \cdots & \sum_{j=0}^n a_{nj} f_j^{q_m} \\ \sum_{j=0}^n a_{0j} D_t^{(w_0)} f_j & \cdots & \sum_{j=0}^n a_{nj} D_t^{(w_0)} f_j \\ \vdots & \ddots & \vdots \\ \sum_{j=0}^n a_{0j} D_t^{(w_{n-m})} f_j & \cdots & \sum_{j=0}^n a_{nj} D_t^{(w_{n-m})} f_j \end{pmatrix} \\ &= \det \begin{pmatrix} a_{00} & \cdots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{n0} & \cdots & a_{nn} \end{pmatrix} \det \begin{pmatrix} f_0^{q_1} & \cdots & f_n^{q_1} \\ \vdots & \ddots & \vdots \\ f_0^{q_m} & \cdots & f_n^{q_m} \\ D_t^{(m_0)} f_0 & \cdots & D_t^{(m_0)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(w_{n-m})} f_0 & \cdots & D_t^{(w_{n-m})} f_n \end{pmatrix} \\ &= \det(a_{ij}) W_t(f). \end{aligned}$$

b) Claramente $(hf)^{q_i} = h^{q_i} f^{q_i}$. De otro lado, usando la Observación 1.4.1 y la hipótesis sobre los espacios generados tenemos que

$$D_t^{(w_0)}(hf_j) = hD_t^{(w_0)} f_j + \sum_{s=1}^{w_0} D_t^{(s)} h D_t^{(w_0-s)} f_j$$

y

$$\Big(\sum_{s=1}^{w_0} D_t^{(s)} h D_t^{(w_0-s)} f_0, \ldots, \sum_{s=1}^{w_0} D_t^{(s)} h D_t^{(w_0-s)} f_n \Big) = \epsilon \big(D_t^{(w_0)} f_0, \ldots, D_t^{(w_0)} f_n \big),$$

para algún $\epsilon \in k(C)$. De manera que $\epsilon = 0$ si $w_0 = 0$. Así,

$$\big(D_t^{(w_0)}(hf_0), \ldots, D_t^{(w_0)}(hf_n) \big) = (\epsilon + h) \big(D_t^{(w_0)} f_0, \ldots, D_t^{(w_0)} f_n \big).$$

Luego, por la Observación 1.4.1 y la linealidad del determinante

$$\begin{aligned} W_t(hf) &= \det \begin{pmatrix} h^{q_1} f_j^{q_1} \\ \vdots \\ h^{q_m} f_j^{q_m} \\ (h+\epsilon) D_t^{(w_0)} f_j \\ h D_t^{(w_1)} f_j + \sum_{s=1}^{w_1} D_t^{(s)} h D_t^{(w_1-s)} f_j \\ \vdots \\ h D_t^{(w_{n-m})} f_j + \sum_{s=1}^{w_{n-m}} D_t^{(s)} h D_t^{(w_{n-m}-s)} f_j \end{pmatrix} \\ &= (\epsilon + h) h^{\sum_{i=1}^m q_i + n - m} W_t(f). \end{aligned}$$

Además, si $w_0 = 0$ entonces $\epsilon = 0$ y

$$W_t(hf) = h^{\sum_{i=1}^{m} q_i + n - m + 1} W_t(f).$$

c) Análogamente a b) pero usando la regla de la cadena para la derivada de Hasse (Observación 1.4.1, 2) tenemos que

$$\begin{aligned} W_u(f) &= \left(\left(\tfrac{dt}{du}\right)^{w_0} + \epsilon\right) \det \begin{pmatrix} f_j^{q_1} \\ \vdots \\ f_j^{q_m} \\ D_t^{(w_0)} f_j \\ \left(\tfrac{dt}{du}\right)^{w_0} D_t^{(w_1)} f_j + \sum_{s=1}^{m_1} D_t^{(s)} h D_t^{(m_1 - s)} f_j \\ \vdots \\ \left(\tfrac{dt}{du}\right)^{w_{n-m}} D_t^{(w_{n-m})} f_j + \sum_{s=1}^{w_{n-m}} D_t^{(s)} h D_t^{(w_{n-m} - s)} f_j \end{pmatrix} \\ &= \left(\left(\tfrac{dt}{du}\right)^{w_0} + \epsilon\right) \left(\tfrac{dt}{du}\right)^{\sum_{i=1}^{n-m} w_i} W_t(f) \end{aligned}$$

y si $w_0 = 0$ entonces

$$W_u(f) = \left(\frac{dt}{du}\right)^{\sum_{i=0}^{n-m} w_i} W_t(f).$$

⊡

Lema 2.3.2. *Sean $a_0, a_1 \ldots, a_n$ elementos de un cuerpo L de característica p y $b_0, b_1 \ldots, b_n \in \mathbb{Z}^+$. Si*

$$a_i \neq a_j,\ b_i > b_j \quad y \quad b_i \equiv b_j \pmod{p}$$

para $i > j$, entonces

$$\det(a_i^{b_j}) = \prod_{i=0}^{n} a_i^{b_0} \prod_{i > j \geq 0}^{n} (a_i - a_j)^{b_{j+1} - b_j} \neq 0.$$

En particular las filas de la matriz $[a_i^{b_j}]$ son linealmente independientes.

Prueba.

Por inducción sobre n. Primeramente, obsérvese que

$$a_i^{b_r} - a_i^{b_s} a_j^{b_r - b_s} = a_i^{b_s}(a_i^{b_r - b_s} - a_j^{b_r - b_s}) = a_i^{b_s}(a_i - a_j)^{b_r - b_s},$$

si $i > j$ y $r > s$ (se usó la condición de los b_t). Ahora, si $n = 1$ entonces

$$\begin{aligned} \det \begin{pmatrix} a_0^{b_0} & a_1^{b_0} \\ a_0^{b_1} & a_1^{b_1} \end{pmatrix} &= \det \begin{pmatrix} a_0^{b_0} & a_1^{b_0} \\ 0 & a_1^{b_0}(a_1 - a_0)^{b_1 - b_0} \end{pmatrix} = a_0^{b_0} a_1^{b_0} (a_1 - a_0)^{b_1 - b_0} \\ &= \textstyle\prod_{i=0}^{1} a_i^{b_0} \prod_{i > j \geq 0}^{1} (a_i - a_j)^{b_{j+1} - b_j} \neq 0. \end{aligned}$$

Supongamos que se tiene el resultado para $n-1$. Es decir,

$$\det(a_i^{b_j}) = \prod_{i=0}^{n-1} a_i^{b_0} \prod_{i>j\geq 0}^{n-1} (a_i - a_j)^{b_{j+1}-b_j} \neq 0$$

para $i, j = 0, 1, \ldots n-1$. Luego,

$$\begin{aligned}
\det(a_i^{b_j}) &= \det \begin{pmatrix} a_0^{b_0} & a_1^{b_0} & \cdots & a_n^{b_0} \\ a_0^{b_1} & a_1^{b_1} & \cdots & a_n^{b_1} \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{b_n} & a_1^{b_n} & \cdots & a_n^{b_n} \end{pmatrix} \\
&= \det \begin{pmatrix} a_0^{b_0} & a_1^{b_0} & \cdots & a_n^{b_0} \\ 0 & a_1^{b_0}(a_1-a_0)^{b_1-b_0} & \cdots & a_n^{b_0}(a_1-a_0)^{b_1-b_0} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_1^{b_0}(a_1-a_0)^{b_n-b_0} & \cdots & a_n^{b_0}(a_1-a_0)^{b_n-b_0} \end{pmatrix} \\
&= \textstyle\prod_{i=0}^{n} a_i^{b_0} \det \begin{pmatrix} (a_1-a_0)^{b_1-b_0} & \cdots & (a_1-a_0)^{b_1-b_0} \\ \vdots & \ddots & \vdots \\ (a_1-a_0)^{b_n-b_0} & \cdots & (a_1-a_0)^{b_n-b_0} \end{pmatrix}
\end{aligned}$$

Luego, del caso $n-1$

$$\begin{aligned}
\det(a_i^{b_j}) &= \textstyle\prod_{i=0}^{n} a_i^{b_0} \prod_{i=0}^{n-1}(a_i-a_0)^{b_1-b_0} \prod_{i>j\geq 1}^{n-1}(a_i-a_j)^{b_{j+1}-b_j} \\
&= \textstyle\prod_{i=0}^{n} a_i^{b_0} \prod_{i>j\geq 0}^{n}(a_i-a_j)^{b_{j+1}-b_j} \neq 0.
\end{aligned}$$

y se tiene el resultado. Además, si el determinante de una matriz es no nulo entonces sus filas son linealmente independientes. ⊡

El lema anterior (2.3.2) es similar al determinante de Vandermonde y nos asegura que el conjunto $\{f^{q_1}, \ldots, f^{q_m}\}$ es linealmente independiente.

Observación 2.3.3. *Si $f : C \to \mathbb{P}^n(k)$ es un $\mathbb{F}_{q_0}$-morfismo y $q_1^{n+1} > \max\{q_i\}$ entonces, $\{f^{q_1}, \ldots, f^{q_m}, f\}$ es linealmente independiente. Es decir,*

$$ran \begin{pmatrix} f_0^{q_1} & \cdots & f_n^{q_1} \\ \vdots & \ddots & \vdots \\ f_0^{q_m} & \cdots & f_n^{q_m} \\ f_0 & \cdots & f_n \end{pmatrix} = m+1$$

Supongamos que $\{f^{q_1}, \ldots, f^{q_m}, f\}$ es linealmente dependiente. Luego, existen $\lambda_0 \ldots, \lambda_m \in k(C)$ tales que $\lambda_0 f_i + \lambda_1 f_i^{q_1} + \ldots + \lambda_m f_i^{q_m} = 0$ para $i = 0, \ldots, n$. Luego, $x = \sum_{j=0}^{n} a_j f_j$ con $a_j \in \mathbb{F}_{q_1}$ es solución del polinomio linealizado $L(X) = \lambda_0 X + \lambda_1 X^{q_1} + \cdots + \lambda_m X_i^{q_m} = 0$.

Pero, $gr(L) \leq \text{máx}\{q_i\}$ y tenemos q_1^{n+1} soluciones de la forma x anterior (exceso de raices. Véase Roman [11], Sec. 9.4, pág. 182-184). Luego, $L(X) = 0$ y $\lambda_r = 0$.

Suponemos en esta generalización que $q_1^{n+1} > \text{máx}\{q_i\}$ de acuerdo a la observación 2.3.3. Sin embargo los resultados procedentes dependerán unicamente de la independencia lineal de $\{f^{q_1}, \ldots, f^{q_m}, f\}$.

Proposición 2.3.4. *Sean $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$ los respectivos ordenes del sistema lineal s.p.b. $\mathfrak{D}$ y f el morfismo inducido por $\mathfrak{D}$. Existen $v_{(m,0)}, \ldots, v_{(m,n-m)}$ enteros no negativos tales que $W_t^{(v_{(m,0)},\ldots,v_{(m,n-m)})}(f) \neq 0$. Además, si la sucesión $(v_{(m,0)}, \ldots, v_{(m,n-m)})$ es escogida en el orden lexicográfico (es decir, $v_{(m,0)} = 0$ y si $f^{q_1}, \ldots, f^{q_m}, D_t^{(v_{(m,0)})}f, \ldots, D_t^{(v_{(m,n-i-1)})}f$ son linealmente independientes entonces $v_{(m,n-i)}$ es el entero más pequeño tal que $f^{q_1}, \ldots, f^{q_m}, D_t^{(v_{(m,0)})}f, \ldots, D_t^{(v_{(m,n-i)})}f$ son linealmente independientes) entonces existen $s_1, \ldots, s_m \in \mathbb{Z}$ tal que*

$$v_{(m,i)} = \begin{cases} \varepsilon_i & si\ i < s_1 \\ \varepsilon_{i+1} & si\ s_1 \leq i < s_2 \\ \vdots & \vdots \\ \varepsilon_{i+m} & si\ s_m \leq i \leq n-m \end{cases}$$

Prueba.

Por inducción sobre m. Para $m = 1$ el resultado se tiene por la Proposición 2.1.3. Supongamos que el resultado se cumple para $s = m - 1$. Es decir, existen $\alpha_r \in \mathbb{Z}$ tales que

$$v_{(s,i)} = \begin{cases} \varepsilon_i & \text{si } i < \alpha_1 \\ \varepsilon_{i+1} & \text{si } \alpha_1 \leq i < \alpha_2 \\ \vdots & \vdots \\ \varepsilon_{i+m} & \text{si } \alpha_s < i \leq n-s \end{cases}$$

donde los $v_{(s,i)}$ están escogidos de forma lexicográfica. Sea l el menor entero tal que

$$ran \begin{pmatrix} f^{q_1} \\ \vdots \\ f^{q_s} \\ f^{q_m} \\ D_t^{(v_{(s,0)})}f \\ \vdots \\ D_t^{(v_{(s,l)})}f \end{pmatrix} = m + l$$

Claramente, $l > 0$ por la Observación 2.3.3. Definamos

$$v_{(m,i)} = \begin{cases} v_{(s,i)} & \text{si } i < l \\ v_{(s,i+1)} & \text{si } l \leq i \geq n-m \end{cases}$$

Así, $W_t^{(v_{(m,0)},\ldots,v_{(m,n-m)})}(f) \neq 0$ (Se ha usado el Lema 2.1.2).

Supongamos ahora que tenemos la sucesión de enteros $(w_0,\ldots,w_{n-m})$ escogida en el orden lexicográfico tal que $0 = w_0 < \cdots < w_{n-m}$ y $W_t^{(w_0,\ldots,w_{n-m})}(f) \neq 0$. Luego, $w_i \leq v_{(m,i)}$ para $i = 0,1,\ldots,n-1$. De otro lado, como $f^{q_1},\ldots,f^{q_m},D_t^{(w_0)}f,\ldots,D_t^{(w_{n-m})}f$ son linealmente independientes, entonces $f^{q_1},\ldots,f^{q_s},D_t^{(w_0)}f,\ldots,D_t^{(w_{n-m})}f$ es linealmente independiente. Así, por la minimalidad de los $v_{(s,i)}$ tenemos que $v_{(s,i)} \leq w_i$ para $i = 0,1,\ldots,n-s$. Luego, $w_i = v_{(m,i)} = v_{(s,i)}$ para $i < l$. Concluimos entonces que $f^{q_1},\ldots,f^{q_m},D_t^{(v_{(m,0)})}f,D_t^{(v_{(m,1)})}f,\ldots,D_t^{(v_{(m,l-1)})}f,D_t^{(w_l)}f,\ldots,D_t^{(w_{n-1})}f$ son linealmente independientes y por el Lema 2.1.2,

$$\{f^{q_1},\ldots,f^{q_s},D_t^{(v_{(s,l)})}f,D_t^{(v_{(m,0)})}f,D_t^{(v_{(m,1)})}f,\ldots,D_t^{(v_{(m,l-1)})}f,D_t^{(w_l)}f,\ldots,D_t^{(w_{n-1})}f\} =$$
$$\{f^{q_1},\ldots,f^{q_s},D_t^{(v_{(m,0)})}f,D_t^{(v_{(m,1)})}f,\ldots,D_t^{(v_{(m,l-1)})}f,D_t^{(v_{(s,l)})}f,D_t^{(w_l)}f,\ldots,D_t^{(w_{n-1})}f\} \text{ es}$$

linealmente independiente. Luego, $v_{(m,i)} = v_{(s,i+1)} \leq w_i$ para $i \geq l$ por la minimalidad de los $v_{(s,i)}$. Por lo tanto, $w_i = v_{(m,i)}$ para $i = 0,1,\ldots,n-m$. Ahora, si $\alpha_a = \text{máx}\{\alpha_i < l\}$ y además, definimos $s_i = \alpha_i$ si $i \leq a$ y, $s_i = \alpha_{i+1}$ si $a < i < n-m$ se tiene el resultado. ⊡

Observación 2.3.5. *Los $v_{(m,i)}$ son mínimos en un sentido aún más general: Si $w_0,w_1,\ldots,w_s$ son enteros no negativos tales que $w_0 < w_1 < \cdots < w_s$ y $f^{q_1},\ldots,f^{q_m},D_t^{(w_0)}f,\ldots,D_t^{(w_s)}f$ son vectores linealmente independientes sobre $k(C)$, entonces $v_{(m,i)} \leq w_i$ para $i = 0,1,\ldots,s$.*

La observación anterior es análoga a la Observación 2.1.4.

En efecto

$$ran\begin{pmatrix} f_0^{q_1} & \cdots & f_n^{q_1} \\ \vdots & \ddots & \vdots \\ f_0^{q_m} & \cdots & f_n^{q_m} \\ D_t^{(0)}f_0(P) & \cdots & D_t^{(0)}f_n(P) \\ D_t^{(1)}f_0(P) & \cdots & D_t^{(1)}f_n(P) \\ \vdots & \ddots & \vdots \\ D_t^{(v_{(m,r)}-1)}f_0(P) & \cdots & D_t^{(v_{(m,r)}-1)}f_n(P) \end{pmatrix} = ran\begin{pmatrix} f^{q_1} \\ \vdots \\ f^{q_m} \\ D_t^{(v_{(m,0)})}f(P) \\ D_t^{(v_{(m,1)})}f(P) \\ \vdots \\ D_t^{(v_{(m,r-1)})}f(P) \end{pmatrix} = r+m.$$

Luego, $v_{(m,r)} - 1 < w_r$ *pues*

$$ran \begin{pmatrix} f_0^{q_1} & \cdots & f_n^{q_1} \\ \vdots & \ddots & \vdots \\ f_0^{q_m} & \cdots & f_n^{q_m} \\ D_t^{(w_0)} f_0(P) & \cdots & D_t^{(w_0)} f_n(P) \\ D_t^{(w_1)} f_0(P) & \cdots & D_t^{(w_1)} f_n(P) \\ \vdots & \ddots & \vdots \\ D_t^{(w_r)} f_0(P) & \cdots & D_t^{(w_r)} f_n(P) \end{pmatrix} = r + m + 1.$$

y $v_{(m,r)} \leq m_r$.

Definición 2.3.6 (Ordenes y Divisor de Frobenius)**.** *Sea* C *una curva y* $\mathfrak{D}$ *un sistema lineal s.p.b. A los enteros* $v_{(m,0)}, \ldots, v_{(m,m-n)}$ *de la Proposición 2.3.4 se le llamamos ordenes* $(q_1, \ldots, q_m)$*-Frobenius de* $\mathfrak{D}$*. Al divisor*

$$S_m(\mathfrak{D}) = div\big(W_t(f)\big) + \Big(\sum_{i=0}^{n-m} v_{(m,i)}\Big) div(dt) + \Big(\sum_{i=1}^{m} q_i + n - m + 1\Big) E$$

lo llamamos divisor $(q_1, \ldots, q_m)$*-Frobenius de* $\mathfrak{D}$ *(Aquí se entiende que* t *es un parametro separante de* $\mathbb{F}_{q_0}(C)/\mathbb{F}_{q_0}$ *y* E *es el divisor de la Sección 1.2, Ecuación (2), pág. 19).*

Cuando se sobreentiende el sistema lineal $\mathfrak{D}$ y m denotaremos al divisor $(q_1, \ldots, q_m)$-Frobenius de $\mathfrak{D}$ por S_m y a $v_{(m,i)}$ por ν_i. Claramente, $gr(S_m) = \big(\sum_{i=0}^{n-m} \nu_i\big)(2g-2) + (\sum_{i=1}^{m} q_i + n - m + 1)d$, donde $d = gr(\mathfrak{D})$.

Ejemplo 2.3.7. Sea C la hermitiana $y^3 + y = x^4$, $\mathbb{F}_{q_0} = \mathbb{F}_{q_1} = \mathbb{F}_3$, $\mathbb{F}_{q_2} = \mathbb{F}_9$ y $f = (1 : x : y)$. Luego, $\nu_0 = 0$ por el Ejemplo 2.1.7 o la Proposición 2.3.4.

Definición 2.3.8 (Sistema lineal clásico y ordinario)**.** *Diremos que un sistema lineal* $\mathfrak{D}$ *definido sobre una curva* $C(\mathbb{F}_{q_0})$ *es* $(q_1, \ldots, q_m)$*-clásico (*$(q_1, \ldots, q_m)$*-ordinario) si la sucesión de ordenes* $(q_1, \ldots, q_m)$*-Frobenius es clásica (ordinaria). Es decir, si*

$$(\nu_0, \ldots, \nu_{n-m}) = (0, \ldots, n-m)\big((\nu_0, \ldots, \nu_{n-m}) = (\varepsilon_0, \ldots, \varepsilon_{n-m})\big).$$

Observación 2.3.9. *El divisor* $(q_1, \ldots, q_m)$*-Frobenius, depende unicamente del sistema lineal* $\mathfrak{D}$.

1) *Independencia de la representación del morfismo inducido.*

Sea $f = (f_0 : \ldots : f_n) : C \to \mathbb{P}^n(k)$ y $hf = (hf_0 : \ldots : hf_n)$ donde $h \in k(C)^*$. Sean E y E' los divisores asociados a los morfismos f y hf (Véase la ecuación (2), pág. 19). Luego,

por la Observación 1.2.3, pág. 19,

$$\begin{aligned} S_m(hf) &= \operatorname{div}\big(W_t(hf)\big) + \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(dt) + (\sum_{i=1}^{m} q_i + n - m + 1)E' \\ &= (\textstyle\sum_{i=1}^{m} q_i + n - m + 1)\operatorname{div}(h) + \operatorname{div}\big(W_t(f)\big) + \big(\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(dt) \\ &\quad +(\textstyle\sum_{i=1}^{m} q_i + n - m + 1)\big(E - \operatorname{div}(h)\big) \\ &= \operatorname{div}\big(W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(dt) + (\sum_{i=1}^{m} q_i + n - m + 1)E \\ &= S_m(\mathfrak{D}) \end{aligned}$$

2) *Independencia del morfismo inducido por* $\mathfrak{D}$.

Si f y $g = (g_0 : \cdots : g_n)$ son dos morfismos inducidos por el sistema lineal $\mathfrak{D}$, entonces $g_i = \sum_{j=0}^{n} a_{ij} f_j$ donde $(a_{ij}) \in GL_{n+1}(\mathbb{F}_{q_0})$. Así que

$$\begin{aligned} S_m(g) &= \operatorname{div}\big(W_t(g)\big) + \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(dt) + (\sum_{i=1}^{m} q_i + n - m + 1)E \\ &= \operatorname{div}\big(\det(a_{ij})W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(dt) + (\sum_{i=1}^{m} q_i + n - m + 1)E \\ &= S_m(\mathfrak{D}) \end{aligned}$$

3) *Independencia del parámetro separante.*

Sea u un parámetro separante de $\mathbb{F}_q(C)/\mathbb{F}_q$. Entonces, por la Proposición 2.3.1

$$\begin{aligned} S_m(u) &= \operatorname{div}\big(W_u(f)\big) + \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(du) + (\sum_{i=1}^{m} q_i + n - m + 1)E \\ &= \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}\Big(\frac{dt}{du}\Big) + \operatorname{div}\big(W_t(f)\big) + \big(\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(du) \\ &\quad +(\textstyle\sum_{i=1}^{m} q_i + n - m + 1)E \\ &= \operatorname{div}\big(W_t(f)\big) + \big(\textstyle\sum_{i=0}^{n-m}\nu_i\big)\operatorname{div}(dt) + (\sum_{i=1}^{m} q_i + n - m + 1)E \\ &= S_m(\mathfrak{D}). \end{aligned}$$

⊡

El divisor $(q_1, \ldots, q_m)$-Frobenius es también invariante bajo permutaciones de los q_i.

Observación 2.3.10. *Si* $\nu_i < q_1$ *y* $q_s = q_1^s$ *(*$q_{r+s} = q_r q_s$*), entonces* $\nu_0, \ldots, \nu_i$ *son los primeros* $i+1$ *ordenes* $(q_1, \ldots, q_{m-1})$*-Frobenius del morfismo* $g = (f_1 - f_1^{q_1} : \cdots : f_n - f_n^{q_1})$

El caso $m = 1$ debe entenderse como en la observación 2.1.10.

Podemos suponer que el morfismo f es $(1 : f_1 : \cdots : f_n)$ (dividiendo por $f_0 \in \mathbb{F}_{q_0}(C)^*$).

Luego,

$$
\begin{aligned}
W_t^{(w_0,\dots,w_{n-m})}(f) &= \det\begin{pmatrix}
1 & f_1^{q_1} & \cdots & f_n^{q_1}\\
1 & f_1^{q_2} & \cdots & f_n^{q_2}\\
\vdots & \vdots & \ddots & \vdots\\
1 & f_1^{q_m} & \cdots & f_n^{q_m}\\
1 & f_1 & \cdots & f_n\\
0 & D_t^{(w_1)}f_1 & \cdots & D_t^{(w_1)}f_n\\
\vdots & \vdots & \ddots & \vdots\\
0 & D_t^{(w_{n-m})}f_1 & \cdots & D_t^{(w_{n-m})}f_n
\end{pmatrix}\\
&= \det\begin{pmatrix}
1 & f_1^{q_1} & \cdots & f_n^{q_1}\\
0 & f_1^{q_2}-f_1^{q_1} & \cdots & f_n^{q_2}-f_n^{q_1}\\
\vdots & \vdots & \ddots & \vdots\\
0 & f_1^{q_m}-f_1^{q_{m-1}} & \cdots & f_n^{q_m}-f_n^{q_{m-1}}\\
0 & f_1-f_1^{q_1} & \cdots & f_n-f_n^{q_1}\\
0 & D_t^{(w_1)}f_1 & \cdots & D_t^{(w_1)}f_n\\
\vdots & \vdots & \ddots & \vdots\\
0 & D_t^{(w_{n-m})}f_1 & \cdots & D_t^{(w_{n-m})}f_n
\end{pmatrix}\\
&= \det\begin{pmatrix}
f_1^{q_2}-f_1^{q_1} & \cdots & f_n^{q_2}-f_n^{q_1}\\
\vdots & \ddots & \vdots\\
f_1^{q_m}-f_1^{q_{m-1}} & \cdots & f_n^{q_m}-f_n^{q_{m-1}}\\
f_1-f_1^{q_1} & \cdots & f_n-f_n^{q_1}\\
D_t^{(w_1)}f_1 & \cdots & D_t^{(w_1)}f_n\\
\vdots & \ddots & \vdots\\
D_t^{(w_{n-m})}f_1 & \cdots & D_t^{(w_{n-m})}f_n
\end{pmatrix}\\
&= (-1)^{m-1}\det\begin{pmatrix}
f_1^{q_1}-f_1^{q_2} & \cdots & f_n^{q_1}-f_n^{q_2}\\
\vdots & \ddots & \vdots\\
f_1^{q_{m-1}}-f_1^{q_m} & \cdots & f_n^{q_{m-1}}-f_n^{q_m}\\
f_1-f_1^{q_1} & \cdots & f_n-f_n^{q_1}\\
D_t^{(w_1)}f_1 & \cdots & D_t^{(w_1)}f_n\\
\vdots & \ddots & \vdots\\
D_t^{(w_{n-m})}f_1 & \cdots & D_t^{(w_{n-m})}f_n
\end{pmatrix}
\end{aligned}
$$

Ahora, si $w_i = \nu_i$ y $q_i = q_1^i$, entonces

$$(f_j^{q_{i-1}} - f_j^{q_i})^{q_1} = f_j^{q_{i-1}q_1} - f_j^{q_iq_1} = f_j^{q_i} - f_j^{q_{i+1}}.$$

De otro lado por la Observación 2.3.5, $\nu_0, \dots, \nu_i$ son los ordenes $(q_1, \dots, q_{m-1})$-Frobenius del morfismo $g = (f_1 - f_1^{q_1} : \cdots : f_n - f_n^{q_1})$. ⊡

La observación anterior también generaliza a la proposición 2.1.11.

Proposición 2.3.11. *Si $\nu_r < q_1$ es un orden $(q_1, \ldots, q_m)$-Frobenius de $\mathfrak{D}$ y $q_i = q_1^i$, entonces cada entero ν tal que $\binom{\nu_r}{\nu} \not\equiv 0 \pmod p$ (ν es p-adicamente más pequeño que ν_r), es también un orden de $(q_1, \ldots, q_m)$-Frobenius. En particular si $v_r < p$, entonces $(v_0, \ldots, v_r) = (0, \ldots, r)$.*

Para hacer una generalización de la proposición 2.1.12, necesitamos un lema:

Lema 2.3.12. *Sea $P \in C$, t un parametro P-uniformizante, $(a_{(r,s)})$ una matriz $(n-m+1) \times (n+1)$ sobre k ($r = 0, 1, \ldots, n-m$ y $s = 0, 1, \ldots, n$), $q_1, \ldots, q_m$ enteros positivos mayores que 1 ordenados de forma ascendente ($q_1 < q_2 < \cdots < q_m$), $j_0, j_1, \ldots, j_n$ enteros no negativos tales que $j_i < j_l$ si $i < l$ y $1 \leq m \leq n$. Si*

$$W_n = \det \begin{pmatrix} t^{j_0 q_1} & t^{j_1 q_1} & \cdots & t^{j_n q_1} \\ \vdots & \vdots & \ddots & \vdots \\ t^{j_0 q_m} & t^{j_1 q_m} & \cdots & t^{j_n q_m} \\ a_{(0,0)} t^{j_0} & a_{(0,1)} t^{j_1} & \cdots & a_{(0,n)} t^{j_n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(n-m,0)} t^{j_0} & a_{(n-m,1)} t^{j_1} & \cdots & a_{(n-m,n)} t^{j_n} \end{pmatrix}$$

entonces

$$W_n = c \det\left((a_{(r,m+s)})\right) t^{\sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-m} j_{i+m}} + t b_n$$

donde $\nu_P(b_n) \geq \sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-m} j_{i+m}$ y $c \in k$. Además, $\nu_P(W_n) \geq \sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-m} j_{i+m}$ y la igualdad se da, si y solo si, $\det\left((a_{(r,m+s)})\right) \not\equiv 0 \pmod p$ ($r = 0, \ldots, n-m$ y $s = 0, \ldots, n-m$).

Prueba.

Por inducción sobre n. Para $n = 1$ tenemos que $m = 1$ y

$$\begin{array}{rclrcl} W_1 & = & \det \begin{pmatrix} t^{j_0 q_1} & t^{j_1 q_1} \\ a_{(0,0)} t^{j_0} & a_{(0,1)} t^{j_1} \end{pmatrix} & & = & t^{j_0 + j_0 q_1} \det \begin{pmatrix} 1 & t^{(j_1 - j_0) q_1} \\ a_{(0,0)} & a_{(0,1)} t^{j_1 - j_0} \end{pmatrix} \\ & = & a_{(0,1)} t^{j_0 + j_0 q_1 + j_1 - j_0} + a_{(0,0)} t^{j_0 + j_0 q_1 + (j_1 - j_0) q_1} & & = & a_{(0,1)} t^{j_0 + j_0 q_1 + j_1 - j_0} + t b_1 \\ & = & a_{(0,1)} t^{j_0 q_1 + j_1} + a_{(0,0)} t^{j_0 + j_0 q_1 + (j_1 - j_0) q_1} & & = & a_{(0,1)} t^{\sum_{i=0}^{1-1} j_i q_{1-i} + \sum_{i=0}^{1-1} j_{i+1}} + t b_1 \end{array}$$

donde $\nu_P(b) \geq j_0 + j_0 q_1 + (j_1 - j_0) q_1 - 1 \geq j_0 q_1 + j_1$. Además, $\nu_P(W_1) \geq j_0 q_1 + j_1$ con igualdad, si y sólo si, $\det(a_{(0,1)}) = a_{(0,1)} = \det\left((a_{(r,1+s)})\right) \not\equiv 0 \pmod p$.

Supongamos que se tiene el resultado para $n-1$. Es decir,

$$W_{n-1} = c \det\left((a_{(r,m+s)})\right) t^{\sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-1-m} j_{i+m}} + t b_{n-1}$$

donde $\nu_P(b_{n-1}) \geq \sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-1-m} j_{i+m}$. Además, $\nu_P(W_{n-1}) \geq \sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-1-m} j_{i+m}$ y la igualdad se da si y solo si,

$\det\left((a_{(r,m+s)})\right) \not\equiv 0 \ (mod\ p)$ ($r = 0,\ldots,n-1-m$ y $s = 0,\ldots,n-1-m$. Ahora, analicemos el caso para n.

$$
\begin{aligned}
W_n &= \det\begin{pmatrix} t^{j_0q_1} & t^{j_1q_1} & \cdots & t^{j_nq_1} \\ \vdots & \vdots & \ddots & \vdots \\ t^{j_0q_m} & t^{j_1q_m} & \cdots & t^{j_nq_m} \\ a_{(0,0)}t^{j_0} & a_{(0,1)}t^{j_1} & \cdots & a_{(0,n)}t^{j_n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(n-m,0)}t^{j_0} & a_{(n-m,1)}t^{j_1} & \cdots & a_{(n-m,n)}t^{j_n} \end{pmatrix} \\
&= t^{(n-m+1)j_0+j_0\sum_{i=1}^m q_i}\det\begin{pmatrix} 1 & t^{(j_1-j_0)q_1} & \cdots & t^{(j_n-j_0)q_1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t^{(j_1-j_0)q_m} & \cdots & t^{(j_n-j_0)q_m} \\ a_{(0,0)} & a_{(0,1)}t^{j_1-j_0} & \cdots & a_{(0,n)}t^{j_n-j_0} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(n-m,0)} & a_{(n-m,1)}t^{j_1-j_0} & \cdots & a_{(n-m,n)}t^{j_n-j_0} \end{pmatrix} \\
&= ct^{(n-m+1)j_0+j_0\sum_{i=1}^m q_i}\det\begin{pmatrix} t^{(j_1-j_0)q_1} & \cdots & t^{(j_n-j_0)q_1} \\ \vdots & \ddots & \vdots \\ t^{(j_1-j_0)q_m} & \cdots & t^{(j_n-j_0)q_m} \\ a_{(0,1)}t^{j_1-j_0} & \cdots & a_{(0,n)}t^{j_n-j_0} \\ \vdots & \ddots & \vdots \\ a_{(n-m,1)}t^{j_1-j_0} & \cdots & a_{(n-m,n)}t^{j_n-j_0} \end{pmatrix} \\
&\quad + t^{(n-m+1)j_0+j_0\sum_{i=1}^m q_i}b
\end{aligned}
$$

donde $\nu_P(b) > \nu_P(\widetilde{W}_{n-1})$ pues b es suma de determinantes (obtenidos por cofactores) cuya valuación es mayor que la de

$$
\widetilde{W}_{n-1} = \begin{pmatrix} t^{(j_1-j_0)q_1} & \cdots & t^{(j_n-j_0)q_1} \\ \vdots & \ddots & \vdots \\ t^{(j_1-j_0)q_m} & \cdots & t^{(j_n-j_0)q_m} \\ a_{(0,1)}t^{j_1-j_0} & \cdots & a_{(0,n)}t^{j_n-j_0} \\ \vdots & \ddots & \vdots \\ a_{(n-m,1)}t^{j_1-j_0} & \cdots & a_{(n-m,n)}t^{j_n-j_0} \end{pmatrix}
$$

Luego,

$$
\begin{aligned}
&W_n = \\
&c\det\big((a_{(r,m+s)})\big)t^{(n-m+1)j_0+j_0\sum_{i=1}^{m}q_i+\sum_{i=0}^{m-1-1}(j_{i+1}-j_0)q_{m-1-i}+\sum_{i=0}^{n-1-(m-1)}j_{i+m-1+1}-j_0} \\
&+tb_n = \\
&c\det\big((a_{(r,m+s)})\big)t^{(n-m+1)j_0+j_0\sum_{i=1}^{m}q_i+\sum_{i=0}^{m-2}j_{i+1}q_{m-1-i}-j_0\sum_{i=0}^{m-2}q_{m-1-i}+\sum_{i=0}^{n-m}j_{i+m}-\sum_{i=0}^{n-m}j_0} \\
&+tb_n = \\
&c\det\big((a_{(r,m+s)})\big)t^{(n-m+1)j_0+j_0\sum_{i=1}^{m}q_i+\sum_{i=0}^{m-2}j_{i+1}q_{m-(i+1)}-j_0\sum_{i=1}^{m-1}q_i+\sum_{i=0}^{n-m}j_{i+m}-(n-m+1)j_0} \\
&+tb_n = c\det\big((a_{(r,m+s)})\big)t^{j_0\left(\sum_{i=1}^{m}q_i-\sum_{i=1}^{m-1}q_i\right)+\sum_{i=1}^{m-1}j_iq_{m-i}+\sum_{i=0}^{n-m}j_{i+m}}+tb_n = \\
&c\det\big((a_{(r,m+s)})\big)t^{\sum_{i=0}^{m-1}j_iq_{m-i}+\sum_{i=0}^{n-m}j_{i+m}}+tb_n
\end{aligned}
$$

donde $\nu_P(b_n) > \sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-m} j_{i+m}$ y, $\nu_P(W_n) \geq \sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-m} j_{i+m}$ con igualdad si y sólo si,

$$\det\big((a_{(r,m-1+1+s)})\big) = \det\big((a_{(r,m+s)})\big) \not\equiv 0 \ (mod\ p). \qquad \boxdot$$

Para generalizar la proposición 2.1.12 debemos tener en cuenta que el orden de las filas f^{q_i} del wronskiano generalizado influyen solamente en el signo del mismo y no alteran su valuación respecto a un punto P. El fin es estimar el número de puntos $\mathbb{F}_q$-racionales de la curva C. Por lo tanto,

Suponemos desde ahora en adelante que $\mathbb{F}_{q_r}$ es el cuerpo más pequeño entre los $\mathbb{F}_{q_i}$ que contiene a $\mathbb{F}_q$ y que $\mathbb{F}_{q_r} \subset \mathbb{F}_{q_s}$ para $s = r+1, \ldots, m$.

Proposición 2.3.13. *Sea P un punto de C con invariantes hermitianos $j_0, \ldots, j_n$ y $w_0, \ldots, w_{n-m}$ enteros no negativos. Entonces:*

a) $\nu_P\big(W_t^{(w_0,\ldots,w_{m-n})}(f)\big) \geq \sum_{i=0}^{n-m}(j_i - w_i)$ *con desigualdad si* $\det\left(\binom{j_r}{w_i}\right) \equiv 0 \pmod p$. *En particular,* $\nu_P\big(S_m(\mathfrak{D})\big) \geq \sum_{i=1}^{n-m}(j_i - \nu_i)$ *con desigualdad si,* $\det\left(\binom{j_r}{\nu_i}\right) \cong 0 \pmod p$ *($r = 0, \ldots, n-m$ e $i = 0, \ldots, n-m$).*

b) Si P es $\mathbb{F}_q$-racional, entonces

$$\nu_P\big(W_t^{(w_0,\ldots,w_{n-m})}(f))\big) \geq \sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-m}(j_{m-r+1+i} - w_i),$$

y la desigualdad se da si, $\det\left(\binom{j_{s+m-r+1}}{w_i}\right) \equiv 0 \pmod p$. *En particular,* $\nu_P(S_m) \geq \sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-m}(j_{m-r+1+i} - \nu_i)$. *Más aún, si $r = 1$ entonces la igualdad se dá si y sólo si,* $\det\left(\binom{j_{s+m}}{w_i}\right) \not\equiv 0 \pmod p$

c) El divisor $S_m(\mathfrak{D})$ es positivo (efectivo).

Prueba.

a) Aplicando una transformación proyectiva T inducida por $(a_{ij}) \in GL_{n+1}(k)$ podemos suponer que $e_P = 0$ y $g = (g_0 : \cdots : g_n) = T \circ f$ satisface que $g_i = \sum_{j=0}^{n} a_{ij} f_j = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$ y $c_i \in k^*$ (Véase los comentarios posteriores al teorema 1.3.6). Así que $\nu_P(g_i) \geq 0$ y $\nu_P(f_i) \geq 0$. Sea $l_{(s,i)} = \sum_{j=0}^{n} a_{ij} f_j^{q_s}$. Luego, $\nu_P(l_{(s,i)}) \geq 0$ y

$$\det \begin{pmatrix} l_{(1,0)} & \cdots & l_{(1,n)} \\ \vdots & \ddots & \vdots \\ l_{(m,0)} & \cdots & l_{(m,n)} \\ D_t^{(w_0)} g_0 & \cdots & D_t^{(w_0)} g_n \\ D_t^{(w_1)} g_0 & \cdots & D_t^{(w_1)} g_n \\ \vdots & \ddots & \vdots \\ D_t^{(w_{n-m})} g_0 & \cdots & D_t^{(w_{n-m})} g_n \end{pmatrix} = \det(a_{ij}) W_t^{(w_0,\ldots,w_{n-m})}(f).$$

Denotaremos a $D_t^{(w_s)} h_i$ por $h_{(s,i)}$. Obsérvese que $\nu_P(h_{(s,i)}) \geq j_i - w_s$.

Ahora, hagamos inducción sobre n. Si $n = 1$, entonces $m = 1$ y

$$\det \begin{pmatrix} l_{10} & l_{11} \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} + h_{(0,0)} & c_1 \binom{j_1}{w_0} t^{j_1 - w_0} + h_{(0,1)} \end{pmatrix} =$$
$$\det \begin{pmatrix} l_{10} & l_{11} \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} & c_1 \binom{j_1}{w_0} t^{j_1 - w_0} \end{pmatrix} + tb = c \binom{j_0}{w_0} t^{j_0 - w_0} + tb$$

donde $\nu_P(b) \geq j_0 - w_0$ (Observación 1.5.3), $\nu_P\big(W_t(f)\big) \geq \sum_{i=0}^{1-1} (j_i - w_i)$ y la desigualdad estricta se da, si $\binom{j_0}{w_0} = \det\left(\binom{j_0}{w_0}\right) \equiv 0 \pmod{p}$.

Supongamos que se tiene el resultado para $n - 1$. Es decir,

$$\begin{aligned} W_{n-1} &= \det \begin{pmatrix} l_{(1,0)} & \cdots & l_{(1,n-1)} \\ \vdots & \ddots & \vdots \\ l_{(m,0)} & \cdots & l_{(m,n-1)} \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} + h_{(0,0)} & \cdots & c_n \binom{j_{n-1}}{w_0} t^{j_{n-1} - w_0} + h_{(0,n)} \\ c_0 \binom{j_0}{w_1} t^{j_0 - w_1} + h_{(1,0)} & \cdots & c_n \binom{j_{n-1}}{w_1} t^{j_{n-1} - w_1} + h_{(1,n)} \\ \vdots & \ddots & \vdots \\ c_0 \binom{j_0}{w_{n-m}} t^{j_0 - w_{n-m}} + h_{(n-m,0)} & \cdots & c_n \binom{j_{n-1}}{w_{n-m}} t^{j_{n-1} - w_{n-m}} + h_{(n-m,n)} \end{pmatrix} \\ &= c \det\left(\binom{j_s}{w_i}\right) t^{\sum_{i=1}^{n-1-m} (j_i - w_i)} + tb. \end{aligned}$$

Sabemos que

$$
\begin{aligned}
W_n &= \det \begin{pmatrix}
l_{(1,0)} & \cdots & l_{(1,n)} \\
\vdots & \ddots & \vdots \\
l_{(m,0)} & \cdots & l_{(m,n)} \\
c_0\binom{j_0}{w_0}t^{j_0-w_0}+h_{(0,0)} & \cdots & c_n\binom{j_n}{w_0}t^{j_n-w_0}+h_{(0,n)} \\
c_0\binom{j_0}{w_1}t^{j_0-w_1}+h_{(1,0)} & \cdots & c_n\binom{j_n}{w_1}t^{j_n-w_1}+h_{(1,n)} \\
\vdots & \ddots & \vdots \\
c_0\binom{j_0}{w_{n-m}}t^{j_0-w_{n-m}}+h_{(n-m,0)} & \cdots & c_n\binom{j_n}{w_{n-m}}t^{j_n-w_{n-m}}+h_{(n-m,n)}
\end{pmatrix} \\
&= \sum_{s=0}^{n} l_{(1,s)}y_s + tb_n.
\end{aligned}
$$

donde $\nu_P(b_n) \geq \nu_P\left(\sum_{s=0}^{n} l_{(1,s)}y_s\right)$ y

$$
\begin{aligned}
y_s = & \\
& \det \begin{pmatrix}
l_{(1,0)} & \cdots & l_{(1,s-1)} & l_{(1,s+1)} & \cdots \\
\vdots & \ddots & \vdots & \vdots & \ddots \\
l_{(m,0)} & \cdots & l_{(m,s-1)} & l_{(m,s+1)} & \cdots \\
c_0\binom{j_0}{w_0}t^{j_0-w_0} & \cdots & c_{s-1}\binom{j_{s-1}}{w_0}t^{j_{s-1}-w_0} & c_{s+1}\binom{j_{s+1}}{w_0}t^{j_{s+1}-w_0} & \cdots \\
\vdots & \ddots & \vdots & \vdots & \ddots \\
c_0\binom{j_0}{w_{n-m}}t^{j_0-w_{n-m}} & \cdots & c_{s-1}\binom{j_{s-1}}{w_{n-m}}t^{j_{s-1}-w_0} & c_{s+1}\binom{j_{s+1}}{w_{n-m}}t^{j_{s+1}-w_{n-m}} & \cdots
\end{pmatrix} \\
& = c\det\left(\binom{j_u^{(s)}}{w_i}\right)t^{\sum_{i=1}^{s-1}(j_i-w_i)+\sum_{i=s+1}^{n-m}(j_i-w_i)} + tb_s.
\end{aligned}
$$

En el procedimiento anterior $0 \leq u, i \leq n-m$ y $j_u^{(s)} = \begin{cases} j_u & \text{si} \quad u < s \\ j_{u+1} & \text{si} \quad u \geq s \end{cases}$.

Luego, $\nu_P(y_s) \geq \sum_{i=1}^{s-1}(j_i - w_i) + \sum_{i=s+1}^{n-m}(j_i - w_i) \geq \sum_{i=1}^{n-m}(j_i - w_i)$. Así,

$$W_n = c\det\left(\binom{j_u}{w_i}\right)t^{\sum_{i=1}^{n-m}(j_i-w_i)} + tb.$$

con desigualdad si $\det(\binom{j_u}{w_i}) \equiv 0 \pmod{p}$ y $\nu_P(W_n) \geq \sum_{i=1}^{n-m}(j_i - w_i)$. Por lo tanto,

$$\nu_P\big(W_t^{(w_0,\ldots,w_{n-m})}(f)\big) \geq \sum_{i=1}^{n-m}(j_i - m_i)$$

con desigualdad si, $\det\left(\binom{j_u}{w_i}\right) \cong 0 \pmod{p}$.

b) La prueba de esta parte es parecida a la parte a), pero usando el Lema 2.3.12. Podemos suponer después de un cambio de coordenadas $T = (a_{ij}) \in GL_{n+1}(\mathbb{F}_q)$ que $e_P = 0$, $g = (g_0 : \cdots : g_n) = T \circ f$, $g_i = \sum_{j=0}^{n} a_{ij}f_j = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$ y

$c_i \in \mathbb{F}_q^*$. Así que $\nu_P(g_i) \geq 0$. Sea $l_{(s,i)} = \sum_{j=0}^{n} a_{ij} f_j^{q_s}$. Luego, $\nu_P(l_{(s,i)}) \geq 0$ y

$$\widetilde{W_n} = \det \begin{pmatrix} l_{(1,0)} & \cdots & l_{(1,n)} \\ \vdots & \ddots & \vdots \\ l_{(r-1,0)} & \cdots & l_{(r-1,n)} \\ c_0 t^{j_0 q_r} + h_0^{q_r} & \cdots & c_n t^{j_n q_r} + h_n^{q_r} \\ \vdots & \ddots & \vdots \\ c_0 t^{j_0 q_m} + h_0^{q_m} & \cdots & c_n t^{j_n q_r} + h_n^{q_m} \\ D_t^{(w_0)} g_0 & \cdots & D_t^{(w_0)} g_n \\ D_t^{(w_1)} g_0 & \cdots & D_t^{(w_1)} g_n \\ \vdots & \ddots & \vdots \\ D_t^{(w_{n-m})} g_0 & \cdots & D_t^{(w_{n-m})} g_n \end{pmatrix} = \det(a_{ij}) W_t^{(w_0,\ldots,w_{n-m})}(f).$$

Denotando a $D_t^{(w_s)} h_i$ por $h_{(s,i)}$ $(\nu_P(h_{(s,i)}) \geq j_i - w_s)$ entonces $\widetilde{W_n} = W_n + tb$ por la Observación 1.5.3, donde

$$W_n = \det \begin{pmatrix} l_{(1,0)} & \cdots & l_{(1,n)} \\ \vdots & \ddots & \vdots \\ l_{(r-1,0)} & \cdots & l_{(r-1,n)} \\ c_0 t^{j_0 q_r} & \cdots & c_n t^{j_n q_r} \\ \vdots & \ddots & \vdots \\ c_0 t^{j_0 q_m} & \cdots & c_n t^{j_n q_r} \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} & \cdots & c_n \binom{j_n}{w_0} t^{j_n - w_0} \\ \vdots & \ddots & \vdots \\ c_0 \binom{j_0}{w_{n-m}} t^{j_0 - w_{n-m}} & \cdots & c_n \binom{j_n}{w_{n-m}} t^{j_n - w_{n-m}} \end{pmatrix}$$

Ahora hagamos inducción sobre n. Si $n = 1$, entonces $m = r = 1$ y por el Lema 2.3.12,

$$\begin{aligned} W_1 &= \det \begin{pmatrix} c_0 t^{j_0 q_1} & c_n t^{j_1 q_1} \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} & c_1 \binom{j_1}{w_0} t^{j_1 - w_0} \end{pmatrix} \\ &= c \binom{j_0}{w_0} t^{j_0 q_1 + j_1 - w_0} + tb \\ &= c \binom{j_0}{w_0} t^{\sum_{i=0}^{0} j_i q_{m-i} + \sum_{i=0}^{0} (j_{i+1} - w_i)} + tb \end{aligned}$$

y $\nu_P(W_1) \geq j_0 q_1 + j_1 - w_0$.

Supongamos que se tiene el resultado para $n - 1$. Es decir,

$$W_{n-1} = c \det \left(\binom{j_{s+m-r+1}}{w_i} \right) t^{\sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-1-m} (j_{i+m-r+1} - w_i)} + tb_{n-1}.$$

Luego $W_n = \sum_{s=0}^{n} l_{(1,s)} y_s$ donde,

$$\begin{aligned} y_s &= \det \begin{pmatrix} l_{(1,0)} & \cdots & l_{(1,s-1)} & l_{(1,s+1)} & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \\ l_{(r-1,0)} & \cdots & l_{(r-1,s-1)} & l_{(r-1,s+1)} & \cdots \\ c_0 t^{j_0 q_r} & \cdots & c_{s-1} t^{j_{s-1} q_r} & c_{s+1} t^{j_{s+1} q_r} & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \\ c_0 t^{j_0 q_m} & \cdots & c_{s-1} t^{j_{s-1} q_m} & c_{s+1} t^{j_{s+1} q_m} & \cdots \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} & \cdots & c_{s-1} \binom{j_{s-1}}{w_0} t^{j_{s-1} - w_0} & c_{s+1} \binom{j_{s+1}}{w_0} t^{j_{s+1} - w_0} & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \\ c_0 \binom{j_0}{w_{n-m}} t^{j_0 - w_{n-m}} & \cdots & c_{s-1} \binom{j_{s-1}}{w_{n-m}} t^{j_{s-1} - w_0} & c_{s+1} \binom{j_{s+1}}{w_{n-m}} t^{j_{s+1} - w_{n-m}} & \cdots \end{pmatrix} \\ &= c \det \left(\binom{j^{(s)}_{u+m-r+1}}{w_i} \right) t^{\sum_{i=0}^{m-1-(r-1)} j_i^{(s)} F_{m-1-i} + \sum_{i=0}^{n-1-(m-1)} (j^{(s)}_{i+m-r+1} - w_i)} + t b_s. \\ &= c \det \left(\binom{j^{(s)}_{u+m-r+1}}{w_i} \right) t^{\sum_{i=0}^{m-r} j_i^{(s)} F_{m-1-i} + \sum_{i=0}^{n-m} (j^{(s)}_{i+m-r+1} - w_i)} + t b_s. \end{aligned}$$

donde $F_i = q_{i+1}$ y $j_u^{(s)} = \begin{cases} j_u & \text{si} \quad u < s \\ j_{u+1} & \text{si} \quad u \geq s \end{cases}$.

Así, $\nu_P(y_s) \geq \sum_{i=0}^{m-r} j_i^{(s)} F_{m-1-i} + \sum_{i=0}^{n-m} (j^{(s)}_{i+m-r+1} - w_i) \geq \sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-m} (j_{i+m-r+1} - w_i)$. Por lo tanto,

$$W_t^{(w_0,\ldots,w_{n-m})}(f) = c \det \left(\binom{j_{s+m-r+1}}{w_i} \right) t^{\sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-m} (j_{i+m-r+1} - w_i)} + tb.$$

con desigualdad si $\det \left(\binom{j_{s+m-r+1}}{w_i} \right) \equiv 0 \pmod{p}$. Obsérvese que el caso $r = 1$ se tiene por el Lema 2.3.12, pues en este caso

$$\begin{aligned} W_n &= \det \begin{pmatrix} c_0 t^{j_0 q_1} & \cdots & c_n t^{j_n q_1} \\ \vdots & \ddots & \vdots \\ c_0 t^{j_0 q_m} + h_0^{q_m} & \cdots & c_n t^{j_n q_r} \\ c_0 \binom{j_0}{w_0} t^{j_0 - w_0} & \cdots & c_n \binom{j_n}{w_0} t^{j_n - w_0} \\ \vdots & \ddots & \vdots \\ c_0 \binom{j_0}{w_{n-m}} t^{j_0 - w_{n-m}} & \cdots & c_n \binom{j_n}{w_{n-m}} t^{j_n - w_{n-m}} \end{pmatrix} \\ &= c \det \left(\binom{j_{s+m}}{w_i} \right) t^{\sum_{i=0}^{m-1} j_i q_{m-i} + \sum_{i=0}^{n-m} j_{i+m} - w_i} + t b_n \end{aligned}$$

con igualdad, si y solo si, $\det \left(\binom{j_{s+m}}{w_i} \right) \not\equiv 0 \pmod{p}$.

c) Sea $P \in C$. Podemos suponer que $f_i = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$ y $c_i \in k^*$ y $j_0, \ldots, j_n$ son los invariantes hermitianos de P. Así, $\nu_P(f_i) \geq 0$ y $\nu_P\big(D_t^{(m)} f_i\big) \geq 0$ para todo m.

Luego, $\nu_P\big(S_m(\mathfrak{D})\big) = \nu_P\big(W_t^{(w_0,\ldots,w_{n-m})}(f)\big) \geq 0$. ⊡

Proposición 2.3.14. *Sea P un punto $\mathbb{F}_q$-racional de C con $(\mathfrak{D}, P)$-ordenes $j_0, \ldots, j_n$ y $\nu_0, \ldots, \nu_{n-m}$ los ordenes $(q_1, \ldots, q_m)$-Frobenius de $\mathfrak{D}$. Si la sucesión de enteros $(w_0, \ldots, w_{n-(m-r+1)})$ son tales que $0 \leq w_0 < \cdots < w_{n-m+r-1}$ y $\det\left(\binom{j_{s+m-r+1}-j_{m-r+1}}{w_i}\right) \not\equiv 0$ (mód p) para $i, s = 0, \ldots, n-m+r-1$, entonces $\nu_i \leq w_{i+r-1}$.*

Prueba.

La mejor escogencia de los w_i son los ordenes del morfismo $g : \mathbb{P}^1(k) \to \mathbb{P}^{n-m+r-1}(k)$ dado por $g(1 : x) = (1 : x^{j_{m-r+2}-j_{m-r+1}} : \cdots : x^{j_n - j_{m-r+1}})$, pues g es equivalente a $(g_{m-r+1} : \cdots : g_n) = (x^{j_{m-r+1}} : x^{j_{m-r+2}} : \cdots : x^{j_n})$. Luego,

$$\det(D_x^{w_i} g_s) = \det\left(\binom{j_{s+m-r+1}}{w_i}\right) x^{\sum_{s=0}^{n-m+r-1}(j_{s+m-r+1}-w_s)}$$

y $\det\left(\binom{j_{s+m-r+1}}{w_i}\right) \not\equiv 0 \ (mod\ p)$.

De manera que podemos suponer que los w_i son los ordenes de g. Además, $\det\left(\binom{j_{s+m-r+1}-j_{m-r+1}}{w_i}\right) \neq 0 \iff det\left(\binom{j_{s+m-r+1}}{w_i}\right) \neq 0$. Luego, con un proceso análogo al de la Proposición 2.3.13 b), podemos asumir que $f_i = c_i t^{j_i} + h_i(t)$; donde $\nu_P(h_i) > j_i$, $c_i \in k^*$ y $W_t^{(w_0,\ldots,w_{n-m+r-1})}(f) = c \det\left(\binom{j_{s+m-r+1}}{w_i}\right) t^{\sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-m+r-1}(j_{i+m-r+1}-w_i)} + tb \neq 0$; donde $\nu_P(b) \geq \sum_{i=0}^{m-r} j_i q_{m-i} + \sum_{i=0}^{n-m+r-1}(j_{i+m-r+1} - w_i)$ y $c \in \mathbb{F}_q^*$. Luego, los ordenes $(q_r, \ldots, q_m)$-Frobenius de $\mathfrak{D}$, $v_{(m-r+1,i)} \leq w_i$ por la Observación 2.3.5. De otro lado los ordenes $(q_1, \ldots, q_m)$-Frobenius $\nu_1, \ldots, \nu_{n-m}$ son un subconjunto del conjunto de ordenes $(q_r, \ldots, q_m)$-Frobenius. Luego, $\nu_i \leq w_{i+r-1}$ pues la igualdad se da eventualmente, en el peor de los casos. ⊡

Una consecuencia inmediata de la Proposición anterior es que $w_i \leq j_{i+m-r+1} - j_{m-r+1}$. Así que estudiar el caso en que

$$\nu_i \leq j_{i+m-r+1} - j_{m-r+1} \tag{7}$$

es un asunto de suma importancia y que no podemos tratar en este trabajo. Esto sucede en el análisis hecho aquí en el caso $r = 1$.

Como consecuencia inmediata de las proposiciones 2.3.13 y 2.3.14 se tienen los siguientes resultados:

Corolario 2.3.15. *Sea $P \in C$ es un punto $\mathbb{F}_q$-racional, $j_0, \ldots, j_n$ sus correspondientes $(\mathfrak{D}, P)$-ordenes y $\nu_1, \ldots, \nu_{n-m}$ los ordenes $(q_1, \ldots, q_m)$-Frobenius del sistema lineal $\mathfrak{D}$. Entonces $\nu_i \leq j_{i+m} - j_{m-r+1}$ y $\nu_P\big(W_t^{(\nu_0,\ldots,\nu_{n-m})}(f)\big) \geq \sum_{i=0}^{m-r} j_i q_{m-i} + (n-m+1)j_{m-r+1} - \sum_{i=0}^{n-m}(j_{i+m} - j_{i+m-r+1})$. Además, si los ν_i satisfacen la condición de la ecuación (7), entonces*

$$\begin{aligned} \nu_P\big(W_t^{(\nu_0,\ldots,\nu_{n-m})}(f)\big) &\geq \sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\varepsilon_{m-r+1} \\ &\geq \sum_{i=0}^{m-r} i q_{m-i} + (n-m+1)(m-r+1) \end{aligned}$$

donde $\varepsilon_1, \ldots, \varepsilon_n$ son los $\mathfrak{D}$-ordenes.

El caso $w_i = i$ o $w_i = \varepsilon_i$ donde $\varepsilon_1, \ldots, \varepsilon_n$ son los ordenes de $\mathfrak{D}$ y $r = 1$ ($\mathbb{F}_q \subset \mathbb{F}_{q_1}$) en la proposición 2.3.14, nos produce el siguiente resultado:

Corolario 2.3.16. *Si $\prod_{s>i\geq m}^{n} \frac{j_s - j_i}{s-i}$ no es divisible por p $\left(\det\left(\binom{j_s}{\varepsilon_i}\right) \not\equiv 0 \pmod{p}\right)$, entonces $\nu_i = i$ ($\nu_i = \varepsilon_i$) y $\nu_P(S_m) = \sum_{i=0}^{m-1} j_i q_{m-i} + n - m + 1 + \sum_{i=0}^{n-m+1}(j_{i+m-1} - i)$ $\left(\nu_P(S) = \sum_{i=0}^{m-1} j_i q_{m-i} + \varepsilon_{n-m+1} + \sum_{i=0}^{n-m+1}(j_{i+m-1} - \varepsilon_i)\right)$.*

Este corolario se obtiene de forma inmediata por el Corolario 1.5.10.

En las mismas condiciones anteriores se tiene el siguiente corolario:

Corolario 2.3.17. *Si la sucesión de ordenes $(q_1, \ldots, q_m)$-Frobenius $(\nu_0, \ldots, \nu_{n-m})$ de difiere de $(0, 1, \ldots, n-m)$, entonces cada punto $\mathbb{F}_q$-racional es de osculación de $\mathfrak{D}$.*

Prueba.

Argumentemos por contradicción suponiendo que existe un punto racional clásico (ordinario). Luego, por (7) $\nu_i \leq i + m - m = i$ y por la Proposición 2.3.4 $v_i = i$. ⊡

Para generalizar el método Stöhr–Voloch se requiere que $\sum_{i=0}^{m-r} j_i q_{m-i} + (n-m+1)j_{m-r+1} - \sum_{i=0}^{n-m}(j_{i+m} - j_{i+m-r+1}) \geq \sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\varepsilon_{m-r+1} - \sum_{i=0}^{n-m}(j_{i+m} - j_{i+m-r+1}) > 0$ (esto se presenta si se tiene la condición de la Ecuación (7)) y que además la desigualdad no dependa de los invariantes hermitianos j_s (estos dependen del punto P considerado). Con este fin en mente, usaremos otros invariantes. Claramente $j_i + (n-i) \leq j_n \leq d$ donde $d = gr(\mathfrak{D})$ (Véase la Sección 1.2). Luego, $j_i \leq d + i - n$ y

$$\begin{aligned}
\nu_P(S_m) &\geq \sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\varepsilon_{m-r+1} - \sum_{i=0}^{n-m}(d + i + m - n - \varepsilon_{i+m-r+1}) \\
&\geq \sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\varepsilon_{m-r+1} \\
&\geq -(n-m+1)(d+m-n) - (n-m+1)\tfrac{n-m}{2} + \sum_{i=0}^{n-m} \varepsilon_{i+m-r+1}) \\
&\geq \sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\Big(\varepsilon_{m-r+1} + n - m - d - \tfrac{n-m}{2} \\
&\geq +\tfrac{1}{n-m+1}\sum_{i=0}^{n-m} \varepsilon_{i+m-r+1}\Big) \\
&\geq \sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\left(\varepsilon_{m-r+1} + \tfrac{1}{n-m+1}\sum_{i=0}^{n-m} \varepsilon_{i+m-r+1} + \tfrac{n-m}{2} - d\right)
\end{aligned}$$

Luego, si $\sum_{i=0}^{m-r} \varepsilon_i q_{m-i} + (n-m+1)\left(\varepsilon_{m-r+1} + \frac{1}{n-m+1}\sum_{i=0}^{n-m} \varepsilon_{i+m-r+1} + \frac{n-m}{2} - d\right) > 0$ entonces se podrá generalizar el Teorema 2.2.2. Obsérvese que se tendría una condición análoga a la de la segunda parte del Corolario 2.3.15 si

$$\varepsilon_{m-r+1} + \frac{1}{n-m+1}\sum_{i=0}^{n-m} \varepsilon_{i+m-r+1} + \frac{n-m}{2} - d > 0. \tag{8}$$

y consecuentemente, si

$$\begin{aligned} 0 &< m-r+1+\tfrac{1}{n-m+1}\textstyle\sum_{i=0}^{n-m}(i+m-r+1)+\tfrac{n-m}{2}-d \\ &< m-r+1+\tfrac{n-m}{2}+m-r+1+\tfrac{n-m}{2}-d \\ &< m-2r+2-(d-n) \end{aligned}$$

En conclusión, la condición $\sum_{i=0}^{m-r}\varepsilon_i q_{m-i}+(n-m+1)\varepsilon_{m-r+1}-\sum_{i=0}^{n-m}(j_{i+m}-j_{i+m-r+1})>0$ se satisface cuando $r<\frac{m-(d-n)+2}{2}$ ó $1\leq r<\frac{m-g+2}{2}$ donde g es el género de la curva C. En la afirmación anterior hemos usado el Teorema de Riemann-Roch y esta nos dice que se puede tener la condición siempre que $m>g$.

Teorema 2.3.18. *Sea C una curva algebraica proyectiva, no singular, de género g, definida sobre $\mathbb{F}_{q_0}$ de característica p contenido en el cuerpo $\subset \mathbb{F}_q$, N el número de puntos $\mathbb{F}_q$-racionales, $\mathbb{F}_{q_1},\mathbb{F}_{q_2},\ldots,\mathbb{F}_{q_n}$ cuerpos de extensión de $\mathbb{F}_{q_0}$ tales que $\mathbb{F}_{q_1}\subset\mathbb{F}_{q_i}$, $q_1^{n+1}\geq \max\{q_i\}$ y $\mathbb{F}_q$ contenido en $\mathbb{F}_{q_r}$ donde $\mathbb{F}_{q_r}$ es el cuerpo $\mathbb{F}_{q_i}$ más pequeño que lo contiene. Si existe un sistema lineal sin puntos básicos definido sobre $\mathbb{F}_{q_0}$ de grado d, dimensión n, con ordenes de $(q_1,\ldots,q_m)$-Frobenius $\nu_0,\ldots,\nu_{n-m}$ y,*

$$\sum_{i=0}^{m-r}\varepsilon_i q_{m-i}+(n-m+1)\left(\varepsilon_{m-r+1}+\frac{1}{n-m+1}\sum_{i=0}^{n-m}\varepsilon_{i+m-r+1}+\frac{n-m}{2}-d\right)>0$$

entonces

$$N\leq\frac{\left(\sum_{i=0}^{n-m}\nu_i\right)(2g-2)+(\sum_{i=1}^{m}q_i+n-m+1)d}{\sum_{i=0}^{m-r}\varepsilon_i q_{m-i}+(n-m+1)\left(\varepsilon_{m-r+1}+\frac{1}{n-m+1}\sum_{i=0}^{n-m}\varepsilon_{i+m-r+1}+\frac{n-m}{2}-d\right)}.$$

Más aún, si $r=1$, entonces

$$N\leq\frac{\left(\sum_{i=0}^{n-m}\nu_i\right)(2g-2)+(\sum_{i=1}^{m}q_i+n-m+1)d}{\sum_{i=0}^{m-1}\varepsilon_i q_{m-i}+(n-m+1)\varepsilon_{m-r+1}}.$$

Prueba.

Claramente $N\leq\frac{gr(S_m)}{\sum_{i=0}^{m-r}\varepsilon_i q_{m-i}+(n-m+1)\left(\varepsilon_{m-r+1}+\frac{1}{n-m+1}\sum_{i=0}^{n-m}\varepsilon_{i+m-r+1}+\frac{n-m}{2}-d\right)}$ y

$$N\leq\frac{\left(\sum_{i=0}^{n-m}\nu_i\right)(2g-2)+(\sum_{i=1}^{m}q_i+n-m+1)d}{\sum_{i=0}^{m-r}\varepsilon_i q_{m-i}+(n-m+1)\left(\varepsilon_{m-r+1}+\frac{1}{n-m+1}\sum_{i=0}^{n-m}\varepsilon_{i+m-r+1}+\frac{n-m}{2}-d\right)}. \qquad \square$$

El caso $r=1$ del teorema no requiere la condición

$$\sum_{i=0}^{m-r}\varepsilon_i q_{m-i}+(n-m+1)\left(\varepsilon_{m-r+1}+\frac{1}{n-m+1}\sum_{i=0}^{n-m}\varepsilon_{i+m-r+1}+\frac{n-m}{2}-d\right)>0.$$

Obsérvese que se pueden tener Teoremas análogos suponiendo las condiciones de las ecuaciones (7) y (8).

La generalización anterior fue desarrollada porque el Teorema de Stöhr–Voloch da estimativos mejores que la cota de Hasse–Weil cuando la sucesión de ordenes de Frobenius es clásica. Ahora cuando esta no es clásica entonces apareceran ordenes de Frobenius mayores que p^s (la característica del cuerpo) por la Proposición 2.1.11 ó Proposición 2.3.11. En tal caso se debe pensar en introducir una fila f^{q_i} en el wronskiano generalizado, con $p^s \geq q_i$ y tal que el orden de Frobenius que se elimine sea $\geq p^s$. Este proceso permite pensar en la obtención de cotas mejores que la del Teorema 2.2.2. Sin embargo este tipo de análisis esta fuera de nuestro alcance en esta tesis.

Sin embargo, en el caso de cuerpos primos p la generalización también podría generar cotas mejores aún si la sucesión de ordenes de Frobenius de la curva fuera clásica. Obsérvese que en tal caso con $m = 2$, $q_0 = p = q_1$ y $q_2 = p^2$ ($m = 2$ y $r = 1$) la cota del Teorema 2.3.18 es

$$N \leq \frac{(n-2)(n-1)(g-1) + (p + p^2 + n - 1)d}{p + 2(n-1)}.$$

Ahora, por ejemplo si $g = 4$, $n = 3$, $d = 5$ y $p = 5$ entonces la cota del Teorema 2.2.2 es 19, la Cota de Hasse–Weil es 23 y la Cota del Teorema 2.3.18 es 18.

3. LA HIPOTESIS DE RIEMANN

La hipótesis de Riemann clásica (sobre $\mathbb{C}$) afirma que los ceros no triviales de la función zeta

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

viven en la linea $Re(s) = \frac{1}{2}$. Esta conjetura no se ha resuelto todavia. Ella está intimamente ligada a la distribución de los números primos, pues Euler vió que

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}$$

cuando $Re(s) > 1$ y de allí su importancia (p recorre los números primos). Sin embargo, en el estudio de las curvas algebraicas tenemos un resultado análogo. Sea C una curva no singular, algebraica definida sobre un cuerpo de Galois $\mathbb{F}_q$ y $\mathcal{D}_C$ el grupo de divisores $D = \sum a_i P_i$ tales que $F_q(D) = D$ donde F_q es el morfismo de Frobenius de C y $P_i \in C$. Decimos que un divisor P es primo si no se puede expresar como suma de dos divisores positivos. Definimos la norma de un divisor D como $\mathcal{N}(D) := q^{gr(D)}$. La función zeta de Riemann de la curva C es

$$\zeta_C(s) = \sum_{D>0} \mathcal{N}(D)^{-s}$$

y esta satisface el producto de Euler

$$\zeta(s) = \prod_{P} (1 - \mathcal{N}(P)^{-s})^{-1}$$

donde P recorre los divisores primos de $\mathcal{D}_C$. La hipótesis de Riemann sobre cuerpos finitos o el teorema de Hasse–Weil afirma que si $\zeta(s) = 0$, entonces $Re(s) = \frac{1}{2}$. Debido a cuestiones geométricas es conveniente hacer la sustitución $t = q^{-s}$ en la función zeta de Riemann de C, para obtener la función zeta de C

$$Z_C(t) = \sum_{D>0} t^{gr(D)} \in \mathbb{C}[[t]]$$

y el L-polinomio de C sobre $\mathbb{F}_q$, $L_C(t) = (1-t)(1-qt)Z_C(t)$.

No podemos hacer un despliegue de los resultados del enfoque aritmético en este trabajo. Sin embargo el lector puede consultar a H. Stichtenoth [16], Cap. V para una introducción aritmética y a E. Bombieri [3] o P. Sarnak [12] para conocer los últimos avances en la materia. Solo nos resta decir que el número de puntos $\mathbb{F}_q$-racionales N_q, está intitamente relacionado a la función analítica Z_C y que $N_q = q + 1 - \sum_{i=1}^{2g} \alpha_i$ (Stichtenoth [16], Coro V.1.16) donde α_i son los reciprocos de las raices del L-polinomio y g es el género de C.

Obsérvese que el teorema de Hasse–Weil nos dice entonces que $|\alpha_i| = q^{\frac{1}{2}}$, lo que implica que

$$N_q \leq q + 1 + 2gq^{\frac{1}{2}} \text{ (Cota de Weil)}$$

El recíproco también es cierto, aún cuando la cota de Weil se tiene para alguna extensión de $\mathbb{F}_q$ (Véase Stichtenoth [16], Lema V.2.4 y Lema V.2.5).

El objetivo principal de este capítulo es obtener la cota de Weil usando el método Stöhr–Voloch. Luego se obtendran cotas para N_q mejores que la de Weil para algunos casos especificos; poniendo en escena un método general para obtener tales cotas. La importancia de las cotas radica en que en algunos casos no es posible entonces construir curvas con un número prescrito de puntos racionales. Esto tiene aplicaciones a la teoría de Códigos pues ciertos parámetros de los códigos dependen fuertemente del número de puntos racionales de la curva.

3.1. La cota de Hasse–Weil

Sea C una curva no singular, algebraica, proyectiva de género g definida sobre $\mathbb{F}_q$ y $\mathfrak{D}$ un sistema lineal completo sin puntos básicos de dimensión n y grado d. Para probar la hipótesis de Riemann tenemos que hacer y recordar algunas observaciones pertinentes. Para esto vamos a suponer que existe un punto $\mathbb{F}_q$-racional $P \in C$ con invariantes hermitianos $j_0, \ldots, j_n$ y que $v_0, \ldots, v_{n-1}$ son los ordenes $\mathbb{F}_q$-Frobenius de $\mathfrak{D}$.

Observación 3.1.1. *Si $i < d - 2g + 1$ entonces $j_i = i$.*

Nótese que $d - i > d - (i + 1) > 2g - 2$. Luego,

$$\dim\left(\mathfrak{D}_i\right) = d - i - g > d - (i + 1) - g = \dim\left(\mathfrak{D}_{i+1}\right)$$

donde $\mathfrak{D}_i := \{D \in \mathfrak{D} : D \geq iP\} \supset \mathfrak{D}_{i+1}$. De manera que $j_i \leq i$ e $i = j_i$ (Mirar la Proposición 1.2.11 y la Observación 1.2.13).

Observación 3.1.2. *Si $P \in C(\mathbb{F}_q)$, entonces $v_i \leq i + d - n$. Además, $v_i = i$ para todo $i < d - 2g$.*

Por definición $j_n \leq d$, $j_i + n - i \leq j_n \leq d$ y $j_i \leq i + d - n$. Luego, por el Corolario 2.1.14 $v_i \leq j_{i+1} - j_1 \leq i + 1 - d - n - j_1 \leq i + d - n$. Ahora, si $i < d - 2g$ entonces $v_i \leq i + 1 - 1 = i$ y $v_i = i$.

Ahora nos disponemos a probar la hipótesis de Riemann.

Teorema 3.1.3 (Cota de Hasse–Weil)**.** *Sea C una curva proyectiva, no singular, algebraica de género g definida sobre $\mathbb{F}_q$ y N el número de puntos racionales. Entonces,*

$$N \leq q + 1 + 2gq^{\frac{1}{2}}.$$

Prueba.

Sin perdida de generalidad podemos suponer que C tiene un punto racional P. Sea $\mathfrak{D} = |dP|$ donde $d \geq 2g$ y $q^{\frac{1}{2}} = n = d - g > 2g^2(g-1)$ (Aquí se ha usado el Teorema de Riemann–Roch y/o las Observaciónes 1.2.13 y 3.1.1). Este sistema lineal es sin puntos básicos, pues las lagunas de Weierstrass están en el intervalo $[1, 2g-1]$ (Véase Stichtenoth [16], Prop I.6.5 pág. 31). Luego, $q > 4g^4(g-1)^2$, $v_i = i$ si $i < n-g$ y $v_i \leq i+g$ cuando $n-g \leq i \leq n-1$ por la Observación 3.1.2. Así, por el Teorema 2.2.2

$$\begin{aligned}
N &\leq \frac{2\left(\sum_{i=0}^{n-g-1} i + \sum_{i=n-g}^{n-1}(i+g)\right)(g-1)+(q+n)(n+g)}{n} \\
&\leq \frac{2\left(\frac{(n-g-1)(n-g)}{2} + gn - \frac{g(g+1)}{2} + g^2\right)(g-1)}{n} + \frac{(q+n)(n+g)}{n} \\
&\leq \frac{2\left(n(n-1) - 2gn + g^2 + g + 2gn - g^2 - g + 2g^2\right)(g-1)}{n} + q + n + g\left(1 + \frac{q}{n}\right) \\
&\leq (n-1)g - n + 1 + q + n + g\left(1 + \frac{q}{n}\right) + \frac{2g^2(g-1)}{n} \\
&\leq q + 1 + g\left(n + \frac{q}{n}\right) + \frac{2g^2(g-1)}{n} \\
&< q + 1 + 2gq^{\frac{1}{2}} + 1
\end{aligned}$$

y por lo tanto,

$$N \leq q + 1 + 2gq^{\frac{1}{2}}. \quad \boxdot$$

3.2. Métodos para obtener mejores cotas

Si el sistema lineal $\mathfrak{D}$ es completo y sus ordenes de Frobenius forman la sucesión clásica, entonces $d \leq n + g$ (Teorema de Riemann–Roch) y por la ecuación (6) $N \leq (n-1)(g-1) + \frac{(q+n)(n+g)}{n} = (n-1)g - n + 1 + q + n + \left(1 + \frac{q}{n}\right)g$. Luego,

$$N \leq q + 1 + \left(n + \frac{q}{n}\right) g. \tag{9}$$

Ahora, si $n = q^{\frac{1}{2}}$, entonces se tiene exactamente la hipótesis de Riemann. De manera que hay muchas formas de mejorar la cota de Hasse–Weil. Si $\mathfrak{D}$ es *especial* con índice de especialidad $i(\mathfrak{D}) = \delta = n + g - d$, entonces

$$N \leq q + 1 + \left(n + \frac{q}{n}\right) g - \left(1 + \frac{q}{n}\right) \delta. \tag{10}$$

Analogamente, de acuerdo a la demostración de la proposición 2.2.1 por cada punto Q no racional tal que $W_t f(Q) = 0$ $\left(Q \in Sopp\big(S(\mathfrak{D})\big)\right)$ se puede restar a (9) el término $\frac{\nu_Q(S)}{n}$. Además, si P es $\mathbb{F}_q$-racional y $\nu_P(S) > nj_1(P)$ entonces podemos sustraer también a $\frac{\nu_p(S) - nj_1}{n}$ ó

$$\frac{\nu_p(S) - n\varepsilon_1}{n} = \frac{\nu_p(S) - n}{n}. \tag{11}$$

Analicemos el caso $\mathfrak{D} = |dP|$ donde $d = gr(\mathfrak{D}) =\geq 2g$ (para que d no sea laguna de Weierstrass y $\mathfrak{D}$ no tenga puntos básicos) y $P \in C$ un punto $\mathbb{F}_q$-racional. Luego, $n = \dim(\mathfrak{D}) = d - g$. Un entero j es un $(\mathfrak{D}, P)$-orden si y sólo si, existe $f \in k(C)$ tal que $\mathrm{div}(f) + dP \geq 0$ y $j = \nu_P(f) + d$, si y sólo si, $d - j$ no es laguna de Weierstrass en P. Sean $\alpha_1, \alpha_2, \ldots, \alpha_g$ las lagunas en P. Luego, un $(\mathfrak{D}, P)$-orden j es distinto de $d - \alpha_i$ y el conjunto de $(\mathfrak{D}, P)$-ordenes es $\{0, 1, \ldots, d\} - \{d-\alpha_1, \ldots, d-\alpha_g\}$. Ahora, si $\mathfrak{D}$ es $\mathbb{F}_q$-clásico $\big((v_0, \ldots, v_{n-1}) = (0, \ldots, n-1)\big)$, entonces por la Proposición 2.1.12,

$$\nu_p(S) \geq \sum_{i=1}^{n} \big[j_i - (i-1)\big] = n + \sum_{i=1}^{n} j_i - \sum_{i=1}^{n} i = n + \sum_{i=1}^{d} i - n - \sum_{i=1}^{g}(d - \alpha_i) - \sum_{i=1}^{n} i.$$

Así,

$$\begin{array}{rcl} \nu_p(S) & \geq & n + \frac{d^2}{2} + \frac{d}{2} - gd + \sum_{i=1}^{g}(\alpha_i - i) + \sum_{i=1}^{g} i - \sum_{i=1}^{n} i \\ & \geq & n + \frac{(n+g)^2}{2} + \frac{n+g}{2} - g(n+g) + \sum_{i=1}^{g}(\alpha_i - i) + \frac{g^2}{2} + \frac{g}{2} - \frac{n^2}{2} - \frac{n}{2} \\ & \geq & n + \frac{n^2}{2} + gn + \frac{g^2}{2} + \frac{n}{2} + \frac{g}{2} - gn - g^2 + \frac{g^2}{2} + \frac{g}{2} - \frac{n^2}{2} - \frac{n}{2} + \sum_{i=1}^{g}(\alpha_i - i) \\ & \geq & n + g + \sum_{i=1}^{g}(\alpha_i - i). \end{array}$$

Luego,

$$\nu_p(S) - n \geq g + \sum_{i=1}^{g}(\alpha_i - i). \tag{12}$$

También, $N \leq q + 1 + \frac{1}{n}(n^2 + q)g - \frac{1}{n}\left(g + \sum_{i=1}^{g}(\alpha_i - i)\right)$ y.

$$N \leq q + 1 + ng - \frac{1}{n}\left(gq - g - \sum_{i=1}^{g}(\alpha_i - i)\right) \tag{13}$$

Supongamos ahora que $\mathfrak{D} = |W + sP|$ donde W es un divisor canónico definido sobre $C(\mathbb{F}_q)$, $s \geq 2$ y P un punto racional. Luego, $d = 2g - 2 + s \geq 2g$ y $n = d - g$. Un entero j es un $(\mathfrak{D}, P)$-orden si y sólo si, $\mathfrak{D}_j = \{D \in \mathfrak{D} : D - jP \geq 0\} \supset \mathfrak{D}_{j+1}$ (Proposición 1.2.11) si y sólo si, $L(W + sP - jP) = L\big(W - (j-s)P\big) \supset L\big(W - (j+1-s)P\big) \iff L\big((j-s)P\big) \supset L\big((j+1-s)P\big)$ (Lema 1.2.8) $\iff$ $j - s + 1$ es una laguna de Weierstrass ó $j - s + 1 < 0$ (Teorema de Riemann–Roch). Así, $\{0, \ldots, s-2, \alpha_1 + s - 1, \ldots, \alpha_g + s - 1\}$ es el conjunto de $(\mathfrak{D}, P)$-ordenes si $\alpha_1, \ldots, \alpha_g$ son las lagunas de Weierstrass. Ahora, si $(v_0, \ldots, v_{n-1}) = (0, \ldots, n-1)$, entonces $j_{i+s-2} = \alpha_i + s - 1$ $(1 \leq i \leq g)$. De manera que

$$\begin{array}{rcll} \nu_p(S) & \geq & \sum_{i=1}^{n}\big[j_i - (i-1)\big] & = \; n + \sum_{i=1}^{n}(j_i - i) \\ & \geq & n + \sum_{i=1}^{n}(j_i - i) & = \; n + \sum_{i=1}^{g}\big[\alpha_i + s - 1 - (i+s-2)\big] \\ & \geq & n + \sum_{i=1}^{g}(\alpha_i - i + 1) & = \; n + g + \sum_{i=1}^{g}(\alpha_i - i). \end{array}$$

y llegamos de nuevo a la ecuación (12) y se obtiene de nuevo (13). Aplicando estas cotas a curvas hiperelipticas se pueden obtener las cotas de Stark [15] y se pueden refinar los

Corolarios 2.2.4 y 2.2.5 para los sistemas lineales de la forma anterior, siempre y cuando se conozcan los invariantes hermitianos de algunos puntos racionales.

Ahora aplicaremos el Teorema 2.2.2, para obtener cotas mejores que la de Hasse–Weil en algunos casos muy particulares.

Proposición 3.2.1. *Sea C una curva proyectiva, no singular, algebraica de género g definida sobre el cuerpo finito $\mathbb{F}_q$ de característica p y N el número de puntos racionales. Si $p \geq g \geq 3$ y la sucesión de lagunas de Weierstrass es clásica para algún punto $P \in C$, entonces*

$$N \leq 2q + g(g-1).$$

Prueba.

Sea $\mathfrak{D}$ el sistema lineal canónico. Como $g \neq 0$ y dado un punto $Q \in C$ distinto de P $(2g-2)Q \in \mathfrak{D}$ entonces $\mathfrak{D}$ no tiene puntos básicos. Luego, $n = g-1$, $(\varepsilon_0, \ldots, \varepsilon_{g-1}) = (0, \ldots, g-1)$ y $\nu_{n-1} \geq g-1 < p$ (Proposición 2.1.3). Así que

$$(v_0, \ldots, v_{g-2}) = (0, \ldots, g-1)$$

y por la ecuación (6)

$$N \leq (g-2)(g-1) + 2\frac{(q+g-1)(g-1)}{g-1} \leq 2q + g(g-1). \qquad \boxdot$$

La hipótesis sobre la sucesión de lagunas en la proposición anterior se satisface si $p > 2g-2 = d$ (Corolario 1.5.11).

Observación 3.2.2. *La cota de la proposición 3.2.1 es mejor que la cota de Hasse–Weil si $|q^{\frac{1}{2}} - g| \leq \sqrt{g+1}$.*

Obsérvese que $2q + g(g-1) \leq q+1+2gq^{\frac{1}{2}} \iff q - 2gq^{\frac{1}{2}} + g^2 \leq g+1 \iff (q^{\frac{1}{2}} - g)^2 \leq g+1 \iff |q^{\frac{1}{2}} - g| \geq \sqrt{g+1}$. $\boxdot$

De lo anterior es claro que $q^{\frac{1}{2}} \leq 2g+1 \leq 2p+1$ y $q \leq (2p+1)^2$. Luego, $q = p$ ó $q = p^2$ si $p > 3$. Además, cuando $g = 3$ la proposición 3.2.1 y el teorema 1.1.1 representan la misma cota. Esto no es sorprendente pues el encaje canónico de una curva que no es hiperelíptica de género 3 es plano y de grado 4.

Proposición 3.2.3. *Sea C una curva proyectiva, no singular, algebraica de género g definida sobre el cuerpo finito $\mathbb{F}_q$ de característica p y N el número de puntos racionales. Si $\frac{p+3}{2} \geq g \geq 3$ $(p \geq 2g-3)$ y C no es hiperelíptica, entonces*

$$N \leq \frac{2g-3}{g-2}q + g(g-2).$$

Prueba.

Consideremos un punto racional $P \in C$ y definamos $\mathfrak{D} = |W - P|$ donde W es un divisor canónico sobre $\mathbb{F}_q$. Como C no es hiperelíptica, el sistema lineal canónico $|W|$ es *muy abundante* (Véase Hartshorne R. [5], Cap. IV Prop 5.2). Es decir, $\dim\big(|W - Q - R|\big) = \dim\big(|W|\big) - 2 = g - 2$ para cualquier par de puntos $Q, R \in C$. De otro lado, por el Teorema de Riemann–Roch y $\dim(0) = \dim(P) = 1$,

$$\dim(|W - P - Q|) = 2g - 3 + 1 - g + 1 = gr(W - P) + 1 - g + \dim(P) = \dim(W - P) - 1.$$

Luego, por Hartshorne R. [5] Cap. IV Prop. 3.1 se tiene que $\mathfrak{D}$ no tiene puntos básicos; $n = g - 2$ y $d = 2g - 3 \leq p$. Así, por el Observación 3.2.2 $v_i \leq i + 2g - 3 - (g - 2) \leq g - 2 + g - 1 = 2g - 4 < p$. Por lo tanto, $v_{n-1} < p$, $(v_0, \ldots, v_{g-3}) = (0, \ldots, g - 3)$ por la Proposición 2.1.11 y

$$N \leq (g - 2 - 1)(g - 1) + 2\frac{(q + g - 2)(g - 2)}{2g - 3} = \frac{2g - 3}{g - 2}q + g(g - 2). \qquad \boxdot$$

Observación 3.2.4. *La cota de la proposición 3.2.3 es mejor que la cota de Hasse–Weil si* $|q^{\frac{1}{2}} - g(g-2)(g-1)^{-1}| \leq (g-1)^{-1}(g-2)^{\frac{1}{2}}(g^2 - g - 1)^{\frac{1}{2}}$.

Obsérvese que $\frac{2g-3}{g-2}q + g(g-2) \leq q + 1 + 2gq^{\frac{1}{2}} \iff \left(\frac{2g-3}{g-2} - 1\right)q - 2gq^{\frac{1}{2}} \leq 1 - g(g-2) \iff \frac{g-1}{g-2}q - 2gq^{\frac{1}{2}} \leq 1 - g(g-2) \iff q - 2g(g-2)(g-1)^{-1}q^{\frac{1}{2}} \leq (g-2)(g-1)^{-1}\big(1 - g(g-2)\big) \iff q - 2g(g-2)(g-1)^{-1}q^{\frac{1}{2}} + g^2(g-2)^2(g-1)^{-2} \leq (g-2)(g-1)^{-1}\big(1 - g(g-2)\big) + g^2(g-2)^2(g-1)^{-2}$. Así

$$\begin{aligned}(q^{\frac{1}{2}} - g(g-2)(g-1)^{-1})^2 &\leq (g-2)(g-1)^{-2}\left[(g-1)\big(1 - g(g-2) + g^2(g-2)\big)\right] \\ &\leq (g-2)(g-1)^{-2}\left[-1 + g(g-2) + g\right] \\ &\leq (g-2)(g-1)^{-2}[g^2 - g - 1].\end{aligned}$$

De donde

$$|q^{\frac{1}{2}} - g(g-2)(g-1)^{-1}| \leq (g-1)^{-1}(g-2)^{\frac{1}{2}}(g^2 - g - 1)^{\frac{1}{2}}$$

$\boxdot$

En la observación anterior,

$$q^{\frac{1}{2}} \leq (g-1)^{-1}\left(g(g-2) + (g-2)^{\frac{1}{2}}(g^2 - g - 1)^{\frac{1}{2}}\right)$$

y

$$q \leq (g-1)^{-2}\left(g(g-2) + (g-2)^{\frac{1}{2}}(g^2 - g - 1)^{\frac{1}{2}}\right)^2.$$

Ahora, como $(g-1)^2 > g^2 - 2g$, $\left(g - \frac{1}{2}\right)^2 > g^2 - g - 1$ y $\left(g - \frac{1}{2}\right)^{\frac{3}{2}} < \frac{4}{5}(g-1)^2$ cuando $g > 4$ $(p > 5)$, entonces $q < (g-1)^{-2}\left((g-1)^2 + \left(g - \frac{1}{2}\right)^{\frac{3}{2}}\right)^2$ y

$$q < (g-1)^{-2}\left(\frac{9}{5}(g-1)^2\right)^2 = \frac{9^2}{5^2}(g-1)^2.$$

Luego, si $p > 7$, $q < \frac{9^2}{10^2}(p+1)^2 < p^2$ y por lo tanto $q = p$. Cabe decir que el mismo resultado ($q = p$) se puede verificar en el caso $p \leq 7$, haciendo el calculo explícito de las cota de q para los posibles valores de g.

De otro lado, la cota de la proposición 3.2.3 es mejor que la cota de la proposición 3.2.1 si y solo si, $\frac{2g-3}{g-2}q + g(g-2) \leq 2q + g(g-1) \iff (2g-3)q - (2g-4)q < (g-1)g(g-2) - (g-2)g(g-2) \iff q \leq g(g-2)$. Así, $q \leq p(p-2) < p^2$ y $q = p$.

Un ejemplo númerico en el que se tienen mejores cotas es el caso $g = 4$ y $q = 7$ ($p = 7 > 2g-3 = 5 > g = 4$) en el que la cota de Hasse–Weil es 29 la de Serre ($N \leq q+1+[|2q^{\frac{1}{2}}|]q$, donde $[|\cdot|]$ es la función parte entera) es 28 la de la proposición 3.2.1 es 26 y la de la proposición 3.2.3 es 25.

Ejemplo 3.2.5. La única curva C de género 3 tal que $N > 2q + g(g-1)$ es la hermitiana $y^3 + y + x^4 = 0$, si $p \geq g$.

Por la proposición 3.2.1 la sucesión de $\mathfrak{D}$-ordenes $(\varepsilon_0, \varepsilon_1, \varepsilon_2)$ o de lagunas de Weierstrass no es clásica $\big(\dim(\mathfrak{D}) = n = g - 1 = 2$ y $gr(\mathfrak{D}) = 2g - 2 = 4\big)$. Luego, por Komiya [8], Teo. 1, pag 379 se tiene que $p = 3$ y C es la hermitiana y $(\varepsilon_0, \varepsilon_1, \varepsilon_2) = (0, 1, 3)$. Luego, la sucesión de invariantes hermitianos de un punto de Weierstrass (estos existen pues $g > 1$) es $(j_0, j_1, j_2) = (0, 1, 4)$ y la sucesión (v_0, v_1) no es clásica, pues de lo contrario, por el Teorema 2.2.2 (Véase la ecuación (6)) $N \leq 2 + 4\frac{(q+2)}{2} = 2q + g(g-1)$. Así, $(v_0, v_1) = (0, 3)$.

La curva hermitiana también da contraejemplos a las siguientes afirmaciones sobre puntos racionales de Weierstrass: $v_i = \varepsilon_i$, $v_i \leq \varepsilon_{i+1} - \varepsilon_1$, $v_i \leq j_i$ y $\nu_P(S) > n$ $\big($Por la Proposición 2.1.12, $\nu_P(S) = \sum_{i=0}^{1} j_{i+1} - v_i = 1 + 4 - 3 = 2 = n\big)$.

Los resultados de esta última sección son solamente vislumbres de una extensa teoría de caracterización de curvas con muchos lugares racionales; mejorando la hipótesis de Riemann y excluyendo algunas curvas cuya sucesión de ordenes de Frobenius no es clásica. De otro lado, queda por analizar si es posible obtener *fórmulas explícitas* para el número de puntos racionales con los métodos desarrollados aquí. Estos problemas no están dentro de nuestro alcance, en este humilde trabajo.

Referencias

[1] Apostol, T., Introduction to Analytic Number Theory, California Institute of Tecnology, California, 1976.

[2] Atiyah, M., MacDonald, I. *Introducción al Algebra Conmutativa*. Universidad de Oxford, Massachusetts, 1969.

[3] Bombieri, E. *Problems of the Millenium:The Riemann Hypothesis*. Institute for Advanced Study, Princeton, NJ, 08540, CLAY (2000).

[4] Fulton, W. *Algebraic Curves*. W.A. Benjamin, Inc. Massachusetts, 1974.

[5] Hartshorne, R. *Algebraic Geometry*. University of California, California, 1977.

[6] Harris, J. *Algebraic Geometry. A First Course*. Harvard University, Cambrige, 1992.

[7] Hilton, P. Stammbach, U. *A Course in Homological Algebra*. Springer-verlag, New York, Heidelberg, Berlin, 1971.

[8] Komiya, K. *Algebraic curves with non-classical types of gap sequences for genus three and four*. Hiroshima Math. J., 8 (1978), 371-400.

[9] Lang, S. *Linear Algebra*. University of Tokyo, Tokyo, 1981.

[10] Litaka, S. *Algebraic Geometry. An introduction to Birrational Geometry of Algebraic Varieties*. University of Tokyo, Tokyo, 1981.

[11] Roman, S. *Field Theory*. Springer-Verlag, New York, California State University, 1991.

[12] Sarnak, P. *Problems of the Millenium:The Riemann Hypothesis (2004)*. Princeton University and Courant Institute of Math. Sciences.

[13] Simarra A. *El Teorema de Bezout*. Universidad del Valle, Cali, 2005 (tesis).

[14] Schmidt, W. M. *Equations over finite fields, an elementary approach*. Lecture Notes in Mathematics 536 , Springer, Berlin, 1976.

[15] Stark, H *On the Riemann hypothesis in hyperelliptic function fields*, Proceedings of Symposia in Pure Mathematics 24 (ed. F. Browder, American Mathematical Society, Providence, R.I., 1973), pp. 285-302.

[16] Stichtenoth, H. *Algebraic Functions Fields and Codes*. Springer, Berlin, 1993.

[17] Stöhr, K-O, Voloch, J. F. *Weierstrass points and curves over finite fields*. Proc. London Math Soc. (3), 1986, 1-19.

Índice alfabético