UNIVERSIDAD NACIONAL DEL LITORAL
FACULTAD DE INGENIERÍA QUÍMICA

Tesis presentada como parte de los requisitos de la Universidad Nacional del Litoral para la obtención del Grado Académico de

Doctor en Matemática

En el campo de: **Teoría de números**

Título de la Tesis:

Estudio del comportamiento asintótico de torres de cuerpos de funciones

Institución donde se realizó:

Instituto de Matemática Aplicada del Litoral (IMAL)

Autor:

Lic. María de los Angeles Chara

Directores de Tesis

Dr. Roberto Miatello Dr. Ricardo Toledano

Defendida ante el jurado compuesto por:

Dra. Teresa Krick

Dr. Ariel Pacetti

Dr. Ricardo Podestá

Año de presentación: 2012

A mi familia y amigos

Agradecimientos

Hay muchos a quienes quiero agradecer, pues ciertamente la culminación de este trabajo no fue sólo un esfuerzo académico personal, sino que requirió del apoyo de muchas personas a través de estos años.

A Dios, por darme *salud*, *dinero* y *amor*, en las justas proporciones y por haberme favorecido con el gusto por la Matemática.

A mis directores, Ricardo y Roberto por su disposición durante todo el doctorado, pues no solo recibí de su parte la instrucción adecuada para afrontar los problemas de la Tesis, sino que constante e incondicionalmente me mostraron su confianza en mis capacidades.

A mis padres Alicia y Leopoldo por inculcar en mí tantos valores, incluyendo el amor al estudio y por apoyarme en mi proyecto de vida. A mis hermanos Vivi, Estani, Anita y Francis y a mi abuela Zule por quererme tanto y estar siempre conmigo.

A la Facultad de Ingeniería Química de la Universidad Nacional del Litoral y al Instituto de Matemática Aplicada del Litoral por concederme la oportunidad de recibir educación de primera en un ambiente tan favorable y al CONICET por permitirme económicamente llevar a cabo estos estudios al otorgarme la beca doctoral. A la Facultad de Astronomía, Matemática y Física de la Universidad Nacional de Córdoba, por recibirme y abrirme sus puertas. A todos mis profesores, por la excelente formación matemática recibida durante estos nueve años de carrera.

A todos los que aceptaron el compromiso de evaluar esta Tesis y más aún a aquellos que han tenido la ardua tarea de leerla. Gracias por los valiosos comentarios y correcciones.

A Richie por aguantarme en mis momentos más negativos, por insistirme y provocarme para sacar lo mejor de mí, por su confianza, y por mostrarme el lado lindo de la matemática: la teoría de números.

A mis amigas Pame y Marilina, por su inagotable amor y paciencia, por el constante soporte anímico y los buenos consejos (incluso los tirones de orejas en los momentos apropiados) y por haber estado conmigo ayudándome a preparar esta Tesis. También a Olguis, Marisa y Gisela, por estar conmigo siempre y quererme como soy.

A Facu y a mis amigos y compañeros corredores, nadadores, montañistas y escaladores, por mostrarme que en la vida uno puede hacer y disfrutar de miles de actividades sin importar los obstáculos, las dificultades ni los tiempos que esto nos lleve. Gracias por los invaluables momentos que pasamos juntos, y por los paisajes y lugares que no voy a olvidar.

A todos los integrantes del IMAL, por tanta calidez no sólo profesional sino personal, y sobre todo a todos aquellos que supieron cómo estar presentes cuando necesité de su ayuda. Por todo su apoyo, predisposición y buena voluntad. Y sobre todo a los *imalitos*, entre los que he conseguido muy buenos amigos. Gracias por crear un agradable ambiente de trabajo y estudio, por los buenos mates, las lindas charlas y los valiosos consejos.

Finalmente, pero no menos importante, a Arnaldo García, Peter Beelen y Henning Stichtenoth, a quienes tuve la oportunidad de conocer en diferentes oportunidades. Gracias por las discusiones matemáticas, las cuales abarcaron desde aclaraciones en demostraciones hasta problemas y sugerencias que hicieron mejor esta Tesis.

María

ÍNDICE GENERAL

RESUMEN

En esta Tesis nos concentramos en obtener resultados estructurales generales sobre el comportamiento asintótico de sucesiones de cuerpos de funciones sobre cuerpos perfectos en general y de torres de cuerpos de funciones sobre cuerpos finitos en particular. En el Capítulo 1 damos las definiciones básicas y resultados conocidos que se usarán a lo largo de la presente Tesis. Luego, abordamos el problema de ver bajo qué condiciones una ecuación del tipo $a(y) = b(x)$, con a y b funciones racionales con coeficientes en un cuerpo finito, define un torre. En el Capítulo 2 damos condiciones suficientes que debe cumplir una ecuación del tipo $a(y) = b(x)$, que define explícitamente a una torre de cuerpos de funciones $\mathcal{F} = (F_0, F_1, F_2, \ldots)$, para garantizar estimaciones no triviales del número de lugares racionales $N(F_i)$ que hay en cada etapa F_i. La formulación de estas condiciones permite una implementación computacional sencilla. Damos ejemplos concretos mostrando que varios ejemplos conocidos son casos particulares de nuestros resultados generales.

El estudio de la ramificación de lugares en una torre de cuerpos de funciones es de importancia central en la teoría general del comportamiento asintótico de torres de cuerpos de funciones. En particular, la finitud del espacio de ramificación de una torre determina, en muchos casos, el comportamiento asintótico del género de los cuerpos de funciones que definen la torre. En el Capítulo 3 estudiamos condiciones para que el espacio de ramificación de cierta clase de torres de tipo Kummer sea finito. La determinación del género es esencial para la obtención de estimaciones no triviales de una función que es objeto de mucha investigación por su importancia en la moderna teoría de códigos algebraicos. Tal función es conocida como la función de Ihara, que se denota $A(q)$, donde q es una potencia de un número primo. Como aplicación de los resultados generales obtenidos, damos una demostración (alternativa a las conocidas) de la no trivialidad

de $A(q)$ cuando $q \geq 3$. También mostramos nuevos ejemplos de torres con espacios de ramificación finita que dan origen a torres asintóticamente buenas.

Por otra parte, hacemos un estudio de los conceptos de subsucesión y de supersucesión de una sucesión de cuerpos de funciones, dando un método general para la construcción de las mismas. Con la construcción de torres y subtorres se encuentran nuevos casos de torres asintóticamente buenas o malas a partir de casos ya estudiados. Comprobamos que muchos de los ejemplos conocidos son casos particulares de nuestra construcción.

Finalmente, en el Capítulo 4 damos condiciones generales para determinar si una sucesión de cuerpos de funciones es asintóticamente mala. Damos varios ejemplos nuevos de torres asintóticamente malas y mostramos que muchos de los criterios conocidos para determinar si una torre es asintóticamente mala se obtienen como casos particulares de nuestros resultados. Damos una nueva demostración de un resultado debido a Garcia, Stichtenoth y Rück [**GSR03**] que establece que si cada extensión F_i/F_0 es de Galois en una sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre un cuerpo perfecto K y el espacio de ramificación es infinito entonces el género de la sucesión es infinito. Esto implica en particular que $\mathcal{F}$ es una torre asintóticamente mala sobre K.

Este resultado es, en realidad, parte de una conjetura debida a Beelen, Garcia y Stichtenoth [**BGS05b**] que establece que en el caso de sucesiones recursivas, la infinitud de su espacio de ramificación implica la infinitud del género de la sucesión.

INTRODUCCIÓN

El estudio del comportamiento asintótico de torres de cuerpos de funciones sobre cuerpos finitos está motivado, en gran parte, por problemas relativos a la existencia de códigos lineales con "buenos" parámetros en el sentido que definiremos a continuación. Sea $\mathbb{F}_q$ el cuerpo finito con q elementos. Un código lineal $\mathcal{C}$ sobre el alfabeto $\mathbb{F}_q$ es un subespacio lineal de $\mathbb{F}_q^n$, donde los elementos de $\mathbb{F}_q^n$ se llaman palabras y los elementos de $\mathcal{C}$ se llaman palabras código. Decimos que n es la longitud del código y que $k = \dim \mathcal{C}$ es la dimensión del código (como espacio vectorial sobre $\mathbb{F}_q$). Para $a = (a_1, a_2, \ldots, a_n)$ y $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$, sea $d(a, b) = |\{i : 1 \leq i \leq n,\, a_i \neq b_i\}|$. Esta función d se llama distancia de Hamming y es una métrica en $\mathbb{F}_q^n$. La distancia mínima $d(\mathcal{C})$ de un código $\mathcal{C}$ es la menor distancia de Hamming entre palabras código distintas, es decir, $d(\mathcal{C}) = \text{mín}\{d(x, y) : x \in \mathcal{C},\, y \in \mathcal{C},\, x \neq y\}$. Un $[n, k, d]$-código $\mathcal{C}$ es un código de longitud n, dimensión k y distancia mínima d y un tal código $\mathcal{C}$ puede detectar hasta $d-1$ errores y corregir hasta $\lfloor (d-1)/2 \rfloor$ errores en cualquier palabra código, donde $\lfloor x \rfloor$ denota el piso del número real x, es decir, el mayor entero m tal que $m \leq x$. Dado un $[n, k, d]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$, definimos su tasa de trasmisión de información como $R = R(\mathcal{C}) = k/n$ y su distancia mínima relativa como $\delta = \delta(\mathcal{C}) = d/n$.

Los códigos buenos son aquellos en los cuales tanto la tasa de transmisión de información como la distancia mínima relativa tienen valores lo más cercanos a 1 posible, ya que la primera regula la cantidad de mensajes que se pueden enviar con respecto a la longitud de las palabras necesarias, mientras que la segunda permite corregir un porcentaje positivo de errores por palabra, lo cual es un problema de interés en la teoría de códigos sobre cuerpos finitos. Sin embargo, estas condiciones son de alguna manera incompatibles ya que la conocida cota de Singleton establece que para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

$k + d \leq n + 1$. Por lo tanto, la obtención de buenos códigos requiere realizar un delicado balance entre estos parámetros.

A principio de la década del 80, Manin [**Man81**] demostró que existe una función continua $\alpha_q : [0,1] \to [0,1]$ tal que $U_q = \{(\delta, R) : 0 \leq \delta \leq 1 \text{ y } 0 \leq R \leq \alpha_q(\delta)\}$, donde U_q es el conjunto de puntos límite del conjunto $V_q = \{(\delta(C), R(C)) : C \text{ es un código sobre } \mathbb{F}_q\}$. Se sabe que la función α_q es decreciente en el intervalo $[0, 1 - q^{-1}]$, que $\alpha_q(0) = 1$ y que $\alpha_q(\delta) = 0$ para $1 - q^{-1} \leq \delta \leq 1$, pero su valor en cada punto no se conoce explícitamente, solamente se conocen cotas inferiores. La función de Manin es una función de interés en la teoría de códigos sobre cuerpos finitos pues la existencia de cotas inferiores para α_q garantiza la existencia de códigos *largos* buenos sobre $\mathbb{F}_q$ tales que $\delta(\mathcal{C}) \approx \delta$ y $R(\mathcal{C}) \gtrsim \alpha_q(\delta) > 0$, para $0 \leq \delta \leq 1 - q^{-1}$, es decir, códigos con longitud arbitrariamente grande, tasa de transmisión de información positiva y que son capaces de corregir una buena cantidad de errores por palabra. Si $H_q : [0, 1 - q^{-1}] \to \mathbb{R}$ es la función entropía q-aria, definida por

$$H_q(x) = \begin{cases} 0 & \text{si } x = 0; \\ x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x) & \text{si } x \neq 0. \end{cases}$$

entonces la versión asintótica de la cota conocida como Gilbert-Varshamov (ver [**HK03**]) establece que

$$\alpha_q(\delta) \geq 1 - H_q(\delta) \qquad \text{para } 0 \leq \delta \leq 1 - q^{-1}.$$

La existencia de códigos algebraicos cuyos parámetros superan la cota de Gilbert-Varshamov (ver [**Hil86**] o [**HK03**]) era desconocida hasta la década del 80. Ideas de Manin sobre la existencia de una sucesión de códigos con propiedades asintóticas especiales permitieron a Tsfasman, Vladut y Zink, con métodos de geometría algebraica, demostrar la existencia de códigos cuyos parámetros superaron la cota de Gilbert-Varshamov, ([**TVZ82**]). Estos códigos se basan en las ideas de Goppa, quien a mediados de la década del 70, utilizó métodos de geometría algebraica en el contexto de los cuerpos finitos para la construcción de códigos con interesantes propiedades. La construcción de Goppa (que apareció por primera vez publicada a principios de la década del 80 en [**Gop81**]) requiere disponer de torres de cuerpos de funciones con "muchos" lugares racionales, en el sentido

de que el número de lugares racionales supere sustancialmente al género, y además que los cuerpos que componen la torre estén definidos por ecuaciones explícitas.

Sea q una potencia de un primo y sea $F/\mathbb{F}_q$ un cuerpo de funciones. Un famoso resultado de Weil [**Wei48**] establece que si $N(F)$ denota al número de lugares racionales (o lugares de grado uno) y $g(F)$ denota al género de $F/\mathbb{F}_q$, entonces

$$|N(F) - (q+1)| \leq 2g(F)\sqrt{q}.$$

La desigualdad anterior se conoce como la cota de Hasse-Weil. Una mejora debida a Serre [**Ser83**],[**Ser85**] establece que

$$|N(F) - (q+1)| \leq g(F)\lfloor 2\sqrt{q}\rfloor.$$

A principios de la década del 80, Ihara [**Iha81**] introdujo la función

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$$

donde $N_q(g)$ es el máximo número de lugares racionales de un cuerpo de funciones sobre $\mathbb{F}_q$ con género g. Esta función representa una cota inferior para la función de Manin, ya que se puede probar (ver [**Sti09**, Proposición 8.4.6]) que si $A(q) > 1$ entonces

$$\alpha_q(\delta) \geq 1 - A(q)^{-1} - \delta \qquad \text{para todo } \delta \in [0, 1 - A(q)^{-1}],$$

y de ahí la importancia de su estudio.

Drinfeld y Vladut [**VD83**] mostraron que $A(q) \leq \sqrt{q}-1$. Ihara, e independientemente Tsfasman, Vladut y Zink, mostraron que si q es un cuadrado entonces $A(q) = \sqrt{q} - 1$. Cuando q no es un cuadrado, el valor exacto de $A(q)$ no se conoce. Sin embargo, Serre [**Ser83**] probó que existe una constante $c > 0$ tal que $A(q) \geq c \cdot \log q$ para todo q. Zink [**Zin85**] probó que cuando $q = p^3$ es una potencia cúbica de un primo entonces

$$A(p^3) \geq \frac{2(p^2-1)}{p+2},$$

y más tarde, Bezerra, Garcia y Stichtenoth [**BGS05c**] generalizaron este mismo resultado para cualquier potencia cúbica. Una manera de obtener cotas inferiores no triviales para la función de Ihara es a través de la construcción de torres de cuerpos de funciones asintóticamente buenas sobre $\mathbb{F}_q$ (Ver [**GS07**]).

Como un primer paso en la construcción de tales torres, es necesario encontrar cotas inferiores no triviales para el número $N(F_i)$ de lugares racionales de un cuerpo de funciones $F_i/\mathbb{F}_q$ que pertenezca a una sucesión $(F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ tales que $F_i \subsetneq F_{i+1}$. Un método para obtener este tipo de cotas, hace uso del llamado espacio de descomposición de una sucesión de cuerpos de funciones (Ver Sección 2 del Capítulo 2).

La Tesis está organizada de la siguiente manera. En el capítulo 1 introducimos las definiciones y resultados básicos de la teoría de cuerpos de funciones algebraicas y de sucesiones y torres de cuerpos de funciones. Enunciamos resultados conocidos sobre ramificación de lugares en extensiones de cuerpos de funciones y mostramos algunos resultados asintóticos. En el caso de torres definidas recursivamente por una ecuación de la forma $f(x, y) = 0$, donde $f \in \mathbb{F}_q[x, y]$, no toda elección del polinomio f define una torre. En la Sección 4 probamos resultados que establecen condiciones suficientes para que un polinomio de la forma $f(x, y) = a_1(y)b_2(x) - b_1(x)a_2(y)$ donde a_1 y a_2 son polinomios coprimos entre sí, como así también b_1 y b_2, defina una torre recursiva de cuerpos de funciones.

En el capítulo 2 mostramos la existencia de una cota inferior para el espacio de descomposición en función del tamaño de un subconjunto no vacío de $\Sigma \subset \mathbb{F}_q \cup \{\infty\}$ con ciertas propiedades. El objetivo principal en este capítulo es dar condiciones suficientes para encontrar tal conjunto Σ para una cierta clase de sucesiones de cuerpos de funciones que llamamos de tipo (a, b). Además, aplicamos los resultados obtenidos al caso de sucesiones de tipo Kummer sobre el cuerpo $\mathbb{F}_p$ con p primo. Este caso es de interés pues se conocen muy pocos ejemplos de espacios de descomposición no triviales de una sucesión sobre un cuerpo primo. Los resultados de este capítulo fueron publicados en el *Journal of Pure and Applied Algebra* ([**CT11**]) y pueden encontrarse online en `http://dx.doi.org/10.1016/j.jpaa.2011.03.003`.

En el capítulo 3 damos condiciones sobre las ecuaciones que definen una sucesión para obtener torres asintóticamente buenas a través del cálculo del espacio de ramificación. Utilizando los resultados obtenidos mostramos diferentes ejemplos de torres asintóticamente buenas. Además hacemos un estudio general sobre los conceptos de subtorre y de

supertorre de cuerpos de funciones. Estos conceptos son importantes en cuanto a que definen si un ejemplo de torre asintóticamente buena puede considerarse nuevo o no. También son útiles para demostrar si una torre es asintóticamente buena o no, comparándola con torres ya estudiadas. Damos un método general de construcción de subtorres y mostramos que la mayoría de los ejemplos conocidos son casos particulares de esta construcción. Uno de los resultados a destacar de este capítulo se encuentra en la Sección 3, donde mostramos que la ecuación

$$y^{q-1} = \frac{x^{q-1}}{x^{q-1} - (x-\alpha)^{q-1}}$$

con $\alpha \in \mathbb{F}_q^*$ define una sucesión de tipo Kummer con ramificación finita sobre $\mathbb{F}_q$ para todo $q \geq 3$. Esta ecuación define una torre asintóticamente buena sobre $\mathbb{F}_{2^n}$ si $n > 1$ y también sobre $\mathbb{F}_{q^2}$ si $q = p^n$ con p primo impar y $n \geq 1$. De esta manera, presentamos una demostración alternativa de la no trivialidad de la función de Ihara para potencias de dos y para potencias pares de primos impares.

Finalmente, en el Capítulo 4, estudiamos condiciones para que una sucesión recursiva de cuerpos de funciones sea asintóticamente mala. La principal motivación para este tipo de enfoque se encuentra en la búsqueda de invariantes que permitan abordar el problema de la clasificación de torres asintóticamente buenas o malas de tipo Kummer. Los principales resultados de este Capítulo están enunciados en los Teoremas 4.1.2 y 4.2.1. En la Proposición 4.1.2 damos condiciones suficientes para que una sucesión recursiva de cuerpos de funciones sea asintóticamente mala a través de la existencia de un divisor con ciertas propiedades. Demostramos que con la ayuda de esta proposición se puede hacer un estudio unificado de varios de los ejemplos existentes en la literatura sobre torres asintóticamente malas que, debido a las diferentes ecuaciones que definen estas torres, lucen como ejemplos de muy distinta naturaleza. En el Teorema 4.2.1 damos una nueva demostración de un resultado debido a Garcia, Stichtenoth y Rück [**GSR03**] que establece que si cada extensión F_i/F_0 es de Galois en una sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre un cuerpo perfecto K y el espacio de ramificación es infinito entonces el género de la sucesión es infinito. Esto implica en particular que $\mathcal{F}$ es una torre asintóticamente mala sobre K.

Este resultado es, en realidad, parte de una conjetura debida a Beelen, Garcia y Stichtenoth [**BGS05b**] que establece que en el caso de sucesiones recursivas, la infinitud de su espacio de ramificación implica la infinitud del género de la sucesión.

CAPÍTULO 1

PRELIMINARES

En este Capítulo introducimos las definiciones y resultados básicos de la teoría de cuerpos de funciones algebraicas y de sucesiones y torres de cuerpos de funciones. Enunciamos resultados sobre ramificación de lugares en extensiones de cuerpos de funciones y mostramos algunos resultados asintóticos conocidos. Además damos condiciones suficientes generales para que una sucesión sea una torre de cuerpos de funciones.

1.1. Cuerpos de funciones algebraicas

En esta Sección introduciremos las nociones básicas sobre cuerpos de funciones, las mismas pueden ser consultadas en [**Sti09**].

Definición 1.1.1. Un *cuerpo de funciones algebraicas F/K de una variable sobre un cuerpo K* es una extensión de cuerpos $F \supseteq K$ tal que F es una extensión algebraica finita de $K(x)$ para algún elemento $x \in F$ que sea trascendente sobre K.

Por simplicidad, nos referiremos a F/K como un *cuerpo de funciones*. El conjunto $\tilde{K} := \{z \in F : z \text{ es algebraico sobre } K\}$ es un subcuerpo de F, ya que sumas, productos e inversos de elementos algebraicos son también algebraicos. $\tilde{K}$ se llama *cuerpo de constantes de F/K*. Tenemos que $K \subseteq \tilde{K} \subseteq F$, y se verifica fácilmente que $F/\tilde{K}$ es un cuerpo de funciones sobre $\tilde{K}$. Decimos que K es *algebraicamente cerrado en F* (o que K *es el cuerpo total de constantes de F*) si $\tilde{K} = K$.

Definición 1.1.2. Sea F/K un cuerpo de funciones. Un *anillo de valuaciones* de F/K es un anillo $\mathcal{O} \subseteq F$ tal que:

I) $K \subsetneq \mathcal{O} \subsetneq F$, y

II) para cualquier $z \in F$ se tiene que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Se demuestra en [**Sti09**, Proposición 1.1.5] que $\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal P.

Teorema 1.1.3. [**Sti09**, Teorema 1.1.6] *Sea $\mathcal{O}$ un anillo de valuaciones del cuerpo de funciones F/K y sea P su único ideal maximal. Entonces:*

a) P es un ideal principal.

b) Si $P = t\mathcal{O}$ entonces cualquier $0 \neq z \in F$ tiene una representación única en la forma $z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$.

c) $\mathcal{O}$ es un dominio de ideales principales. Más precisamente, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.

Definición 1.1.4. Un *lugar (o lugar) P* del cuerpo de funciones F/K es el ideal maximal de algún anillo de valuaciones $\mathcal{O}$ de F/K. Cualquier elemento $t \in P$ tal que $P = t\mathcal{O}$ se llama *elemento primo* (o *parámetro local*) para P.

Cada anillo de valuaciones determina un único lugar y recíprocamente, cada lugar determina un único anillo de valuaciones, por lo tanto decimos que $\mathcal{O}_P$ es el *anillo de valuaciones del lugar P*.

El conjunto de lugares de F/K se denota por $\mathbb{P}(F)$. Podemos omitir el cuerpo base, K, en esta notación pues para cada lugar P de F/K se puede probar que $\tilde{K} \subseteq \mathcal{O}_P$.

Una segunda descripción de un lugar, que resulta de utilidad en muchos casos, está dada en términos de valuaciones.

Definición 1.1.5. Una *valuación discreta* de F/K es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:

(1) $v(x) = \infty$ si y sólo si $x = 0$.

(2) $v(xy) = v(x) + v(y)$ para todo $x, y \in F$.

(3) $v(x+y) \geq \min\{v(x), v(y)\}$ para todo $x, y \in F$.

(4) Existe un elemento $z \in F$ con $v(z) = 1$.

(5) $v(a) = 0$ para todo $0 \neq a \in K$.

En este contexto el símbolo ∞ representa algún elemento que no está en $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = n + \infty = \infty$ y $\infty > m$ para todo $m, n \in \mathbb{Z}$. De las propiedades (2) y (4) se obtiene que $v : F \to \mathbb{Z} \cup \{\infty\}$ es sobreyectiva. La propiedad (3) se llama *Desigualdad Triangular*.

Una versión más fuerte de la Desigualdad Triangular puede ser derivada de los axiomas y es en general de mucha utilidad.

Lema 1.1.6. [**Sti09**, Lema 1.1.11](Desigualdad Triangular Estricta) *Sea v una valuación discreta de F/K y sean $x, y \in F$ con $v(x) \neq v(y)$. Entonces*

$$v(x+y) = \min\{v(x), v(y)\}.$$

Definición 1.1.7. Para un lugar $P \in \mathbb{P}(F)$ asociamos una función $v_P : F \to \mathbb{Z} \cup \{\infty\}$ de la siguiente manera: sea t un elemento primo para P. Entonces todo $0 \neq z \in F$ tiene una representación única $z = t^n u$ con $u \in \mathcal{O}_P^*$ y $n \in \mathbb{Z}$. Definimos $v_P(z) := n$ y $v_P(0) := \infty$.

Teorema 1.1.8. [**Sti09**, Teorema 1.1.13] *Sea F/K un cuerpo de funciones. Para un lugar $P \in \mathbb{P}(F)$, la función v_P de la definición anterior es una valuación discreta de F/K. Más aún, tenemos que*

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\},$$

$$\mathcal{O}_P^* = \{z \in F : v_P(z) = 0\},$$

$$P = \{z \in F : v_P(z) > 0\}.$$

Sea P un lugar de F/K y sea $\mathcal{O}_P$ su anillo de valuaciones. Como P es un ideal maximal, el anillo de clases residuales $\mathcal{O}_P/P$ es un cuerpo que contiene una copia isomorfa de K. Para $x \in \mathcal{O}_P$ denotamos por $x(P)$ a la clase de residuos módulo P, para $x \in F \setminus \mathcal{O}_P$ definimos $x(P) = \infty$.

Definición 1.1.9. Sea $P \in \mathbb{P}(F)$.

(a) $F_P := \mathcal{O}_P/P$ es el *cuerpo de clases residuales* de P. La función

$$\begin{aligned} F &\longrightarrow F_P \cup \{\infty\} \\ x &\longmapsto x(P) \end{aligned}$$

es llamada *función de clases residuales.*

(b) Definimos el *grado de* P como $deg\, P := [F_P : K]$. Un lugar de grado uno, se dice que es un *lugar racional* de F/K.

El grado de un lugar es siempre finito, más aún, tenemos el siguiente resultado.

Proposición 1.1.10. [**Sti09**, Proposición 1.1.15] *Si P es un lugar de F/K y $0 \neq x \in P$ entonces*

$$deg\, P \leq [F : K(x)] < \infty.$$

Observación 1.1.11. Para el caso en que $deg\, P = 1$ tenemos que $F_P = K$, y la función de clases residuales, aplica F en $K \cup \{\infty\}$. En particular, si K es algebraicamente cerrado, todos los lugares son de grado uno, y por lo tanto se puede mirar a cada elemento $z \in F$ como una función

$$\begin{aligned} z: \ \mathbb{P}(F) &\longrightarrow K \cup \{\infty\} \\ P &\longmapsto z(P). \end{aligned}$$

Es por esto que F/K se dice que es un cuerpo de funciones. Los elementos de K interpretados como funciones son funciones constantes. Por esta razón K se llama el cuerpo de constantes de F.

Definición 1.1.12. Sea $z \in F$ y $P \in \mathbb{P}(F)$. Decimos que P es un *cero* de orden m de z si $v_P(z) = m > 0$. Decimos que P es un *polo* de orden m de z si $v_P(z) = m < 0$.

Observación 1.1.13. [**Sti09**, Corolario 1.3.4] En un cuerpo de funciones F/K todo elemento $0 \neq z \in F$ tiene una cantidad finita de ceros y de polos.

Es conveniente en este punto, suponer que el cuerpo base K es algebraicamente cerrado en el cuerpo de funciones F (es decir, $\tilde{K} = K$), por lo tanto de ahora en adelante supondremos que tenemos esta condición en la definición de cuerpo de funciones.

Definición 1.1.14. El grupo abeliano libre generado por los lugares de F se denomina *grupo de divisores* de F/K y lo denotamos por $\mathcal{D}_F$, es decir,

$$\mathcal{D}_F = \left\{ \sum_{P\in\mathbb{P}(F)} n_P P : n_P \in \mathbb{Z} \text{ y casi todo}^1\ n_P = 0 \right\}.$$

Los elementos de $\mathcal{D}_F$ se llaman *divisores* de F/K. Si $D = \sum_{P\in\mathbb{P}(F)} n_P P \in \mathcal{D}_F$ el *soporte* de D se define como

$$suppD := \{P \in \mathbb{P}(F) : n_P \neq 0\}.$$

Un divisor de la forma $D = P$ con $P \in \mathbb{P}(F)$ se dice que es un *divisor primo*. Dos divisores $D_1 = \sum n_P P$ y $D_2 = \sum m_P P$ se suman coeficiente a coeficiente,

$$D_1 + D_2 = \sum_{P\in\mathbb{P}(F)} (n_P + m_P)P.$$

El elemento neutro del grupo de divisores $\mathcal{D}_F$ es el divisor

$$0 := \sum_{P\in\mathbb{P}(F)} r_P P,$$

con $r_P = 0$ para todo $P \in \mathbb{P}(F)$.

Para $Q \in \mathbb{P}(F)$ y $D = \sum n_P P \in \mathcal{D}_F$ definimos $\mathrm{v}_Q(D) := n_Q$, por lo tanto

$$suppD = \{P \in \mathbb{P}(F) : \mathrm{v}_P(D) \neq 0\} \quad \text{y} \quad D = \sum_{P\in\mathbb{P}(F)} \mathrm{v}_P(D)P.$$

Definimos un orden parcial en $\mathcal{D}_F$ de la siguiente manera

$$D_1 \leq D_2 \quad \text{si y sólo si} \quad \mathrm{v}_P(D_1) \leq \mathrm{v}_P(D_2) \text{ para todo } P \in \mathbb{P}(F).$$

Si $D_1 \leq D_2$ y $D_1 \neq D_1$ escribiremos que $D_1 < D_2$. Un divisor D se llama *positivo (o efectivo)* si $D \geq 0$.

El *grado* de un divisor D se define como

$$deg\, D := \sum_{P\in\mathbb{P}(F)} \mathrm{v}_P(D) deg\, P.$$

Por la Observación 1.1.13, sabemos que todo elemento no nulo $z \in F$ tiene una cantidad finita de ceros y polos en $\mathbb{P}(F)$. Por lo tanto la siguiente definición tiene sentido.

[1]Una propiedad en $\mathbb{Z}$ se dice que vale para casi todo entero si vale para todos los enteros excepto un número finito de ellos.

Definición 1.1.15. Sea $0 \neq z \in F$ y denotemos por Z al conjunto de ceros (resp. N al conjunto de polos) de z en $\mathbb{P}(F)$. Entonces definimos

$$(z)_0 := \sum_{P \in Z} v_P(z)P, \qquad \text{el } \textit{divisor de ceros} \text{ del elemento } z,$$

$$(z)_\infty := \sum_{P \in N} (-v_P(z))P, \qquad \text{el } \textit{divisor de polos} \text{ del elemento } z,$$

$$(z) := (z)_0 - (z)_\infty, \qquad \text{el } \textit{divisor principal} \text{ del elemento } z.$$

Teorema 1.1.16. [**Sti09**, Teorema 1.4.11] *Sea $z \in F \setminus K$. Entonces*

$$deg\,(z)_0 = deg\,(z)_\infty = [F : K(z)].$$

En particular, todos los divisores principales tienen grado cero.

Definición 1.1.17. Para un divisor $D \in \mathcal{D}_F$ definimos el *espacio de Riemann-Roch* asociado a D por

$$\mathcal{L}(D) := \{x \in F : v_P(x) \geq -\mathrm{v}_P(D)\} \cup \{0\}.$$

El espacio de Riemann-Roch, es un espacio vectorial de dimensión finita sobre K, cuya dimensión se denota por $\ell(D)$.

Definición 1.1.18. El *género* g de un cuerpo de funciones se define como

$$g = \text{máx}\{deg\, D - \ell(D) + 1 \ : \ D \in \mathcal{D}_F\}.$$

El género es uno de los invariantes más importantes de un cuerpo de funciones, se puede probar que existe y que es un entero no negativo, (ver [**Sti09**, Proposición 1.4.14]).

1.2. Extensiones algebraicas y ramificación

De aquí en adelante K denotará un cuerpo perfecto[2]. Sea F/K un cuerpo de funciones y sea F' una extensión algebraica de F tal que la extensión F'/K es separable. Entonces F' es un cuerpo de funciones sobre K' donde K' es una clausura algebraica de K en F'.

[2]Un cuerpo K se dice *perfecto* si toda extensión algebraica L/K es separable. En particular, los cuerpos de característica cero y los cuerpos finitos son cuerpos perfectos

Definición 1.2.1. Si $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$ decimos que Q *divide* a P o que Q *está arriba* de P si $P \subset Q$, y lo denotamos $Q|P$.

Se puede probar (ver [**Sti09**, Proposición 3.1.4]) que $Q|P$ es equivalente a la existencia de un entero $e \geq 1$ tal que $v_Q(x) = e\, v_P(x)$ para todo $x \in F$, y además $Q \cap F = P$.

Definición 1.2.2. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$ tales que Q está arriba de P.

(a) El *índice de ramificación* $e(Q|P)$ de Q sobre P se define como el único entero $e(Q|P) := e$ que satisface

$$v_Q(x) = e\, v_P(x).$$

(ver [**Sti09**, Definición 3.1.5])

(b) Decimos que $Q|P$ está *ramificado* si $e(Q|P) > 1$, y que $Q|P$ *no ramifica* si $e(Q|P) = 1$. Decimos que un lugar $P \in \mathbb{P}(F)$ está *ramificado* en F'/F si existe $Q \in \mathbb{P}(F')$ tal que $Q|P$ y $Q|P$ ramifica, en caso contrario decimos que P *no ramifica* en F'/F.

(c) $f(Q|P) := [F'_Q : F_P]$ es el *grado de inercia* (o *grado relativo*) de Q sobre P.

Si F'/F es una extensión algebraica separable y $Q \in \mathbb{P}(F')$ entonces la restricción $Q \cap F$ de Q a F es un lugar de F.

Si F''/F' es otra extensión algebraica separable, y $P \in \mathbb{P}(F)$, $Q \in \mathbb{P}(F')$ y $R \in \mathbb{P}(F'')$ son tales que $R|Q$ y $Q|P$ entonces tenemos que $R|P$ valen

$$e(R|P) = e(R|Q)e(Q|P) \qquad \text{y} \qquad f(R|P) = f(R|Q)f(Q|P).$$

Con las definiciones anteriores estamos en condiciones de probar el siguiente lema que será de utilidad en el Capítulo 4 cuando trabajemos con extensiones isomorfas de cuerpos de funciones y en particular con torres de cuerpos de funciones.

Lema 1.2.3. *Sea F un cuerpo de funciones sobre K y sean H y H' extensiones de F de manera que exista un K-isomorfismo de cuerpos, $\sigma : H \to H'$, y sea $F' = \sigma(F)$. Entonces tenemos que*

1. *Si Q es un lugar de H entonces $\sigma(Q) = \{\sigma(x) : x \in Q\}$ es un lugar de H' y $\sigma(\mathcal{O}_Q) = \mathcal{O}_{\sigma(Q)}$.*
2. *Si $0 \neq z \in H'$ entonces $v_{\sigma(Q)}(z) = v_Q(\sigma^{-1}(z))$.*

3. Si $Q \in \mathbb{P}(H)$, $P \in \mathbb{P}(F)$ y $Q|P$ entonces $\sigma(Q)|\sigma(P)$. Más aún, $e(\sigma(Q)|\sigma(P)) = e(Q|P)$ y $f(\sigma(Q)|\sigma(P)) = f(Q|P)$.

Demostración. *1.* Probemos primero que $\sigma(Q)$ es un lugar. Para ello vamos a mostrar que $\sigma(\mathcal{O}_Q)$ es un anillo de valuaciones de H' y que $\sigma(Q) = \sigma(\mathcal{O}_Q) \setminus (\sigma(\mathcal{O}_Q))^*$.

Como σ es un homomorfismo de cuerpos, entonces $\sigma(\mathcal{O}_Q)$ es un anillo de H'. Claramente, $\sigma(\mathcal{O}_Q) \subsetneq H'$ (pues en caso contrario tendríamos que $\mathcal{O}_Q = \sigma^{-1}(H') = H$ lo cuál es absurdo).

De manera similar, para probar que $K \subsetneq \sigma(\mathcal{O}_Q)$, basta con probar que $K \subset \sigma(\mathcal{O}_Q)$ (pues en otro caso tendríamos un absurdo). Ahora, como $K \subset \mathcal{O}_Q$ y $\sigma(K) = K$ entonces

$$K = \sigma(K) \subset \sigma(\mathcal{O}_Q).$$

Luego $K \subsetneq \sigma(\mathcal{O}_Q) \subsetneq H'$.

Sea ahora $0 \neq z \in H'$ tal que $z \notin \sigma(\mathcal{O}_Q)$. Sea $0 \neq y \in H$ tal que $\sigma(y) = z$. Como $z \notin \sigma(\mathcal{O}_Q)$ entonces $y \notin \mathcal{O}_Q$ y como $\mathcal{O}_Q$ es un anillo de valuaciones en H, tenemos que $y^{-1} \in \mathcal{O}_Q$. Luego

$$z^{-1} = (\sigma(y))^{-1} = \sigma(y^{-1}) \in \sigma(\mathcal{O}_Q).$$

Tenemos entonces que $\sigma(\mathcal{O}_Q)$ es un anillo de valuaciones de H'.

Observemos ahora que en general, si A es un anillo en H' entonces $(\sigma(A))^* = \sigma(A^*)$. En efecto,

$$(\sigma(A))^* = \{\sigma(a) : a \in A \text{ y } \exists \sigma(b) \in \sigma(A) : \sigma(a)\sigma(b) = 1\}$$

y como

$$\sigma(a)\sigma(b) = 1 \Leftrightarrow \sigma(ab) = 1 \Leftrightarrow ab = 1$$

entonces $(\sigma(A))^* = \sigma(A^*)$.

Luego,

$$\sigma(\mathcal{O}_Q) \setminus (\sigma(\mathcal{O}_Q))^* = \sigma(\mathcal{O}_Q) \setminus \sigma(\mathcal{O}_Q^*) = \sigma(\mathcal{O}_Q \setminus \mathcal{O}_Q^*) = \sigma(Q)$$

y por lo tanto $\sigma(Q)$ es un lugar de H' y $\sigma(\mathcal{O}_Q) = \mathcal{O}_{\sigma(Q)}$.

2. Sea t un elemento primo de Q, es decir $Q = t\mathcal{O}_Q$. Entonces $\sigma(Q) = \sigma(t)\sigma(\mathcal{O}_Q) = \sigma(t)\mathcal{O}_{\sigma(Q)}$ y por lo tanto $\sigma(t)$ es un elemento primo de $\sigma(Q)$.

Sea $0 \neq z \in H'$ y sea $0 \neq y \in H$ el único elemento tal que $z = \sigma(y)$. Como $y \neq 0$ existen $n \in \mathbb{Z}$ y $u \in \mathcal{O}_Q^*$ tales que $y = t^n u$, y por lo tanto $v_Q(y) = n$.

Entonces

$$z = \sigma(y) = \sigma(t^n u) = \sigma(t)^n \sigma(u)$$

con $\sigma(u) \in \mathcal{O}_{\sigma(Q)}^*$ y por lo tanto $v_{\sigma(Q)}(z) = n$. Luego,

$$v_{\sigma(Q)}(z) = n = v_Q(y) = v_Q(\sigma^{-1}(z)).$$

3. Consideremos ahora la siguiente situación

$$\begin{array}{ccc} H & \xrightarrow{\quad\sigma\quad} & H' \\ | & & | \\ F & \longrightarrow & \sigma(F) \end{array} \qquad \begin{array}{ccc} Q & \xrightarrow{\quad\sigma\quad} & \sigma(Q) \\ | & & \\ P & \longrightarrow & \sigma(P) \end{array}$$

Como $Q|P$ entonces $P \subset Q$ y tenemos que $\sigma(P) \subset \sigma(Q)$. Luego $\sigma(Q)|\sigma(P)$.

Para probar que los índices de ramificación coinciden, recordemos que $e(\sigma(Q)|\sigma(P))$ es el único entero mayor o igual a 1 que satisface

$$v_{\sigma(Q)}(z) = e(\sigma(Q)|\sigma(P)) v_{\sigma(P)}(z)$$

para todo $0 \neq z \in H'$.

Pero si $0 \neq z \in H'$ entonces

$$v_{\sigma(Q)}(z) = v_Q(\sigma^{-1}(z)) = e(Q|P) v_P(\sigma^{-1}(z)) = e(Q|P) v_{\sigma(P)}(z).$$

Luego, $e(\sigma(Q)|\sigma(P)) = e(Q|P)$.

Finalmente para probar la igualdad de los índices de inercia consideremos la aplicación

$$\begin{array}{rccc} \tilde{\sigma}: & \mathcal{O}_Q/Q & \longrightarrow & \sigma(\mathcal{O}_Q)/\sigma(Q) \\ & z+Q & \longmapsto & \sigma(z)+\sigma(Q) \end{array}$$

Entonces $\tilde{\sigma}$ es un isomorfismo de cuerpos y tenemos que

$$\begin{aligned} f(Q|P) &= [\mathcal{O}_Q/Q : \mathcal{O}_P/P] \\ &= [\sigma(\mathcal{O}_Q)/\sigma(Q) : \sigma(\mathcal{O}_P)/\sigma(P)] \\ &= [\mathcal{O}_{\sigma(Q)}/\sigma(Q) : \mathcal{O}_{\sigma(P)}/\sigma(P)] \end{aligned}$$

$$= f(\sigma(Q)|\sigma(P)).$$

□

A continuación mencionamos algunos de los resultados conocidos más importantes sobre extensiones de cuerpos de funciones, que serán de utilidad más adelante.

Teorema 1.2.4. [**Sti09**, Teorema 3.1.11](Igualdad Fundamental) *Si F'/F es una extensión finita de cuerpos de funciones y $P \in \mathbb{P}(F)$ entonces*

$$\sum_{\substack{Q \in \mathbb{P}(F') \\ Q|P}} e(Q|P) f(Q|P) = [F' : F].$$

Definición 1.2.5. Sea F'/F una extensión finita de cuerpos de funciones de grado n y sea $P \in \mathbb{P}(F)$.

(a) Decimos que P se *descompone completamente* en la extensión F'/F si existen exactamente n lugares distintos de F' arriba de P. En este caso se tiene que $e(Q|P) = f(Q|P) = 1$ para todo $Q|P$.

(b) Si existe un lugar $Q \in \mathbb{P}(F')$ tal que $e(Q|P) = n$ entonces decimos que el lugar P es *totalmente ramificado* en la extensión F'/F. En este caso se tiene que hay un único lugar de F' arriba de P. La recíproca es cierta si $f(Q|P) = 1$.

El siguiente resultado establece un criterio muy útil para chequear la irreducibilidad de ciertos polinomios sobre un cuerpo de funciones. Un caso especial de la siguiente proposición se conoce como el *Criterio de Irreducibilidad de Eisenstein*.

Proposición 1.2.6 . [**Sti09**, Proposición 3.1.15] *Sea F/K un cuerpo de funciones y consideremos el polinomio*

$$\varphi(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0$$

con coeficientes $a_i \in F$. Supongamos que existe un lugar $P \in \mathbb{P}(F)$ tal que una de las siguientes condiciones vale:

(1) $v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ para $i = 1, \ldots, n-1$, y $\operatorname{mcd}(n, v_P(a_0)) = 1$.

(2) $v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ *para* $i = 1, \ldots, n-1$, $\mathrm{mcd}(n, v_P(a_0)) = 1$ *y* $v_P(a_0) < 0$.

Entonces $\varphi(T)$ *es irreducible en* $F[T]$. *Si* $F' = F(y)$ *donde* y *es una raíz de* $\varphi(T)$, *entonces* P *tiene una única extensión* $P' \in \mathbb{P}(F')$, *y tenemos que* $e(P'|P) = n$ *y* $f(P'|P) = 1$, *es decir,* P *es totalmente ramificado en* $F(y)/F$.

En varios resultados de esta Tesis vamos a generar extensiones de cuerpos de funciones, adjuntando a un cuerpo un elemento integral sobre un anillo de valuaciones de ese cuerpo. El siguiente resultado, da un criterio de integrabilidad utilizando el polinomio mínimo del elemento a adjuntar.

Proposición 1.2.7. [**Sti09**, Proposición 3.3.1] *Sea* F/K *un cuerpo de funciones con cuerpo total de constantes* K *y sea* $F' \supseteq F$ *una extensión de cuerpos finita. Sea* R *un subanillo de* F/K *integralmente cerrado tal que* F *es el cuerpo cociente de* R *(es decir,* R *es un anillo de holomorfía de* F/K*). Para* $z \in F'$ *denotemos por* $\varphi(T) \in F[T]$ *a su polinomio mínimo sobre* F. *Entonces tenemos que*

$$z \text{ es integral sobre } R \iff \varphi(T) \in R[T].$$

Para determinar el comportamiento de la ramificación de un lugar en ciertas extensiones el Teorema de Kummer que enunciamos a continuación es en general de utilidad. Observar que si $\psi(T) = \sum c_i T^i$ es un polinomio con coeficientes $c_i \in \mathcal{O}_P$ entonces denotamos por $\overline{\psi}(T)$ al polinomio

$$\overline{\psi}(T) := \sum c_i(P) T^i \in F_P[T].$$

Teorema 1.2.8. [**Sti09**, Teorema 3.3.7](Teorema de Kummer) *Sea* F/K *un cuerpo de funciones. Supongamos que* $F' = F(y)$ *donde* y *es un elemento integral sobre* $\mathcal{O}_P$, *y consideremos el polinomio mínimo* $\varphi(T) \in \mathcal{O}_P[T]$ *de* y *sobre* F. *Sea*

$$\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i}$$

la descomposición de $\overline{\varphi}(T)$ *en factores irreducibles sobre* F_P *(es decir, los polinomios* $\gamma_1(T), \ldots, \gamma_r(T)$ *son irreducibles, mónicos y distintos dos a dos en* $F_P[T]$ *y* $\epsilon_i \geq 1$*).*

Elijamos polinomios mónicos $\varphi_i(T) \in \mathcal{O}_P[T]$ *con*

$$\overline{\varphi}(T) = \gamma_i(T) \qquad y \qquad deg\,(\varphi_i(T)) = deg\,(\gamma_i(T)).$$

Entonces para $1 \leq i \leq r$*, hay lugares* $P_i \in \mathbb{P}(F')$ *que satisfacen*

$$P_i|P, \qquad \varphi_i(y) \in P_i \qquad y \qquad f(P_i|P) \geq deg\,(\gamma_i(T)).$$

Más aún $P_i \neq P_j$ *para* $i \neq j$*.*

Bajo hipótesis adicionales se puede probar más. Supongamos que al menos una de las siguientes hipótesis $(*)$ *o* $(**)$ *vale:*

$$\epsilon_i = 1 \qquad para \qquad i = 1, \ldots, r; \tag{$*$}$$

o

$$\{1, y, \ldots, y^{n-1}\} \quad es\ una\ base\ integral\ para\ P. \tag{$**$}$$

Entonces para $1 \leq i \leq r$ *existe exactamente un lugar* $P_i \in \mathbb{P}(F')$ *con* $P_i|P$ *y* $\varphi_i(y) \in P_i$*. Cada extensión* $P_i|P$ *es no ramificada y satisface* $f(P_i|P) = deg\,\gamma_i$ *(y por lo tanto, por la igualdad fundamental los lugares* $P_1, \ldots, P_r$ *son exactamente los lugares de* $\mathbb{P}(F')$ *que dividen a* P*).*

El *diferente* de F'/F es un divisor que se define de la siguiente manera:

$$\mathrm{Diff}(F'/F) := \sum_{P \in \mathbb{P}(F)} \sum_{Q|P} d(Q|P)Q,$$

donde $d(Q|P)$ es un entero no negativo unívocamente definido por P y Q llamado *exponente diferente*, (ver [**Sti09**, Sección 3.4]). Este divisor tiene un papel destacado en el cálculo del género en extensiones finitas y separables de cuerpos de funciones.

Para poder determinar explícitamente o, al menos, poder encontrar cotas para la Diferente, es necesario tener algún control sobre los exponentes diferentes involucrados. El siguiente teorema relaciona el exponente diferente con el índice de ramificación permitiendo en muchos casos obtener aproximaciones y cotas del diferente.

Teorema 1.2.9. [**Sti09**, Teorema 3.5.1](Teorema del diferente de Dedekind) *Siguiendo la notación anterior tenemos que para todo $Q|P$*

$$d(Q|P) \geq e(Q|P) - 1,$$

y la igualdad vale si y sólo si $e(Q|P)$ no es divisible por la característica de $\mathbb{F}_q$.

El siguiente resultado relaciona el exponente diferente de una extensión de cuerpos con los exponentes diferentes de extensiones intermedias.

Proposición 1.2.10. [**Sti09**, Corolario 3.4.12](Transitividad del exponente diferente) *Sean F''/F' y F'/F extensiones finitas y separables, donde F es un cuerpo de funciones sobre K. Entonces, para $P \in \mathbb{P}(F)$, $Q \in \mathbb{P}(F')$, y $R \in \mathbb{P}(F'')$ tales que $P \subset Q \subset R$ tenemos que*

$$d(R|P) = e(R|Q)d(Q|P) + d(R|Q).$$

La llamada Fórmula del género de Hurwitz establece una importante relación entre los géneros de los cuerpos de funciones involucrados.

Teorema 1.2.11. [**Sti09**, Teorema 3.4.13](Fórmula del género de Hurwitz) *Sea F/K un cuerpo de funciones sobre K y sea F'/F una extensión finita y separable. Denotemos por K' al cuerpo de constantes de F'. Entonces*

$$2g(F') - 2 = \frac{[F' : F]}{[K' : K]}(2g(F) - 2) + deg\ \mathrm{Diff}(F'/F),$$

donde $\mathrm{Diff}(F'/F)$ *denota al diferente de F'/F.*

Para calcular el género de un cuerpo de funciones F sobre un cuerpo K, se puede reemplazar el cuerpo base K por cualquier extensión algebraica de éste, siempre que K sea un cuerpo perfecto (ver [**Sti09**, Teorema 3.6.3]). En particular, para cuerpos finitos tenemos el siguiente resultado.

Proposición 1.2.12. *Sea $F/\mathbb{F}_q$ un cuerpo de funciones y sea $\mathbb{F}'_q$ una extensión algebraica de $\mathbb{F}_q$. Consideremos la extensión de cuerpos constante $F' = F\,\mathbb{F}'_q$. Entonces F' es un cuerpo de funciones sobre $\mathbb{F}'_q$. Más aún, todo lugar $P \in \mathbb{P}(F)$ no ramifica en F'/F y se tiene que $g(F') = g(F)$.*

Sean Q y P lugares tales que $Q|P$. Decimos que $Q|P$ *es moderadamente ramificado* si *char* $\mathbb{F}_q$ no divide a $e(Q|P)$; en otro caso decimos que $Q|P$ *tiene ramificación salvaje* o *no moderada.*

El siguiente resultado fundamental permite determinar el índice de ramificación de una composición de dos cuerpos de funciones utilizando la información sobre la ramificación en cada cuerpo siempre que en uno de ellos la ramificación sea moderada.

Proposición 1.2.13. [**Sti09**, Teorema 3.9.1](Lema de Abhyankar) *Sea F'/F una extensión finita y separable de cuerpos de funciones y supongamos que F' es la composición de dos cuerpos intermedios $F \subset F_1, F_2 \subset F'$. Sea $Q \in P(F')$ una extensión de $P \in \mathbb{P}(F)$ y denotemos por $P_i = Q \cap F_i$ para $i = 1, 2$. Si una de las extensiones $P_1|P$ o $P_2|P$ es moderada entonces*

$$e(Q|P) = \text{mcm}(e(P_1|P), e(P_2|P)).$$

Enunciamos ahora un resultado sobre la ramificación en una clase especial de extensiones de cuerpos de funciones llamadas extensiones de Kummer, ya que trabajaremos con extensiones de este tipo en el Capítulo 2.

Teorema 1.2.14. [**Sti09**, Proposición 3.7.3](Extensiones de Kummer) *Sea F/K un cuerpo de funciones algebraicas donde K contiene una raíz n-ésima primitiva de la unidad (con $n > 1$ y $\text{mcd}(n, char\, K) = 1$). Supongamos que $u \in F$ es un elemento que satisface*

$$u \neq w^d \quad \textit{para todo } w \in F \textit{ y } d|n,\ d > 1.$$

Sea

$$F' = F(y) \quad \textit{con } y^n = u.$$

La extensión F'/F se llama extensión de Kummer de F. Tenemos entonces que:

1. *El polinomio $\Phi(T) = T^n - u$ es el polinomio mínimo de y sobre F (en particular es irreducible sobre F). La extensión F'/F es una extensión de Galois de grado $[F' : F] = n$; su grupo de Galois es cíclico y los automorfismos de F'/F están dados por $\sigma(y) = \zeta y$ donde $\zeta \in \mathbb{F}_q$ es una n-ésima raíz de la unidad.*

2. *Sea $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$ una extensión de P. Entonces*

$$e(Q|P) = \frac{n}{r_P} \quad y \quad d(Q|P) = \frac{n}{r_P} - 1,$$

donde

$$r_P := \text{mcd}(n, v_P(u)) > 0$$

es el máximo común denominador de n y $v_P(u)$.

3. *Si K' denota el cuerpo de constantes de F' entonces*

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

Corolario 1.2.15. *Sea F/K un cuerpo de funciones y sea $F' = F(y)$ con $y^n = u$ y $u \in F$, donde $n \not\equiv 0 \mod char\, K$ y K contiene una n-ésima raíz primitiva de la unidad. Supongamos que existe un lugar $Q \in \mathbb{P}(F)$ tal que $\text{mcd}(v_Q(u), n) = 1$. Entonces K es el cuerpo total de constantes del cuerpo F', la extensión F'/F es cíclica de grado n, y*

$$g(F') = 1 + n(g(F) - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}(F)} (n - r_P) deg\, P.$$

Observación 1.2.16. Los resultados de la Proposición 1.2.14 y del Corolario 1.2.15 valen incluso si K no contiene una n-ésima raíz primitiva de la unidad. En este caso $F(y)/F$ ya no será, en general, una extensión de Galois. En el caso de una extensión cuadrática sí lo es.

Teniendo en cuenta la observación anterior, damos la siguiente definición.

Definición 1.2.17. Sea F/K un cuerpo de funciones algebraicas y sea $n > 1$ un entero coprimo con la característica de K. Supongamos que $u \in F$ es un elemento que satisface

$$u \neq w^d \quad \text{para todo } w \in F \text{ y } d|n,\ d > 1.$$

Sea

$$F' = F(y) \quad \text{con } y^n = u.$$

En este caso decimos que la extensión F'/F es un extensión *de tipo Kummer* de F.

Para finalizar esta Sección damos algunos resultados sobre otra clase especial de extensiones con las cuales también trabajaremos en esta Tesis, las extensiones de tipo Artin-Schreier. Antes de enunciar el teorema principal de la teoría de este tipo de extensiones necesitamos un lema previo.

Lema 1.2.18. [**Sti09**, Lema 3.7.7] *Sea F/K un cuerpo de funciones algebraicas con característica $p > 0$. Dado un elemento $u \in F$ y un lugar $P \in \mathbb{P}(F)$, lo siguiente vale:*

(a) o bien existe un elemento $z \in F$ tal que $v_P(u - (z^p - z)) \geq 0$,

(b) o bien para algún $z \in F$,

$$v_P(u - (z^p - z)) = -m < 0 \quad \text{con } m \not\equiv 0 \mod p.$$

En el último caso el entero m está unívocamente determinado por u y P, de la siguiente manera

$$-m = \max\{v_P(u - (w^p - w)) : w \in F\}.$$

Teorema 1.2.19. [**Sti09**, Proposición 3.7.8](Extensiones de Artin-Schreier) *Sea F/K un cuerpo de funciones algebraicas con característica $p > 0$. Supongamos que $u \in F$ es un elemento que satisface la siguiente condición:*

$$u \neq w^p - w \quad \text{para todo } w \in F.$$

Sea

$$F' = F(y) \qquad \text{con } y^p - y = u.$$

Una extensión F'/F de este tipo se llama extensión de Artin-Schreier de F. Para P en $\mathbb{P}(F)$ definimos el entero m_P por

$$m_P := \begin{cases} m & \text{si existe un elemento } z \in F \text{ que satisfaga} \\ & v_P(u - (z^p - z)) = -m < 0 \quad \text{con } m \not\equiv 0 \mod p. \\ -1 & \text{si } v_P(u - (z^p - z)) \geq 0 \text{ para algún } z \in F. \end{cases}$$

(Observar que m_P está bien definido por el Lema 1.2.18). Entonces tenemos que:

(a) F'/F es una extensión cíclica de Galois de grado p. Los automorfismos de F'/F están dados por $\sigma(y) = y + \nu$, con $\nu = 0, 1, \ldots, p-1$.

(b) P es no ramificado en F'/F si y sólo si $m_P = -1$.

(c) P es totalmente ramificado en F'/F si sólo si $m_P > 0$. Denotemos por P' al único lugar de F' arriba de P. Entonces el exponente diferente $d(P'|P)$ está dado por

$$d(P'|P) = (p-1)(m_P - 1).$$

(d) Si al menos un lugar $Q \in \mathbb{P}(F)$ satisface $m_P > 0$, entonces K es algebraicamente cerrado en F' y

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

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

1.3. Torres de cuerpos de funciones

La construcción de cuerpos de funciones con una cantidad creciente de lugares racionales tiene un papel importante en la teoría algebraica de códigos, (ver [**Sti09**], [**TV91**]). En esta dirección, si denotamos por $N(F)$ al número de lugares racionales y por $g(F)$ al género de un cuerpo de funciones F/K, tenemos el siguiente resultado que fue probado primero por H. Hasse [**Has34**] en el caso $g(F) = 1$, y luego por A. Weil [**Wei48**] en el caso general.

Teorema 1.3.1. *Sea $F/\mathbb{F}_q$ un cuerpo de funciones sobre el cuerpo finito $\mathbb{F}_q$. Entonces*

$$|N(F) - (q+1)| \leq 2g(F)\sqrt{q}.$$

La desigualdad anterior se conoce como la cota de Hasse-Weil. Hay una mejora debida a Jean-Pierre Serre que establece que

$$|N(F) - (q+1)| \leq g(F)\lfloor 2\sqrt{q} \rfloor,$$

donde $\lfloor x \rfloor$ denota el piso del número real x, es decir, el mayor entero m tal que $m \leq x$.

Los cuerpos de funciones con muchos lugares racionales, obtuvieron mucha atención en temas relacionados con cuerpos de funciones globales luego de que Ihara [**Iha81**] introdujera la función

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

donde $N_q(g)$ es el máximo número de lugares racionales de un cuerpo de funciones sobre $\mathbb{F}_q$ con género g.

Drinfeld y Vladut [**VD83**] mostraron que $A(q) \leq \sqrt{q}-1$. Ihara, e independientemente Tsfasman, Vladut y Zink, mostraron que si q es un cuadrado entonces $A(q) = \sqrt{q} - 1$. Cuando q no es un cuadrado, el valor exacto de $A(q)$ no se conoce. Sin embargo, Serre [**Ser83**] probó que existe una constante $c > 0$ tal que $A(q) \geq c \cdot \log q$ para todo q. Zink [**Zin85**] probó que cuando $q = p^3$ es una potencia cúbica de un primo entonces

$$A(p^3) \geq \frac{2(p^2-1)}{p+2},$$

y más tarde, Garcia, Stichtenoth y Thomas [**GST97**] generalizaron este mismo resultado para cualquier potencia cúbica. Una manera de obtener cotas inferiores no triviales para la función de Ihara es a través de la construcción de torres de cuerpos de funciones asintóticamente buenas sobre $\mathbb{F}_q$ (Ver [**GS07**]).

Definición 1.3.2. Una *sucesión de cuerpos de funciones sobre un cuerpo perfecto* K es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre K de manera que se cumplan las siguientes propiedades:

(i) $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$, *y*

(ii) la extensión F_{i+1}/F_i es finita y separable para todo $i \geq 0$.

Si además se cumple que:

(iii) K es el cuerpo total de constantes de cada F_i; es decir, el cuerpo K debe ser algebraicamente cerrado en F_i para cada $i \geq 0$, *y*

(iv) el género satisface $g(F_i) \to \infty$ para $i \to \infty$;

entonces decimos que la sucesión $\mathcal{F}$ es un *torre de cuerpos de funciones sobre* K.

Observación 1.3.3 . La condición (iv) se obtiene de las condiciones (i), (ii) y de la siguiente condición que es levemente más débil:

(iv') existe $i_0 \geq 0$ tal que $g(F_{i_0}) > 1$.

En efecto, por la fórmula del género de Hurwitz, tenemos que

$$g(F_{i+1}) - 1 \geq [F_{i+1} : F_i](g(F_i) - 1) \qquad \forall\, i.$$

Como $g(F_{i_0}) > 1$ y $[F_{i+1} : F_i] > 1$, entonces

$$g(F_{i_0}) < g(F_{i_0+1}) < g(F_{i_0+2}) < \cdots,$$

y por lo tanto $g(F_i) \to \infty$ para $i \to \infty$.

Definición 1.3.4. Decimos que una sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre K es *recursiva* si existe una sucesión $\{x_i\}_{i=0}^{\infty}$ de elementos trascendentes sobre K y un polinomio (separable)

$$f(x, y) \in K[x, y],$$

tales que

(i) $F_0 = K(x_0)$;

(ii) $F_{i+1} = F_i(x_{i+1})$ donde x_{i+1} es un cero de $f(x_i, y) \in \mathbb{F}_q[y]$, es decir, $f(x_i, x_{i+1}) = 0$ para $i \geq 0$.

Asociado a una sucesión recursiva $\mathcal{F} = (F_0, F_1, F_1, \ldots)$ de cuerpos de funciones F_i sobre K tenemos el denominado *cuerpo de funciones básico* $K(x, y)$ donde x es trascendente sobre K y $f(x, y) = 0$.

En general, trabajaremos con sucesiones recursivas $\mathcal{F}$ sobre $\mathbb{F}_q$ donde $f(x, y)$ es de la forma

$$f(x, y) := a_1(y)b_2(x) - a_2(y)b_1(x),$$

con $a_1(T)$, $a_2(T)$, $b_1(T)$ y $b_2(T) \in \mathbb{F}_q[T]$ tales que

$$\text{mcd}(a_1, a_2) = \text{mcd}(b_1, b_2) = 1.$$

En este caso diremos que $\mathcal{F}$ es una sucesión recursiva de cuerpos de funciones sobre $\mathbb{F}_q$ de tipo (a, b), o simplemente una sucesión recursiva de tipo (a, b), para hacer referencia a las funciones racionales

$$a(T) := \frac{a_1(T)}{a_2(T)} \qquad \text{y} \qquad b(T) := \frac{b_1(T)}{b_2(T)},$$

que generan la sucesión.

Otra manera usual de hacer referencia a esta situación es decir que la ecuación

$$a(y) = b(x)$$

define una sucesión recursiva $\mathcal{F} = (F_0, F_1, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$.

Notar que de la definición de sucesión recursiva tenemos que cada extensión F_{i+1}/F_i es finita, pues $[F_{i+1} : F_i] \leq deg\, _T(f(x_i, T))$. Además

$$F_i = K(x_0, \ldots, x_i) \qquad \text{para } i \geq 0,$$

y por lo tanto

$$F_0 = K(x_0) \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots .$$

Entonces para probar que una sucesión recursiva de cuerpos de funciones sobre K es una torre basta que mostrar que:

(i) K es el cuerpo total de constantes de todos los F_i.

(ii) $g(F_{i_0}) > 1$ para algún i_0.

La siguiente proposición de [**Sti09**, Proposición 7.2.15] da condiciones suficientes para que ocurra (i).

Proposición 1.3.5. *Consideremos una sucesión recursiva de cuerpos de funciones $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ donde F_0 es un cuerpo de funciones con cuerpo total de constantes K y $[F_{i+1} : F_i] < \infty$ para todo $i \geq 0$. Supongamos que para todo i existen lugares $P_i \in \mathbb{P}(F_i)$ y $Q_i \in \mathbb{P}(F_{i+1})$ con $Q_i|P_i$ e índice de ramificación $e(Q_i|P_i) > 1$. Entonces $F_i \subsetneq F_{i+1}$.*

Más aún, si suponemos que $e(Q_i|P_i) = [F_{i+1} : F_i]$ para todo i, entonces K es el cuerpo total de constantes de F_i para todo $i \geq 0$.

Si una sucesión recursiva $\mathcal{F}$ es una torre decimos que $\mathcal{F}$ es una *torre recursiva* (de cuerpos de funciones sobre K).

Definición 1.3.6. Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una sucesión de cuerpos de funciones sobre K.

(a) Decimos que un lugar $P \in \mathbb{P}(F_i)$ se *descompone completamente* en $\mathcal{F}$ si P se descompone completamente en cada extensión F_j/F_i, para $j > i$. El *espacio de descomposición* de $\mathcal{F}$ sobre F_0 está definido por

$$Split(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) \,:\, deg\, P = 1 \text{ y } P \text{ se descompone completamente en } \mathcal{F}\}.$$

(b) Decimos que un lugar $P \in \mathbb{P}(F_i)$ *ramifica* en $\mathcal{F}$ si P ramifica en alguna extensión F_i/F_0, para $i > 0$. El *espacio de ramificación* de $\mathcal{F}$ sobre F_0 está definido por

$$Ram(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) \,:\, P \text{ ramifica en } \mathcal{F}\}.$$

(c) Un lugar $P \in \mathbb{P}(F_i)$ está *totalmente ramificado* en $\mathcal{F}$ si P está totalmente ramificado en cada extensión F_j/F_i, para $j > i$. El *espacio de ramificación completa* (o *espacio de ramificación total*) de $\mathcal{F}$ sobre F_0 se define como

$$Cram(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : deg\, P = 1 \text{ y } P \text{ es totalmente ramificado en } \mathcal{F}\}.$$

Cuando $K = \mathbb{F}_q$ uno de los problemas principales de esta teoría es la determinación precisa del número $N(F_i)$ de lugares racionales de F_i y del género $g(F_i)$ para cada $i \geq 0$ de una sucesión o torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ dada.

Las siguientes definiciones son importantes al abordar el problema anterior.

Definición 1.3.7. Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$. La *tasa de descomposición* $\nu(\mathcal{F}/F_0)$ y el *género* $\gamma(\mathcal{F}/F_0)$ de $\mathcal{F}$ sobre F_0 se definen, respectivamente, como

$$\nu(\mathcal{F}/F_0) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}, \qquad \gamma(\mathcal{F}/\mathbb{F}_0) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}.$$

Si $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$, el *límite* $\lambda(\mathcal{F})$ de $\mathcal{F}$ está definido como

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

Se puede probar que la sucesión $\{N(F_i)/[F_i : F_0]\}_{i\geq 0}$ es monótonamente decreciente y que la sucesión $\{(g(F_i)-1)/[F_i : F_0]\}_{i\geq 0}$ es monótonamente creciente, por lo tanto ambas convergen en $\mathbb{R}^{\geq 0} \cup \{\infty\}$. Luego los límites anteriores existen (en $\mathbb{R} \cup \{\infty\}$) y tenemos que $0 \leq \nu(\mathcal{F}/F_0) < \infty$, $0 < \gamma(\mathcal{F}/F_0) \leq \infty$, y, por la definición de $A(q)$,

$$0 \leq \lambda(\mathcal{F}) \leq A(q), \tag{1.3.1}$$

para cualquier sucesión $\mathcal{F}$ con $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$, para algún i_0 (ver [**Sti09**, Capítulo 7]).

Notar que la definición del género de $\mathcal{F}$ tiene sentido incluso en el caso de una sucesión $\mathcal{F}$ de cuerpos de funciones sobre un cuerpo perfecto K.

Definición 1.3.8 . Una sucesión $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es *asintóticamente buena* si $\nu(\mathcal{F}/F_0) > 0$ y $\gamma(\mathcal{F}/F_0) < \infty$. Si no es asintóticamente buena se dice que $\mathcal{F}$ es *asintóticamente mala*. Por lo tanto,una sucesión $\mathcal{F}$ es asintóticamente mala si $\nu(\mathcal{F}/F_0) = 0$ o si $\gamma(\mathcal{F}/F_0) = \infty$.

Como vimos antes, la condición $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$ implica $g(F_i) \to \infty$ cuando $i \to \infty$. Por lo tanto, cuando hablamos del límite de una sucesión $\lambda(\mathcal{F})$ en realidad estamos hablando del límite de una torre.

Es claro que en el caso de una torre $\mathcal{F}$ tenemos que $\mathcal{F}$ es asintóticamente buena si y sólo si $\lambda(\mathcal{F}) > 0$. Por lo tanto una torre $\mathcal{F}$ es asintóticamente mala si y sólo si $\lambda(\mathcal{F}) = 0$. Si $\lambda(\mathcal{F}) = A(q)$, donde $A(q)$ es la función de Ihara, decimos que $\mathcal{F}$ es *asintóticamente óptima*.

Notar que una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ puede ser asintóticamente buena pero podría no ser una torre.

1.4. Construyendo torres de cuerpos de funciones

Como mencionamos en la Introducción de esta Tesis, un problema importante en la teoría de códigos algebraicos es el cálculo de $A(q)$. De la desigualdad (1.3.1) vemos que se pueden conseguir cotas inferiores de $A(q)$ calculando, o al menos estimando, el límite $\lambda(\mathcal{F})$ de torres recursivas de cuerpos de funciones sobre $\mathbb{F}_q$. El primer problema a resolver es que la ecuación que define recursivamente a una sucesión sea una torre. En esta Sección estudiaremos condiciones suficientes para que una ecuación de la forma $a(y) = b(x)$ defina una torre recursiva de cuerpos de funciones sobre $\mathbb{F}_q$.

Usando propiedades básicas de las valuaciones en un cuerpo de funciones el siguiente lema es inmediato.

Lema 1.4.1. *Sean F/K un cuerpo de funciones sobre K, $x \in F$ un elemento trascendente sobre K y $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ un polinomio de grado n. Supongamos además que $i \in \{0, 1, \ldots, n\}$ es el menor índice tal que $a_i \neq 0$. Entonces, si*

P es un lugar de F, tenemos que

$$v_P(f(x)) = \begin{cases} v_P(a_i x^i) = i v_P(x) & \text{si } v_P(x) > 0; \\ v_P(a_n x^n) = n v_P(x) & \text{si } v_P(x) < 0. \end{cases}$$

Si $v_P(x) = 0$ entonces $v_P(f(x)) \geq 0$.

Corolario 1.4.2 . *Con las condiciones del lema anterior tenemos que si $v_P(x) \geq 0$ entonces $v_P(f(x)) \geq 0$ y si $v_P(x) < 0$ entonces $v_P(f(x)) < 0$.*

Definición 1.4.3. Sea x un elemento trascendente sobre un cuerpo K. Consideremos el cuerpo de funciones racionales $K(x)$ sobre K. Para $\alpha \in K$, denotamos por $P_{x-\alpha}$ al único lugar de $K(x)$ que es un cero de $x - \alpha$. De la misma manera, denotamos por P_∞ al único polo de x en $K(x)$.

Teorema 1.4.4 . *Sea K un cuerpo perfecto y sean $a(T), b_1(T), b_2(T) \in K[T]$ polinomios coprimos dos a dos. Supongamos que $\deg(a(T)) = \deg(b_1(T)) = m \geq 2$ y que $\deg(b_2(T)) = m - r$ con $\mathrm{mcd}(m, r) = 1$. Consideremos los siguientes cuerpos de funciones definidos de manera recursiva:*

$$F_0 = K(x_0) \text{ es el cuerpo de funciones racionales sobre } K;$$
$$F_{i+1} = F_i(x_{i+1}) \text{ con } a(x_{i+1}) = b_1(x_i)/b_2(x_i) \text{ para todo } i \geq 0.$$

Entonces $\mathcal{F} = (F_0, F_1, \ldots)$ es una sucesión recursiva de cuerpos de funciones sobre K. Más aún, se cumple que:

(i) *$F_i \subsetneq F_{i+1}$.*

(ii) *El lugar P_∞, que es el único polo de x_0 en F_0, es totalmente ramificado en la sucesión. En consecuencia, K es el cuerpo total de constantes de F_i para todo $i \geq 0$.*

Si, además, $a(T) - \frac{b_1(x_i)}{b_2(x_i)}$ es separable en F_i para todo $i \geq 0$, entonces F_{i+1}/F_i es separable para todo $i \geq 0$.

Demostración. Sea x_0 un elemento trascendente sobre K. Sea $F_0 = K(x_0)$ el cuerpo de funciones racionales y para cada $i \geq 0$ sea $F_{i+1} = F_i(x_i)$ donde

$$a(x_{i+1}) = b_1(x_i)/b_2(x_i).$$

Claramente, tenemos que $F_0 \subset F_1 \subset F_2 \subset \cdots$.

Veamos ahora que el lugar $P = P_\infty$, que es un polo de la función x_0 en F_0, es totalmente ramificado en todas las extensiones.

Sea Q un lugar de F_1 tal que $Q|P$. Como P es un polo de x_0 sabemos que $v_P(x_0) < 0$. Más aún, tenemos que $v_P(x_0) = -1$ (pues el grado del divisor de polos de la función x_0 satisface $deg\,(x_0)_\infty = [F_0 : K(x_0)] = [K(x_0) : K(x_0)] = 1$ y por lo tanto x_0 tiene sólo un polo simple).

Entonces por el Lema 1.4.1 tenemos que $v_P(b_1(x_0)) = m v_P(x_0) = -m$ y $v_P(b_2(x_0)) = (m-r)v_P(x_0) = -(m-r)$. Luego

$$v_P\left(\frac{b_1(x_0)}{b_2(x_0)}\right) = v_P(b_1(x_0)) - v_P(b_2(x_0)) = -m + (m-r) = -r.$$

Ahora, como sabemos que x_0 y x_1 verifican $a(x_1) = b_1(x_0)/b_2(x_0)$ y $Q|P$ entonces tenemos que

$$v_Q(a(x_1)) = e(Q|P)v_P\left(\frac{b_1(x_0)}{b_2(x_0)}\right) = -r\,e(Q|P) \leq -1.$$

Si $v_Q(x_1) \geq 0$, el Corolario 1.4.2 nos dice que $v_Q(a(x_1)) \geq 0$ lo que contradice la desigualdad anterior. Luego $v_Q(x_1) < 0$ y, nuevamente por el Lema 1.4.1, tenemos que $v_Q(a(x_1)) = m\,v_Q(x_1)$.

Entonces,

$$m\,v_Q(x_1) = v_Q(a(x_1)) = e(Q|P)v_P\left(\frac{b_1(x_0)}{b_2(x_0)}\right) = -r\,e(Q|P)$$

y como $\mathrm{mcd}(m, r) = 1$ tenemos que $m|e(Q|P)$. Pero como $e(Q|P) \leq [F_1 : F_0] \leq m$ debe ser que $e(Q|P) = m$ y, más aún, $v_Q(x_1) = -r$, es decir, Q es un polo simple de la función x_1.

Hemos demostrado que $[F_1 : F_0] = m$ y que el lugar Q es el único lugar de F_1 arriba de P, es decir, el lugar P de F_0 es totalmente ramificado en F_1/F_0. Supongamos ahora que para $k \geq 1$ tenemos que $[F_k : F_0] = m^k$ y que existe un único lugar, $P_k \in \mathbb{P}(F_k)$ tal que $e(P_k|P) = m^k$ y $v_{P_k}(x_k) = -r^k$. Sea $P_{k+1} \in \mathbb{P}(F_{k+1})$ tal que $P_{k+1}|P_k$. Entonces como $a(x_{k+1}) = \frac{b_1(x_k)}{b_2(x_k)}$ tenemos que

$$v_{P_{k+1}}(a(x_{k+1})) = e(P_{k+1}|P_k)v_{P_k}\left(\frac{b_1(x_k)}{b_2(x_k)}\right)$$

$$= e(P_{k+1}|P_k)[m\, v_{P_k}(x_k) - (m-r)v_{P_k}(x_k)]$$
$$= -r^{k+1}e(P_{k+1}|P_k) < 0.$$

Entonces debe ser que $v_{P_{k+1}}(x_{k+1}) < 0$ y por lo tanto

$$m\, v_{P_{k+1}}(x_{k+1}) = -r^{k+1}e(P_{k+1}|P_k)$$

y como $\mathrm{mcd}(m, r) = 1$, tenemos que $e(P_{k+1}|P_k) = m$ y que $v_{P_{k+1}}(x_{k+1}) = -r^{k+1}$.

Por lo tanto, hemos probado por inducción que $[F_{i+1} : F_i] = m$ y que el lugar P es totalmente ramificado en todas las extensiones F_{i+1}/F_i para todo $i \geq 0$.

Finalmente, como $a(T) - b_1(x_i)/b_2(x_i)$ es separable, las extensiones F_{i+1}/F_i son separables para todo $i \geq 0$. □

Observación 1.4.5. Si en el Teorema 1.4.4 tenemos que $a(T) = T^m$, $deg\,(b_1(T)) = m-r$ y $deg\,(b_2(T)) = m \geq 2$ con $\mathrm{mcd}(m, r) = 1$, entonces se prueba al igual que en el teorema, que el polo de x_n en F_n es totalmente ramificado en F_{n+1} y por lo tanto también se obtiene que K es el cuerpo total de constantes de F_n para todo $n \geq 0$.

Corolario 1.4.6. *Sea K un cuerpo perfecto y sean $a(T), b_1(T), b_2(T) \in K[T]$ polinomios coprimos dos a dos con $deg\,(a(T)) = deg\,(b_1(T)) = m$, $deg\,(b_2(T)) = m-r$ y $\mathrm{mcd}(m, r) = 1$. Supongamos que $b_2(T)$ tiene la siguiente descomposición en el anillo de polinomios $\bar{K}[T]$:*

$$b_2(T) = \prod_{i=1}^{s}(T - \alpha_i)^{\varepsilon_i}$$

donde $\alpha_i \in \bar{K}$ son distintos dos a dos y $\varepsilon_i \in \mathbb{N}$ para todo $i = 1, \ldots, s$. Consideremos los siguientes cuerpos de funciones definidos de manera recursiva:

$$F_0 = K(x_0) \text{ es el cuerpo de funciones racionales sobre } K;$$
$$F_{i+1} = F_i(x_{i+1}) \text{ con } a(x_{i+1}) = b_1(x_i)/b_2(x_i) \text{ para todo } i \geq 0.$$

Supongamos además que $a(T) - \frac{b_1(x_i)}{b_2(x_i)}$ es separable en F_i para todo $i \geq 0$. Si alguna de las siguientes condiciones vale:

Hip. A) *$b_2(T)$ separable y $1 \leq r \leq m-2$;*

Hip. B) *$m = p$ es un número primo y $s \geq 2$;*

entonces $\mathcal{F} = (F_0, F_1, \ldots)$ *es una torre recursiva de cuerpos de funciones sobre* K.

Demostración. Como se cumplen las hipótesis del Teorema 1.4.4, sólo tenemos que probar que $g(F_{i_0}) > 1$ para algún $i_0 > 0$. Tenemos que

$$b_2(T) = \prod_{i=1}^{s} (T - \alpha_i)^{\varepsilon_i}$$

con $\alpha_i \in \bar{K}$ y $\varepsilon_i \in \mathbb{N}$. Sea $P_j \in \mathbb{P}(\bar{K}(x))$ el cero de $x - \alpha_j$ para algún $0 \leq j \leq s$. Entonces como $b_1(T)$ y $b_2(T)$ son coprimos y los α_i son distintos dos a dos tenemos que

$$v_{P_j}\left(\frac{b_1(x)}{b_2(x)}\right) = -\varepsilon_j.$$

Sea $Q_j \in \mathbb{P}(\bar{K}(x,y))$ tal que $Q_j | P_j$. Entonces

$$\begin{aligned} v_{Q_j}(a(y)) &= e(Q_j|P_j) v_{P_j}\left(\frac{b_1(x)}{b_2(x)}\right) \\ &= (-\varepsilon_j) e(Q_j|P_j). \end{aligned}$$

Tenemos entonces que si $v_{Q_j}(y) \geq 0$, por el Lema 1.4.1, $v_{Q_j}(a(y)) \geq 0$, lo que conduce a un absurdo ya que $v_{Q_j}(a(y)) = (-\varepsilon_j) e(Q_j|P_j) < 0$. Por lo tanto $v_{Q_j}(y) < 0$, y en este caso

$$v_{Q_j}(a(y)) = m\, v_{Q_j}(y).$$

Luego,

$$m\, v_{Q_j}(y) = (-\varepsilon_j) e(Q_j|P_j)$$

y entonces

$$m | (-\varepsilon_j) e(Q_j|P_j).$$

Ahora miramos dos casos. Si se cumple que $b_2(T)$ es separable, entonces $\varepsilon_i = 1$ para todo i y $s = m - r$. Luego, $m | e(Q_j|P_j)$ y como $e(Q_j|P_j) \leq [\bar{K}(x,y) : \bar{K}(x)] = m$, entonces $e(Q_j|P_j) = m$. Por otro lado, si se cumple que $m = p$ primo, entonces tenemos que $m | \varepsilon_j$ o $m | e(Q_j|P_j)$. Pero como $\varepsilon_j \leq s \leq m - r$ entonces $m \nmid \varepsilon_j$ y tenemos, también en este caso, que $e(Q_j|P_j) = m$.

En ambos casos, tenemos que para cada $i = 1, \ldots, s$ el lugar P_i es totalmente ramificado y por el Teorema del diferente de Dedekind, el exponente diferente satisface $d(Q_j|P_j) \geq e(Q_j|P_j) - 1 = m - 1$. Utilizando el hecho de que el cuerpo de funciones

racionales tiene género cero, la fórmula del género de Hurwitz y denotando con P_∞ al polo de x_0 en F_0 y con Q_∞ al único lugar de F_1 arriba de P_∞ tenemos que

$$\begin{aligned} 2g(F_1) - 2 &= \frac{[F_1 : F_0]}{[\bar{K} : \bar{K}]}(2g(F_0) - 2) + deg\ \mathrm{Diff}(F_1/F_0) \\ &\geq m(-2) + \left(\sum_{i=1}^{s}(deg\, Q_i\, d(Q_i|P_i)) + deg\, Q_\infty\, d(Q_\infty|P_\infty)\right) \\ &= m(-2) + \sum_{i=1}^{s}(m-1) + m - 1 \\ &= m(-2) + (s+1)(m-1), \end{aligned}$$

por lo tanto

$$g(F_1) \geq \frac{(m-1)(s-1)}{2}.$$

Nuevamente, separando los casos, tenemos que si se cumple la primera hipótesis, entonces $s = m - r$ y $g(F_1) \geq \frac{(m-1)(m-r-1)}{2}$. Por lo tanto, como $1 \leq r \leq m-2$, $g(F_1) \geq 1$. Si se cumple la segunda hipótesis, tenemos que $s \geq 2$ y por lo tanto, $g(F_1) \geq 1$.

En ambos casos, como el lugar P_∞ es totalmente ramificado en la torre, tenemos que para la extensión F_2/F_1,

$$2g(F_2) \geq m(2g(F_1) - 2) + (m-1) + 2 \geq \frac{(m-1)+2}{2}$$

y por lo tanto $g(F_2) \geq 2$.

Luego, la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ es una torre recursiva de cuerpos de funciones sobre K. □

Corolario 1.4.7. *Sean $b_1(T), b_2(T) \in K[T]$ polinomios coprimos dos a dos de manera que $deg\,(b_1(T)) = m \geq 2$, $deg\,(b_2(T)) = m - r$ y $\mathrm{mcd}(m, r) = 1$. Supongamos que $b_1(T)$ y $b_2(T)$ tiene las siguientes descomposiciones en el anillo de polinomios $\bar{K}[T]$:*

$$b_1(T) = C\prod_{i=1}^{k}(T - \beta_i)^{\delta_i} \qquad y \qquad b_2(T) = \prod_{i=1}^{s}(T - \alpha_i)^{\varepsilon_i}$$

donde $C \in K$, β_i, $\alpha_i \in \bar{K}$ *son distintos dos a dos y* δ_i, $\varepsilon_i \in \mathbb{N}$ *para todo* i. *Consideremos los cuerpos de funciones definidos de manera recursiva por:*

$$F_0 = K(x_0) \text{ es el cuerpo de funciones racionales sobre } K;$$
$$F_{i+1} = F_i(x_{i+1}) \text{ con } x_{i+1}^m = b_1(x_i)/b_2(x_i) \text{ para todo } i \geq 0.$$

Supongamos además que $T^m - \frac{b_1(x_i)}{b_2(x_i)}$ *es separable en* F_i *para todo* $i \geq 0$ *y que* $s + k \geq m$ *con* $k \geq 2$. *Entonces* $\mathcal{F} = (F_0, F_1, \ldots)$ *es una torre recursiva de cuerpos de funciones sobre* K.

Demostración. Como se cumplen las hipótesis del Teorema 1.4.4, sólo tenemos que probar que $g(F_{i_0}) > 1$ para algún $i_0 > 0$. Como en la prueba del teorema anterior, tenemos que si $P_j \in \mathbb{P}(\bar{K}(x))$ es el cero de $x - \alpha_j$ para algún $0 \leq j \leq s$ y $Q_j \in \mathbb{P}(\bar{K}(x, y))$ es tal que $Q_j | P_j$ entonces

$$m\, v_{Q_j}(y) = -\varepsilon_j\, e(Q_j|P_j).$$

Como $m \nmid \varepsilon_j$ entonces $e(Q_j|P_j) \geq 2$.

De manera similar, tenemos que si $R_j \in \mathbb{P}(\bar{K}(x))$ es el cero de $x - \beta_j$ para algún $0 \leq j \leq k$ y $S_j \in \mathbb{P}(\bar{K}(x, y))$ es tal que $S_j | R_j$ entonces

$$m\, v_{S_j}(y) = \delta_j\, e(S_j|R_j);$$

y como $m \nmid \delta_j$ entonces $e(S_j|R_j) \geq 2$.

En ambos casos tenemos que, por el Teorema del diferente de Dedekind, el exponente diferente satisface $d(Q_j|P_j) \geq e(Q_j|P_j) - 1 \geq 1$ para todo $j = 1, \ldots, s$ y $d(S_j|R_j) \geq e(S_j|R_j) - 1 \geq 1$ para todo $j = 1, \ldots, k$. Entonces utilizando la fórmula del género de Hurwitz y denotando con P_∞ al polo de x_0 en F_0 y con Q_∞ al único lugar de F_1 arriba de P_∞ tenemos que

$$\begin{aligned} 2g(F_1) - 2 &= \frac{[F_1 : F_0]}{[\bar{K} : \bar{K}]}(2g(F_0) - 2) + deg\ \mathrm{Diff}(F_1/F_0) \\ &\geq m(-2) + \left(\sum_{i=1}^{s} 1 + \sum_{i=1}^{k} 1 + d(Q_\infty|P_\infty) \right) \\ &= m(-2) + s + k + m - 1 \\ &= s + k - m - 1, \end{aligned}$$

y por lo tanto

$$g(F_1) \geq \frac{s+k-m+1}{2}.$$

Ahora, como el lugar P_∞ es totalmente ramificado en la torre, tenemos que, para la extensión F_2/F_1,

$$2g(F_2) \geq m(2g(F_1)-2)+(m-1)+2 \geq \frac{(m-1)+2}{2}$$

y por lo tanto $g(F_2) \geq 2$.

Luego, la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ es una torre recursiva de cuerpos de funciones sobre K.

□

Ejemplo 1.4.8. Si $\text{mcd}(m,p) = 1$ donde $p = char\, \mathbb{F}_q$ entonces la ecuación

$$y^m = \frac{x^m - \alpha}{\beta x^{m-r}}$$

con $\text{mcd}(m,r) = 1$ y $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$ define una torre recursiva de cuerpos de funciones sobre $\mathbb{F}_q$.

A continuación damos algunos ejemplos de ecuaciones que cumplen las condiciones de los resultados que hemos demostrado. Estas ecuaciones definen torres que han sido importantes en el desarrollo de la teoría de torres recursivas.

Ejemplo 1.4.9. La torre de cuerpos de funciones definida sobre $\mathbb{F}_8$ por la ecuación

$$y^2 + y = \frac{x^2+x+1}{x},$$

considerada por van der Geer y van der Vlugt en [**vdGvdV02**]. Esta es una torre asintóticamente buena cuyo límite fue calculado exactamente y es 3/2.

Ejemplo 1.4.10. La torre de cuerpos de funciones sobre $\mathbb{F}_{p^2}$ (p primo impar) definida recursivamente por la ecuación

$$y^2 = \frac{x^2+1}{2x},$$

fue estudiada por Garcia, Stichtenoth y Rück en [**GSR03**]. Esta ecuación define una torre asintóticamente buena sobre $\mathbb{F}_{q^2}$ y óptima sobre $\mathbb{F}_{p^2}$.

Ejemplo 1.4.11. La torre de cuerpos de funciones sobre $\mathbb{F}_{q^2}$ definida recursivamente por la ecuación

$$y^q + y = \frac{x^q}{x^{q-1}+1},$$

fue estudiada por Garcia y Stichtenoth en [**GS96**]. Esta ecuación define una torre óptima sobre $\mathbb{F}_{q^2}$.

En el Capítulo 3 daremos más ejemplos de torres asintóticamente buenas.

CAPÍTULO 2

LUGARES RACIONALES

En este Capítulo demostraremos resultados sobre la cantidad de lugares racionales en extensiones simples y sucesiones de cuerpos de funciones sobre cuerpos finitos. Damos condiciones suficientes para obtener cotas no triviales en cada paso de una sucesión, y en particular, para el caso de extensiones y sucesiones de tipo Kummer. Además aplicamos los resultados obtenidos para estimar el número de lugares racionales en una familia de sucesiones de cuerpos de funciones de tipo Kummer sobre cuerpos primos.

En la primera Sección probamos un resultado sobre el número de lugares racionales en ciertas extensiones simples de cuerpos de funciones que será utilizado luego para el caso de sucesiones de cuerpos de funciones. Como aplicación, damos dos ejemplos de extensiones de tipo Kummer sobre cuerpos primos tales que el número de lugares racionales es $N_p(g)$.

En la segunda Sección trabajamos con sucesiones recursivas de tipo (a, b) sobre cuerpos finitos, donde a y b son funciones racionales. En uno de los resultados principales del presente Capítulo (Teorema 2.2.1) obtenemos una cota no trivial para el número de lugares racionales en cada paso de una sucesión recursiva de tipo (a, b) sobre el cuerpo $\mathbb{F}_q$, para a y b satisfaciendo ciertas condiciones.

En la tercera Sección, mostramos varios ejemplos. Entre ellos, mostramos que algunas cotas inferiores para $N(F_i)$ conocidas para ciertas sucesiones debidas a Garcia et al. [**GSR03**] y a van der Geer y van deer Vlugt [**vdGvdV**] se pueden deducir del Teorema 2.2.1.

Finalmente en la Sección cuarta nos concentramos en el interesante caso de cuerpos primos, aplicando los resultados de las secciones anteriores para construir sucesiones de tipo Kummer sobre $\mathbb{F}_p$ para todo p primo con cotas inferiores no triviales para $N(F_i)$.

A lo largo del Capítulo usaremos la siguiente notación: para cualquier polinomio mónico e irreducible $f(x) \in \mathbb{F}_q[x]$ denotamos por $P_{f(x)}$ al lugar racional de $\mathbb{F}_q(x)$ correspondiente al polinomio $f(x)$. Además, si P es un lugar de F escribimos v_P para denotar la valuación discreta inducida por P en F y v_∞ para denotar la valuación discreta inducida por el lugar infinito P_∞ de $\mathbb{F}_q(x)$.

Sea $F/\mathbb{F}_q$ un cuerpo de funciones. A lo largo del presente Capítulo asumiremos que $\mathbb{F}_q$ es el cuerpo total de constantes de F. Denotaremos por $\mathbb{P}_n(F)$ al conjunto de lugares de F de grado n.

2.1. Extensiones de cuerpos de funciones

En esta Sección probaremos ciertos resultados sobre la cantidad de lugares racionales en extensiones simples de cuerpos de funciones que serán útiles en el caso de sucesiones de cuerpos de funciones.

El siguiente resultado es una consecuencia directa del Teorema de Kummer y del Criterio de Irreducibilidad de Eisenstein (Teorema 1.2.8 y Proposición 1.2.6 del Capítulo 1, respectivamente) para cuerpos de funciones.

Proposición 2.1.1. *Sea $F/\mathbb{F}_q$ un cuerpo de funciones. Supongamos que existen polinomios $a_1(T)$ y $a_2(T) \in \mathbb{F}_q[T]$ y un elemento $u \in F$ tales que el polinomio*

$$\sigma(T) := a_1(T) - a_2(T)u \in F[T],$$

es mónico e irreducible en $F[T]$. Consideremos la extensión

$$F' := F(y) \qquad \text{donde} \qquad \sigma(y) = 0.$$

Para $P \in \mathbb{P}(F)$ y $u \in \mathcal{O}_P$ definimos

$$\overline{\sigma}_P(T) := a_1(T) - a_2(T)u(P),$$

que es un polinomio con coeficientes en el cuerpo de clases residuales $\mathcal{O}_P/P = \mathbb{F}_{q^r}$*, donde* $r = deg\,(P)$*. Sean*

$$S_1 = \{P \in \mathbb{P}(F) : v_P(u) \geq 0\},$$

$$S_2 = \{P \in \mathbb{P}(F) : \overline{\sigma}_P(T) \text{ es separable}\},$$

$$S_3 = \{P \in \mathbb{P}(F) : \overline{\sigma}_P(T) \text{ no es separable}\}.$$

Sea $S = S_1 \cap S_2 \cap \mathbb{P}_1(F)$ *y supongamos que* $S \neq \emptyset$*. Para* $P \in S$ *sea* L_P *el número de factores lineales en la factorización de* $\bar{\sigma}_P(T)$ *en* $\mathbb{F}_q[T]$*. Entonces*

(i) *Todos los lugares ramificados de* F *en* F' *están en* $(S_1 \cap S_3) \cup \{$*polos de* u *en* $F\}$*.*

(ii) $N(F') \geq \sum_{P \in S} L_P$*.*

(iii) *Supongamos que* $a_2(T) = 1$*. Si un polo* P *de* u *es tal que* $\text{mcd}(deg\,(\sigma), v_P(u)) = 1$ *entonces* $\mathbb{F}_q$ *es el cuerpo total de constantes de* F'*. Más aún, si* $P_1, \ldots, P_n$ *son polos de* u *en* F *tales que*

$$\text{mcd}(deg\,(\sigma), v_{P_i}(u)) = 1 \quad \text{para } 1 \leq i \leq n,$$

entonces

$$N(F') \geq n + \sum_{P \in S} L_P.$$

(iv) *Sea* $a(y) := a_1(y)/a_2(y)$*. Si* $deg\,(\sigma) | v_Q(a(y))$ *y* $\text{mcd}(deg\,(\sigma), v_P(u)) = 1$ *para los* $Q \in \mathbb{P}(F')$ *arriba de* $P \in \mathbb{P}(F)$*, entonces* P *es totalmente ramificado en* F'*. Sea* S_4 *(resp.* S_5*) el conjunto de lugares* $P \in \mathbb{P}(F) \setminus (S_1 \cap S_2)$ *tales que para cada* $Q \in \mathbb{P}(F')$ *arriba de* P *se tenga que* $deg\,(\sigma) | v_Q(a(y))$ *y* $\text{mcd}(deg\,(\sigma), v_P(u)) = 1$ *(resp.* $\text{mcd}(deg\,(\sigma), v_P(u)) \neq 1$*). Si* $\mathbb{P}(F) \setminus (S_1 \cap S_2) = S_4 \cup S_5$ *entonces*

$$N(F') = |\mathbb{P}_1(F) \cap S_4| + N + \sum_{P \in S} L_P,$$

donde N *es el número de lugares racionales de* F' *arriba de algún lugar de* $\mathbb{P}_1(F) \cap S_5$*.*

Demostración. Sea $P \in S_1$. Entonces $\sigma(T) \in \mathcal{O}_P[T]$ y por la Proposición 1.2.7 del Capítulo 1 tenemos que y es integral sobre $\mathcal{O}_P$. Como $a_1(T)$ y $a_2(T) \in \mathbb{F}_q[T]$ tenemos que

$$\overline{\sigma}_P(T) = \sigma(T) \quad \text{mód } P.$$

Dado que $\mathbb{F}_{q^r}$ es el cuerpo de clases residuales de P, entonces $\overline{\sigma}_P(T)$ se descompone en factores irreducibles distintos dos a dos en $\mathbb{F}_{q^r}$ cuando $P \in S_2$, y como

$$\mathbb{P}(F) = (S_1 \cap S_2) \cup (S_1 \cap S_3) \cup \{\text{polos de } u \text{ en } F\}, \tag{2.1.1}$$

y esta unión es disjunta dos a dos, vemos que (i) y (ii) siguen del Teorema de Kummer.

Supongamos ahora que $a_2(T) = 1$ y sea P un polo de u en F tal que $\mathrm{mcd}(deg\,(\sigma), v_P(u)) = 1$. Dado que $a_1(T) \in \mathbb{F}_q[T] \subset \mathcal{O}_P[T]$ y que

$$\mathrm{mcd}(deg\,(\sigma), v_P(a_1(0) - u)) = \mathrm{mcd}(deg\,(\sigma), v_P(u)) = 1,$$

entonces se puede aplicar el Criterio de Irreducibilidad de Eisenstein para obtener que P es totalmente ramificado en F'. Luego, hay exactamente un lugar racional de F' arriba de P y por lo tanto la igualdad en (iii) vale. El mismo argumento usado en el Corolario 1.2.15 del Capítulo 1 muestra que $\mathbb{F}_q$ es el cuerpo total de constantes del cuerpo F'.

Finalmente supongamos que $P \in S_4$. Entonces para cualquier $Q \in \mathbb{P}(F')$ arriba de P tenemos que $\mathrm{mcd}(deg\,(\sigma), v_P(u)) = 1$. Como $a(y) = u$, $deg\,(\sigma) | v_Q(a(y))$ y $v_Q(a(y)) = e(Q|P)v_P(u)$ entonces tenemos que $e(Q|P) = deg\,(\sigma)$ y por lo tanto, P es totalmente ramificado en F'. Usando (2.1.1) tenemos que

$$\mathbb{P}_1(F) = S \cup (\mathbb{P}_1(F) \cap S_4) \cup (\mathbb{P}_1(F) \cap S_5),$$

es una unión disjunta de a pares. Luego, (iv) vale. □

El item (iv) de la Proposición 2.1.1 se aplica bien al caso particular de una extensión de tipo Kummer F'/F de un cuerpo de funciones $F/\mathbb{F}_q$ dado. Esto significa que existe un elemento y algebraico sobre F tal que $F' = F(y)$ y el polinomio mínimo de y sobre F es de la forma $T^m - u \in F[T]$ para algún entero $m \geq 2$ con $\mathrm{mcd}(m, q) = 1$.

Proposición 2.1.2 . *Sean $F/\mathbb{F}_q$ un cuerpo de funciones, $m \geq 2$ un entero tal que $\mathrm{mcd}(m, q) = 1$ y $u \in F$ tal que $\mathrm{mcd}(m, v_P(u)) = 1$ para algún lugar P de F. Sean S y S_i para $i = 1, 2, 3, 4, 5$ los conjuntos de lugares de F definidos en la Proposición 2.1.1. Sea $F' = F(y)$ donde y es una raíz del polinomio*

$$\sigma(T) := T^m - u \in F[T]. \tag{2.1.2}$$

Entonces:

(a) F'/F *es de tipo Kummer y* $\mathbb{F}_q$ *es el cuerpo total de constantes de* F'*. Además*

$$S_1 \cap S_3 = \{\textit{ceros de } u \textit{ en } F\}.$$

Por lo tanto,

$$S = \mathbb{P}_1(F) \setminus \{\textit{polos y ceros de } u \textit{ en } F\}.$$

(b) Para cualquier $P \in S$ *tenemos que el polinomio* $\overline{\sigma}_P(T) := T^m - u(P)$ *se factoriza en* $\mathbb{F}_q[T]$ *en factores irreducibles distintos dos a dos.*

(c) El conjunto de polos y ceros P *de* u *en* F *tales que* $v_P(u) \not\equiv 0 \mod m$ *es el conjunto de lugares de* F *que están ramificados en* F'*. Además*

$$S_4 = \{P \in \mathbb{P}(F) : v_P(u) \neq 0 \ y \ \operatorname{mcd}(m, v_P(u)) = 1\}$$

y

$$S_5 = \{P \in \mathbb{P}(F) : v_P(u) \neq 0 \ y \ \operatorname{mcd}(m, v_P(u)) \neq 1\}.$$

De (iv) de la Proposición 2.1.1 tenemos que

$$N(F') = |\mathbb{P}_1(F) \cap S_4| + N + \sum_{P \in S} L_P, \tag{2.1.3}$$

donde L_P *denota el número de factores lineales en la factorización de* $T^m - u(P) \in \mathbb{F}_q[T]$ *y* N *es el número de lugares racionales de* F' *arriba de todos los lugares en* $\mathbb{P}_1(F) \cap S_5$*.*

(d) Sea $S_6 := \{P \in \mathbb{P}(F) : v_P(u) \neq 0 \ y \ v_P(u) \not\equiv 0 \mod m\}$*. Entonces*

$$g(F') = 1 + m(g(F) - 1) + \frac{m}{2} \sum_{P \in S_6} \left(1 - \frac{m}{\operatorname{mcd}(m, v_P(u))}\right) deg\, P.$$

Demostración. Las dos primeras afirmaciones en *(a)* están probadas en el Corolario 1.2.15 del Capítulo 1. Sea $P \in \mathbb{P}(F)$. Si P es un cero de u en F entonces $u(P) = 0$ y por lo tanto $\overline{\sigma}_P(T)$ no es un polinomio separable. Por otro lado, si $v_P(u) = 0$, entonces $u(P) \in \mathbb{F}_{q^r} \setminus \{0\}$ (donde $r = deg\, P$) y tenemos que $\overline{\sigma}_P(T)$ es un polinomio separable. Por lo tanto $S_1 \cap S_3 = \{\text{ceros de } u \text{ en } F\}$ y de (2.1.1) tenemos que *(a)* y *(b)* valen.

Por el Teorema 1.2.14 del Capítulo 1 tenemos que

$$e(Q|P) = \frac{m}{\text{mcd}(m, v_P(u))},$$

para cualquier $Q \in \mathbb{P}(F')$ que esté arriba de $P \in \mathbb{P}(F)$ y entonces P ramifica en F' si y sólo si $\text{mcd}(m, v_P(u)) \not\equiv 0 \mod m$. De *(a)* se obtiene entonces la primera afirmación en *(c)*. Como $a(y) = y^m$ tenemos que $m = deg\,(\sigma)$ divide a $v_Q(a(y))$ y por lo tanto las afirmaciones restantes en *(c)* se obtienen de (iv) de la Proposición 2.1.1.

Finamente, de *(c)* tenemos que los lugares en S_6 son exactamente los lugares ramificados de F en F'. Entonces *(d)* se obtiene de la fórmula del género para extensiones de Kummer dada en el Teorema 1.2.14 del Capítulo 1. □

Bajo las hipótesis de la Proposición 2.1.2, de la fórmula (2.1.3) obtenida para $N(F)$, podemos observar que para tener cuerpos de funciones de tipo Kummer F'/F con muchos lugares racionales necesitamos que el conjunto S tenga la mayor cantidad de elementos posibles, o lo que es equivalente, que la cantidad de factores lineales en (2.1.2) sea pequeña, ya que es más probable que $L_P > 1$ para $P \in S$. En esta dirección es conveniente considerar enteros positivos m que sean divisores de $q-1$ lo más grande posible y $u(P) = 1$ para $P \in S$ ya que de esta forma tendremos muchos factores lineales en la factorización de $T^m - 1$ en *(b)* de la Proposición 2.1.2.

Por otro lado, nos interesa tener cuerpos de funciones con muchos lugares racionales en comparación con el género. De la fórmula (2.1.3) de la Proposición 2.1.2 vemos que necesitamos tener ceros y polos de u en F que tengan el menor grado posible.

Estos son los hechos generales que guiaron la búsqueda y construcción explícita de cuerpos de funciones de tipo Kummer con muchos lugares racionales en [**vdGvdV00**] y en [**GG03**]. Los métodos usados en los trabajos anteriores permiten obtener buenos ejemplos de cuerpos de funciones de tipo Kummer con muchos lugares racionales siempre que se los considere sobre cuerpos finitos no primos. Veamos ahora algunos ejemplos sobre cuerpos primos.

Consideremos cuerpos de funciones de tipo Kummer $F' = F(y)$ donde $F = \mathbb{F}_q(x)$ y el polinomio mínimo de y sobre F es de la forma

$$T^m = u \quad \text{con} \quad u = \frac{x^{n+1} + f(x)}{f(x) + x},$$

con $f(x) \in \mathbb{F}_q[x]$ y m y n divisores de $q-1$. Notar que si $\gamma \in \mathbb{F}_q$ y $f(\gamma) + \gamma \neq 0$ entonces

$$\frac{\gamma^{n+1} + f(\gamma)}{f(\gamma) + \gamma} = 1$$

si y sólo si $\gamma = 0$ o γ es una $n-$ésima raíz de la unidad en $\mathbb{F}_q$.

Como F es ahora un cuerpo de funciones racionales, identificamos al lugar racional $P_{x-\gamma}$ de F para $\gamma \in \mathbb{F}_q$ con γ para que $S \subset \mathbb{F}_q$ donde S es como en la Proposición 2.1.2. Escribiremos L_γ en lugar de $L_{P_{x-\gamma}}$, por simplicidad. En todos los ejemplos que damos a continuación tenemos que o bien $S_5 = \emptyset$ o bien $S_5 = \{P_\infty\}$.

Ejemplo 2.1.3. Sea $q = 5$ y consideremos

$$f(x) = x.$$

Entonces tenemos que

$$\frac{x^5 + x}{x + x} = \frac{x(x^2+2)(x^2+3)}{2x} = 3(x^2+2)(x^2+3),$$

en $\mathbb{F}_5$. La ecuación

$$y^4 = 3(x^2+2)(x^2+3)$$

define una extensión de Kummer F'/F, pues $5 \equiv 1 \mod 4$, que satisface las condiciones de la Proposición 2.1.2. Como en este caso $S = \mathbb{F}_5$ y $f(\gamma) + \gamma = 2\gamma \neq 0$ para $\gamma \in S \setminus \{0\}$ tenemos que

$$L_\gamma = 4 \quad \text{para cada } \gamma \in S \setminus \{0\},$$

y

$$L_0 = 0,$$

pues el polinomio $T^4 - 3$ es irreducible sobre $\mathbb{F}_5$. Luego

$$\sum_{\gamma \in S} L_\gamma = 16.$$

Claramente, $\mathbb{P}_1(F) \cap S_4 = \emptyset$. Como $v_\infty(u) = -4$ tenemos que $S_5 = \{P_\infty\}$ y tenemos que calcular N. Dado que F'/F es un extensión (cíclica) de Galois de grado 4, de la cota superior de Serre para $N(F')$, deducimos que $N = 0$. En efecto, como P_∞ no ramifica y sabemos que

$$\sum_{Q|P_\infty} e(Q|P_\infty) f(Q|P_\infty) = 4,$$

entonces pueden pasar tres cosas: que haya un lugar arriba de P_∞ con grado de inercia 4, que haya dos lugares con grado de inercia 2 cada uno, o que haya cuatro lugares racionales. Pero en este último caso, tendríamos que $N(F') = 20$ y por la cota superior de Serre para $N(F')$ sabemos que $N(F') \leq 18$. Luego sólo puede darse alguno de los dos primeros casos y por lo tanto $N = 0$.

Hemos probado entonces que

$$y^4 = 3(x^2 + 2)(x^2 + 3)$$

define un cuerpo de funciones $F'/\mathbb{F}_5$ de género $g(F) = 3$ tal que

$$N(F') = 0 + 0 + 16 = 16.$$

éste es el valor de $N_5(3)$ (ver las tablas disponibles en http://www.manypoints.org/) que fue conseguido, también, por una extensión de tipo Kummer (llamada en este caso de tipo Fermat) cuya ecuación definitoria es

$$y^4 = 2 - x^4.$$

Para más detalles ver [**Ser85**].

Ejemplo 2.1.4. Sea $q = 7$, $m = 3$, $n = 3$ y consideremos nuevamente $f(x) = x$. Tenemos que

$$\frac{x^3 + x}{x + x} = 4(x^2 + 1),$$

en $\mathbb{F}_7$. La ecuación

$$y^3 = 4(x^2 + 1)$$

define una extensión de Kummer F'/F, pues $7 \equiv 1 \mod 3$, que satisface las condiciones de la Proposición 2.1.2. En este caso, $S = \mathbb{F}_7$ y se puede probar que

$$L_1 = L_2 = L_5 = L_6 = 3 \quad \text{y que} \quad L_0 = L_3 = L_4 = 0.$$

Luego, tenemos que

$$\sum_{\gamma \in S} L_\gamma = 12.$$

Tenemos que $v_\infty(u) = -2$ y por lo tanto $\mathbb{P}_1(F) \cap S_4 = \{P_\infty\}$. Luego $S_5 = \emptyset$ y entonces $N = 0$. De (2.1.3) de la Proposición 2.1.2 tenemos que

$$N(F') = 1 + 0 + 12 = 13.$$

En este caso, $g(F) = 1$ por lo que $F'/\mathbb{F}_7$ es un cuerpo de funciones elípticas. De hecho

$$F' = \mathbb{F}_7(u, v) \quad \text{con } v^2 = u^3 + 3.$$

El valor de $N_7(1)$ es 13 (ver las tablas en http://www.manypoints.org/). La curva elíptica

$$v^2 = u^3 + 3$$

fue encontrada por M. Deuring en 1941.

Ahora consideramos cuerpos de funciones de tipo Kummer $F' = F(y)$ donde $F = \mathbb{F}_q(x)$ y el polinomio mínimo de y sobre F es de la forma

$$T^m = u \quad \text{con } u := g(x) + 1,$$

donde $g(T) \in \mathbb{F}_q[T]$ es un divisor de $(T^q - T)^n$ para algún $n \in N$.

Ejemplo 2.1.5. Sea $q = 11$ y consideremos $m = 5$ y

$$g(T) = T^2(T-1)(T-2)(T-3).$$

La ecuación

$$y^5 = x^2(x-1)(x-2)(x-3) = x^5 + 5x^4 + 5x^2 + 1,$$

define una extensión de Kummer F'/F, pues $11 \equiv 1 \mod 5$, que satisface las condiciones de la Proposición 2.1.2. En este caso $S = \mathbb{F}_{11}$ y $\mathbb{P}_1(F) \cap S_4 = \emptyset$ ya que el polinomio $g(T)$

es irreducible en $\mathbb{F}_{11}[T]$ y por lo tanto el lugar $P_{g(x)}$ es el único cero de u y es de grado 5. Se ve fácilmente que

$$L_0 = L_1 = L_2 = L_3 = L_8 = L_{10} = 5 \quad \text{y} \quad L_4 = L_5 = L_6 = L_7 = L_9 = 0.$$

Por lo tanto

$$\sum_{\gamma \in S} L_\gamma = 30.$$

Como $v_\infty(u) = -5$ tenemos que $S_5 = \{P_\infty\}$ y entonces tenemos que calcular N.

Consideremos ahora la ecuación $z^5 = 1 + 5/x + 5/x^3 + 1/x^5$. Entonces

$$F' = \mathbb{F}_{11}(x, y) = \mathbb{F}_{11}(x, z),$$

y en este caso tenemos que

$$T^5 - (1 + 5/x + 5/x^3 + 1/x^5) \in \mathcal{O}_{P_\infty}[T],$$

y

$$T^5 - (1 + 5/x + 5/x^3 + 1/x^5) = T^5 - 1 \quad \text{mód } P_\infty.$$

Como $\mathbb{F}_{11}$ es el cuerpo de clases residuales de P_∞ y $T^5 - 1$ se descompone en 5 factores lineales en $\mathbb{F}_{11}[T]$, del Teorema de Kummer tenemos que P_∞ se descompone completamente en F' y por lo tanto $N = 5$. Utilizando (2.1.3) de la Proposición 2.1.2 tenemos que

$$N(F') = 0 + 5 + 30 = 35.$$

En este caso $g(F') = 6$. De las tablas en http://www.manypoints.org/ sólo se sabe que $N_{11}(6) \leq 45$ por lo tanto este ejemplo da una buena cota inferior para $N_{11}(6)$.

2.2. Sucesiones de cuerpos de funciones.

Estamos interesados en el estudio del número de lugares racionales en sucesiones recursivas de cuerpos de funciones de tipo (a, b) y esto significa encontrar cotas inferiores no triviales para $N(F_i)$ para todo F_i de una sucesión recursiva $\mathcal{F}$.

Recordemos que por una sucesión recursiva $\mathcal{F}$ de tipo (a, b) entendemos que tenemos una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones F_i sobre $\mathbb{F}_q$ y una sucesión $\{x_i\}_{i=0}^{\infty}$ de elementos trascendentes sobre $\mathbb{F}_q$ tales que

$$F_0 := \mathbb{F}_q(x_0) \subset F_1 \subset \ldots \subset F_i \subset F_{i+1} \subset \ldots$$

y $F_{i+1} = F_i(x_{i+1})$ donde

$$a(x_{i+1}) = b(x_i);$$

y si $a(T) = a_1(T)/a_2(T)$ y $b(T) = b_1(T)/b_2(T)$ entonces el polinomio $H(x_i, T) = a_1(T)b_2(x_i) - b_1(x_i)a_2(T)$ es separable para $i \geq 0$.

Recordemos también que el espacio de descomposición de $\mathcal{F}$ sobre F_0 es

$$Split(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : deg\, P = 1 \text{ y } P \text{ se descompone completamente en } \mathcal{F}\},$$

y que el espacio de ramificación completa de $\mathcal{F}$ sobre F_0 es

$$Cram(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : deg\, P = 1 \text{ y } P \text{ es totalmente ramificado en } \mathcal{F}\}.$$

Dado que cada lugar de $Q \in \mathbb{P}(F_i)$ que está arriba de algún lugar de $Split(\mathcal{F}/F_0) \cup Cram(\mathcal{F}/\mathbb{F}_q)$ es un lugar racional, tenemos que

$$N(F_i) \geq [F_i : F_0]|Split(\mathcal{F}/F_0)| + |Cram(\mathcal{F}/F_0)|. \tag{2.2.1}$$

En efecto, si $Q|P$ y $P \in Split(\mathcal{F}/F_0)$ entonces $deg\, P = 1$ y $e(Q|P) = f(Q|P) = 1$. Si $Q|P$ y $P \in Cram(\mathcal{F}/\mathbb{F}_q)$ entonces $deg\, P = 1$, $e(Q|P) = [F_i : F_0]$ y $f(Q|P) = 1$. En ambos casos tenemos que

$$\begin{aligned} deg\, Q &= [\mathcal{O}_Q/_Q : \mathbb{F}_q] \\ &= [\mathcal{O}_Q/_Q : \mathcal{O}_P/_P]\,[\mathcal{O}_P/_P : \mathbb{F}_q] \\ &= f(Q|P) deg\, P \\ &= 1 \end{aligned}$$

y por lo tanto Q es un lugar de $N(F_i)$. En particular, tenemos que la tasa de descomposición de la torre $\nu(\mathcal{F}/F_0)$ satisface

$$\nu(\mathcal{F}/F_0) \geq |Split(\mathcal{F}/F_0)|.$$

Claramente el espacio de descomposición $Split(\mathcal{F}/F_0)$ es un conjunto finito (que puede ser vacío). En el siguiente teorema establecemos condiciones suficientes para obtener una cota inferior no trivial para el tamaño de $Split(\mathcal{F}/F_0)$. Si $g(T) \in \mathbb{F}_q[T]$, denotamos por Z_g al conjunto de los ceros de $g(T)$ en una clausura algebraica $\bar{\mathbb{F}}_q$ de $\mathbb{F}_q$. En el caso de una función racional $g(T) = g_1(T)/g_2(T) \in \mathbb{F}_q(T)$, con g_1 y g_2 polinomios coprimos, Z_g es el conjunto de los ceros de $g_1(T)$ en una clausura algebraica $\bar{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Teorema 2.2.1. *Sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una sucesión recursiva de cuerpo de funciones sobre $\mathbb{F}_q$ de tipo (a, b) de manera que $\mathbb{F}_q$ sea el cuerpo total de constantes de todo F_i para $i \geq 0$. Supongamos que existe una función racional $\phi(T) \in \mathbb{F}_q(T)$ tal que su numerador y denominador no tienen factores comunes y que las siguientes condiciones valen:*

(i) $Z_{a_1} \cap Z_{a_2} = \emptyset$.

(ii) $Z_{\phi \circ a} \subset \mathbb{F}_q$.

(iii) $Z_{\phi \circ a} \subset Z_{\phi \circ b}$.

(iv) $\sigma_{i+1}(T) = a_1(T) - a_2(T)b(x_i) \in F_i[T]$ *es el polinomio mínimo de* x_{i+1} *sobre* F_i *para todo* $i \geq 0$.

(v) *Para todo* $\gamma \in Z_{\phi \circ a}$ *el polinomio* $\overline{\sigma}_\gamma(T) = a_1(T) - a_2(T)b(\gamma) \in \mathbb{F}_q[T]$ *tiene grado* $d = deg\,(a_1)$ *y todas sus raíces son simples.*

Entonces para todo $\gamma \in Z_{\phi \circ a}$, el lugar $P_{x_0 - \gamma}$ de $F_0 = \mathbb{F}_q(x_0)$ se descompone completamente en $\mathcal{F}$ y por lo tanto el espacio de descomposición de $\mathcal{F}/F_0$ satisface

$$|Split(\mathcal{F}/F_0)| \geq |Z_{\phi \circ a}|.$$

En particular $g(F_i) \to \infty$ cuando $i \to \infty$ y

$$N(F_i) \geq (deg\,(a))^i |Z_{\phi \circ a}| + |Cram(\mathcal{F}/F_0)| \geq (deg\,(a))^{i+1} + |Cram(\mathcal{F}/F_0)|. \qquad (2.2.2)$$

Demostración. Este resultado es consecuencia directa de la siguiente afirmación que será probada por inducción: para cada $\gamma \in Z_{\phi \circ a}$ el lugar $P_{x_0 - \gamma}$ de F_0 se descompone completamente en F_i para $i \geq 1$ y si Q es un lugar de F_i arriba de $P_{x_0 - \gamma}$ entonces existe $\gamma' \in Z_{\phi \circ a}$ tal que $x_i(Q) = \gamma'$.

Para la extensión F_1/F_0 tenemos que $\sigma_1(T) = a_1(T) - a_2(T)b(x_0) \in F_0[T]$ es el polinomio mínimo de x_1 sobre F_0. Ahora si $\gamma \in Z_{\phi\circ a}$ entonces $\phi(b(\gamma)) = 0$ por (iii) y entonces $b_2(\gamma) \neq 0$, lo que implica que $Z_{\phi\circ a} \subset \mathbb{F}_q \setminus Z_{b_2}$.

Ahora veamos que las raíces de $\overline{\sigma}_\gamma(T)$ están en $\mathbb{F}_q$ para todo $\gamma \in Z_{\phi\circ a}$. Si $\overline{\sigma}_\gamma(\alpha) = 0$ entonces

$$0 = a_1(\alpha) - a_2(\alpha)b(\gamma).$$

Tenemos además que $a_2(\alpha) \neq 0$ pues en otro caso tendríamos $a_1(\alpha) = 0$ y por lo tanto $\alpha \in Z_{a_1} \cap Z_{a_2}$ contradiciendo (i). Por lo tanto

$$a(\alpha) = b(\gamma),$$

y por (iii)

$$\phi(a(\alpha)) = \phi(b(\gamma)) = 0.$$

Luego, $\alpha \in Z_{\phi\circ a} \subset \mathbb{F}_q$ por (ii).

Seguimos la notación de la Proposición 2.1.2 e identificamos el lugar racional $P_{x_0-\gamma}$ de F_0 con γ para que $S \subset \mathbb{F}_q$. Ahora, por (iv), (v) y tomando $S = Z_{\phi\circ a}$ tenemos por la Proposición 2.1.2 que para cada $\gamma \in Z_{\phi\circ a}$ hay exactamente d lugares racionales de F_1 sobre el lugar racional $P_{x_0-\gamma}$ y por lo tanto $P_{x_0-\gamma} \in \mathbb{P}(F_0)$ se descompone completamente en F_1. Más aún, el Teorema de Kummer nos dice que si Q es un lugar de F_1 arriba de $P_{x_0-\gamma}$ entonces $x_1(Q) = \gamma'$ para alguna raíz simple γ' de $\overline{\sigma}_\gamma(T)$. Entonces $a(\gamma') = b(\gamma)$ y por lo tanto $\phi(a(\gamma')) = \phi(b(\gamma)) = 0$ de donde concluimos que $\gamma' \in Z_{\phi\circ a}$ y tenemos probada la afirmación para $i = 1$.

Supongamos ahora que la afirmación es válida para F_i/F_0. Sea $\gamma \in Z_{\phi\circ a}$ y sea $Q \in \mathbb{P}(F_i)$ uno de los lugares arriba de $P_{x_0-\gamma}$. Por la hipótesis inductiva, existe $\gamma' \in Z_{\phi\circ a}$ tal que $x_i(Q) = \gamma'$. Sea x_{i+1} tal que $a(x_{i+1}) = b(x_i)$.

Por (iv) el polinomio

$$\sigma_{i+1}(T) = a_1(T) - a_2(T)b(x_i) \in F_i[T],$$

es el polinomio mínimo de x_{i+1} sobre F_i. Además

$$\overline{\sigma}_\gamma(T) = a_1(T) - a_2(T)b(\gamma') = \sigma_{i+1}(T) \mod Q,$$

$\overline{\sigma}_\gamma(T)$ tiene grado $d = deg\,(a_1(T)) = [F_{i+1} : F_i]$ y todas sus raíces son simples por (v) y están en $Z_{\phi\circ a} \subset \mathbb{F}_q$ como ya hemos visto. Por otro lado, como $\gamma' \in Z_{\phi\circ b}$ por (iii), y $x_i(Q) = \gamma'$ entonces

$$0 \neq b_2(\gamma') = b_2(x_i(Q)) = b_2(x_i) \mod Q,$$

y por lo tanto $v_Q(b_2(x_i)) = 0$. Luego $v_Q(b(x_i)) = v_Q(b_1(x_i)) \geq 0$ y tenemos que $\sigma_{i+1}(T) \in \mathcal{O}_Q$. Esto, junto con (iv) implica que x_{i+1} es integral sobre $\mathcal{O}_Q$.

Entonces por el Teorema de Kummer tenemos que hay exactamente $d = [F_{i+1} : F_i]$ extensiones $\tilde{Q}_1, \ldots, \tilde{Q}_d$ de Q en F_{i+1} tales que $x_{i+1}(\tilde{Q}_j) = \eta_j \in Z_{\phi\circ a}$ para $j = 1, \ldots, d$ y por lo tanto la afirmación está probada para F_{i+1}/F_0.

Finalmente para completar la prueba del teorema, observar que como

$$\nu(\mathcal{F}/F_0) \geq |\mathrm{Split}(\mathcal{F}/F_0)| \geq |Z_{\phi\circ a}|,$$

entonces la ecuación (2.2.2) vale y utilizando la cota de Hasse-Weil (Teorema 1.3.1 del Capítulo 1) tenemos que

$$g(F_i) \geq \frac{N(F_i) - (q+1)}{2\sqrt{q}} \underset{i\to\infty}{\longrightarrow} \infty,$$

como queríamos demostrar.

□

Observación 2.2.2. Si en el Teorema 2.2.1, en lugar de (iv) y (v) tenemos

(iv') $\sigma_{i+1}(T) = b(x_i)^{-1}a_1(T) - a_2(T) \in F_i[T]$ es el polinomio mínimo de x_{i+1} sobre F_i para todo $i > 0$;

(v') para todo $\gamma \in Z_{\phi\circ a}$, $b(\gamma) \neq 0$ y el polinomio $b(\gamma)^{-1}a_1(T) - a_2(T)$ tiene $d = deg\,(a_2(T))$ raíces simples;

entonces el mismo argumento anterior muestra que el Teorema 2.2.1 sigue siendo válido. En esta dirección, notar que si $\phi(0) \neq 0$ entonces $b(\gamma) \neq 0$ para todo $\gamma \in Z_{\phi\circ a}$ por (iii) del Teorema 2.2.1.

En cualquier caso, de la prueba del Teorema se obtiene que

$$|Z_{\phi\circ a}| \geq d = deg\,(a_1)$$

ya que $\eta_j \in Z_{\phi\circ a}$ para todo $j = 1, \ldots, d$.

Observación 2.2.3. La función ϕ del Teorema 2.2.1 no es única. En efecto, supongamos que para una sucesión $\mathcal{F}$ recursiva de tipo (a, b), existe una función ϕ que satisface las condiciones del Teorema. Consideremos $\tilde{\phi} = \phi^\ell$ donde ℓ es una potencia de $char\, \mathbb{F}_q$. Entonces las condiciones (i), (iv) y (v) del teorema siguen siendo válidas, ya que no dependen de ϕ, y (ii) y (iii) valen pues para cualquier $f \in \mathbb{F}_q(T)$ se tiene que

$$Z_{\tilde{\phi}\circ f} = \{\gamma : \tilde{\phi}(f(\gamma)) = 0\} = \{\gamma : \phi(f(\gamma))^\ell = 0\} = \{\gamma : \phi(f(\gamma)) = 0\} = Z_{\phi\circ f}$$

y por lo tanto

$$Z_{\tilde{\phi}\circ f} = Z_{\phi\circ f} \subset \mathbb{F}_q;$$

y

$$Z_{\tilde{\phi}\circ a} = Z_{\phi\circ a} \subset Z_{\phi\circ b} = \{\gamma : \phi(b(\gamma)) = 0\} = Z_{\tilde{\phi}\circ b}.$$

Luego, $\tilde{\phi}$ también satisface las condiciones del Teorema 2.2.1 y como $Z_{\tilde{\phi}\circ a} = Z_{\phi\circ a}$ se obtiene el mismo resultado.

Observación 2.2.4. Consideremos ahora lo siguiente. Supongamos que $\mathcal{F}$ es una sucesión recursiva de tipo (a, b) y supongamos que $\phi(T) = \sum c_j\, T^j \in \mathbb{F}_q[T]$ es un polinomio que satisface las condiciones del Teorema 2.2.1. Consideremos $\tilde{\tilde{\phi}}(T) = \sum c_j^\ell\, T^j$ donde ℓ es un entero tal que $\mathbb{F}_p \subset \mathbb{F}_\ell \subset \mathbb{F}_q$, donde $p = char\, \mathbb{F}_q$.

Si para algún $f \in \mathbb{F}_q[T]$ se tiene que

$$\{f(\gamma) : \gamma \in Z_{\phi\circ f}\} \subset \mathbb{F}_\ell$$

entonces vale también que

$$\begin{aligned}
Z_{\tilde{\tilde{\phi}}\circ f} &= \left\{\gamma : \tilde{\tilde{\phi}}(f(\gamma)) = 0\right\} \\
&= \left\{\gamma : \sum c_j^\ell\, (f(\gamma))^j = 0\right\} \\
&= \left\{\gamma : \sum c_j^\ell\, (f(\gamma))^{\ell j} = 0\right\} \\
&= \left\{\gamma : \left(\sum c_j\, (f(\gamma))^j\right)^\ell = 0\right\} \\
&= \left\{\gamma : \sum c_j\, (f(\gamma))^j = 0\right\}
\end{aligned}$$

$$= \{\gamma : \phi(f(\gamma)) = 0\}$$

$$= Z_{\phi \circ f}.$$

Luego, si a y b satisfacen

$$\{a(\gamma) : \gamma \in Z_{\phi \circ a}\} \subset \mathbb{F}_\ell \quad \text{y} \quad \{b(\gamma) : \gamma \in Z_{\phi \circ b}\} \subset \mathbb{F}_\ell$$

entonces también se cumplen las hipótesis del Teorema 2.2.1 para $\tilde{\tilde{\phi}}$ y se obtiene el mismo resultado.

Ejemplo 2.2.5(Torre BGS de Bezerra-Garcia-Stichtenoth)**.** Esta torre fue considerada en [**BGS05c**].

Sea q una potencia de un primo y consideremos el cuerpo finito $\mathbb{F}_l$ con $l = q^3$. La torre BGS denotada $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ está definida recursivamente por la ecuación

$$\frac{1-y}{y^q} = \frac{x^q + x - 1}{x}.$$

En este caso tenemos que

$$a(T) = \frac{1-T}{T^q} \qquad \text{y} \qquad b(T) = \frac{T^q + T - 1}{T}.$$

Sea

$$\phi(T) = T^{q+1} - T + 1.$$

En [**BS07**], Bassa y Stichtenoth probaron que, en este caso,

$$T^{q^2+q}\,\phi(a(T)) = T^{q+1}\,\phi(b(T)) = (1-T)^{q^2+q+1} + T^{q^2+q+1},$$

$Z_{\phi \circ a} \subset \mathbb{F}_l$ y $|Z_{\phi \circ a}| = q(q+1)$. Por lo tanto se cumplen las condiciones (ii), (iii) . Las condiciones (i) y (iv') se cumplen por la forma en que está definida la torre y el hecho de que todas las extensiones satisfacen $[G_i : G_0] = q^i$ para todo $i \geq 0$.

Finalmente veamos que se cumple la condición (v'). Como $\phi(0) \neq 0$ sólo tenemos que probar que $\bar{\sigma}_\gamma(T) = \frac{1}{b(\gamma)}(1-T) - T^q$ tiene q raíces distintas y esto se ve fácilmente observando que su derivada $\bar{\sigma}'_\gamma(T) = \frac{-1}{b(\gamma)}$ no tiene raíces en común con $\bar{\sigma}_\gamma(T)$.

Luego, como se cumplen todas las condiciones del Teorema 2.2.1, tenemos que

$$|Split(\mathcal{G}/G_0)| \geq |Z_{\phi \circ a}| = q(q+1).$$

Ejemplo 2.2.6. Sea p un número primo impar y sea $q = p^2$. Consideremos la torre $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ definida por la ecuación

$$y^2 = \frac{x^2+1}{2x}.$$

Esta torre fue definida en [**GSR03**] en donde los autores prueban que la torre es óptima haciendo uso de ciertas propiedades del llamado polinomio de Deuring. En [**Sti09**] se considera como ejemplo y utilizando [**Sti09**, Corolario 7.2.21] se obtiene que $\nu(\mathcal{E}/E_0) \geq 4$, para el caso en que $q = 9$.

Veamos que se cumplen las condiciones del Teorema 2.2.1 para calcular una cota inferior para la tasa de descomposición para la torre sobre $\mathbb{F}_9$.

En este caso tenemos que

$$a(T) = T^2 \qquad \text{y} \qquad b(T) = \frac{T^2+1}{2T}.$$

Sea

$$\phi(T) = T^2 + 1.$$

Se puede verificar fácilmente que

$$\phi(a(T)) = T^2\,\phi(b(T)) = (T^2+2T+2)(T^2+T+2).$$

Escribimos $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ con $\alpha^2 = 2\alpha + 1$ y por lo tanto $\mathbb{F}_9 = \{0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2\}$. Entonces tenemos que

$$Z_{\phi\circ a} = \{\gamma \in \bar{\mathbb{F}}_9 \,:\, \phi(a(\gamma)) = 0\} = \{\alpha,\ \alpha+1,\ 2\alpha,\ 2\alpha+2\} \subset \mathbb{F}_9.$$

Esto nos asegura que se cumplen las condiciones (ii) y (iii). Las condiciones (i) y (iv) valen por la forma en que está definida la torre.

Veamos que se cumple la condición (v). Observar que en este caso el polinomio correspondiente es $\bar{\sigma}_\gamma(T) = a(T) - b(\gamma) = T^2 - b(\gamma)$ para todo $\gamma \in Z_{\phi\circ a}$, y como su derivada es $\bar{\sigma}'_\gamma(T) = 2T$, que solo se anula en 0, entonces para poder asegurar que $\bar{\sigma}_\gamma$ y su derivada no tienen raíces comunes tenemos que probar que $b(\gamma) \neq 0$ para todo $\gamma \in Z_{\phi\circ a}$. Calculemos entonces $b(\gamma)$ para todo los $\gamma \in Z_{\phi\circ a}$.

- $b(\alpha) = \alpha + 2$

- $b(\alpha+1) = \alpha+2$
- $b(2\alpha) = 2\alpha+1$
- $b(2\alpha+2) = 2\alpha+1$

y por lo tanto el polinomio $\bar{\sigma}_\gamma(T) = T^2 - b(\gamma)$ tiene 2 raíces simples.

Como se cumplen las condiciones del Teorema 2.2.1 tenemos que

$$|Split(\mathcal{E}/E_0)| \geq 4.$$

Por lo tanto obtenemos el mismo resultado que en el ejemplo en [**Sti09**].

Ejemplo 2.2.7. Consideremos la torre $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_8$ definida recursivamente por

$$y^2 + y = \frac{x^2+x+1}{x}.$$

Esta torre fue considerada por van der Geer y van der Vlugt en [**vdGvdV02**]. Allí calcularon explícitamente el género y la cantidad de lugares racionales en cada paso de la torre y obtuvieron que $N(H_i) = 6 \cdot 2^i + 2$ para todo $i \geq 0$.

Veamos que se cumplen las condiciones del Teorema 2.2.1 para calcular una cota inferior para la tasa de descomposición.

En este caso tenemos que

$$a(T) = T^2 + T \qquad \text{y} \qquad b(T) = \frac{T^2+T+1}{T}.$$

Sea

$$\phi(T) = T^3 + T + 1.$$

Se puede verificar fácilmente que

$$\phi(a(T)) = T^3\,\phi(b(T)) = (T^3+T^2+1)(T^3+T+1).$$

Si escribimos $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ con $\alpha^3 = \alpha+1$ entonces $\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$. Vemos que $\phi(a(T))$ se descompone completamente en $\mathbb{F}_8$ y por lo tanto

$$Z_{\phi\circ a} = \mathbb{F}_8 \setminus \mathbb{F}_2.$$

Esto nos asegura que se cumplen las condiciones (ii) y (iii). Las condiciones (i) y (iv) valen por la forma en que está definida la torre.

Veamos que se cumple la condición (v). Observar que en este caso el polinomio correspondiente es $\bar{\sigma}_\gamma(T) = a(T) - b(\gamma) = T^2 + T - b(\gamma)$ para todo $\gamma \in Z_{\phi\circ a}$, y como su derivada es $\bar{\sigma}'_\gamma(T) = 1$ que es coprimo con $\bar{\sigma}_\gamma(T)$, entonces el polinomio $\bar{\sigma}_\gamma(T) = T^2 - b(\gamma)$ tiene 2 raíces simples.

Como se cumplen las hipótesis del Teorema 2.2.1 tenemos que

$$|Split(\mathcal{H}/H_0)| \geq 6$$

y que

$$N(H_i) \geq 6 \cdot 2^i + |Cram(\mathcal{F}/F_0)|$$

para todo $i \geq 0$.

En este caso, tanto el polo como el cero de x_0 en F_0 son totalmente ramificados en la torre y por (2.2.2) del Teorema 2.2.1 tenemos que

$$N(H_i) \geq 6 \cdot 2^i + 2$$

para todo $i \geq 0$. En efecto, la prueba de que el polo es totalmente ramificado es igual que en la prueba del Teorema 1.4.4. Para ver que el cero P_0 es totalmente ramificado debemos observar que en la primer extensión ramifica totalmente ya que si Q_0 es un lugar de F_1 tal que $Q_0|P_0$ entonces

$$v_{Q_0}(x_1^2 + x_1) = e(Q_0|P_0)\, v_{P_0}\left(\frac{x_0^2 + x_0 + 1}{x_0}\right) = e(Q_0|P_0)(-1).$$

Luego, como la suposición $v_{Q_0}(x_1) \geq 0$ conduce a un absurdo, tenemos que $v_{Q_0}(x_1) < 0$ y por lo tanto $2v_{Q_0}(x_1) = -e(Q_0|P_0)$ de donde obtenemos $e(Q_0|P_0) = 2$ y $v_{Q_0}(x_1) = -1$.

Ahora se puede probar por inducción que si R_0 es un lugar de F_n que esté arriba de P_0 de manera que $e(R_0|P_0) = 2^n$ y $v_{R_0}(x_n) = -1$, y si $S_0 \in \mathbb{P}(F_{n+1})$ es tal que $S_0|R_0$ entonces tenemos que

$$\begin{aligned} v_{S_0}(x_{n+1}^2 + x_{n+1}) &= e(S_0|R_0)\, v_{R_0}\left(\frac{x_n^2 + x_n + 1}{x_n}\right) \\ &= e(S_0|R_0)\, v_{R_0}(2v_{R_0}(x_n) - v_{R_0}) \end{aligned}$$

$$= e(S_0|R_0)\, v_{R_0}(-1)$$

y al igual que antes $e(S_0|R_0) = 2$ y $v_{S_0}(x_{n+1}) = -1$. Luego, P_0 es totalmente ramificado en la torre.

Proposición 2.2.8. *Sea $m \geq 2$ y sea q una potencia de un primo tal que* $\mathrm{mcd}(m, char\, \mathbb{F}_q) = 1$. *Sean $f(T) \in \mathbb{F}_q[T]$ un polinomio separable de grado $m - r$ con $r \in \mathbb{N}$ y* $\mathrm{mcd}(m, r) = 1$*; y $h(T) \in \mathbb{F}_q[T]$ un polinomio de manera que $h(T) - \alpha$ tenga $m = deg(h)$ raíces simples en $\mathbb{F}_q$ para algún $\alpha \in \mathbb{F}_q$. Además supongamos que $Z_{h-\alpha} \cap Z_f = \emptyset$. Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ generada recursivamente por la ecuación*

$$h(y) = \frac{h(x) + \alpha f(x) - \alpha}{f(x)}.$$

Entonces $\mathcal{F}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_q$ tal que

$$|Split(\mathcal{F}/F_0)| \geq m, \qquad y \qquad N(F_i) \geq m^{i+1} + 1, \quad i \geq 0.$$

Demostración. Observar que la ecuación que define esta sucesión satisface las condiciones del Teorema 1.4.4, y por lo tanto para probar que es torre sólo hace falta ver que $g(F_i) \to \infty$ cuando $i \to \infty$.

Veamos que se satisfacen las condiciones (ii)-(v) del Teorema 2.2.1 para obtener la cota para el espacio de descomposición. La condición (i) se satisface por hipótesis.

En este caso tenemos que

$$a(T) = h(T) \qquad \text{y} \qquad b(T) = \frac{h(T) + \alpha f(T) - \alpha}{f(T)}.$$

Sea

$$\phi(T) = T - \alpha.$$

Entonces

$$\phi(a(T)) = a(T) - \alpha = h(T) - \alpha$$

y

$$\phi(b(T)) = b(T) - \alpha = \frac{h(T) + \alpha f(T) - \alpha}{f(T)} - \alpha = \frac{h(T) + \alpha f(T) - \alpha - \alpha f(T)}{f(T)} = \frac{h(T) - \alpha}{f(T)},$$

y por lo tanto, como $Z_{h-\alpha} \cap Z_f = \emptyset$, vale que $Z_{\phi oa} \subset Z_{\phi ob}$. Además, como $h(T) - \alpha$ tiene todas sus raíces en $\mathbb{F}_q$ entonces $Z_{\phi oa} \subset \mathbb{F}_q$.

La condición (iv) se cumple por la forma en que está definida la sucesión y porque se cumplen las condiciones del Teorema 1.4.4.

Finalmente, para cada $\gamma \in Z_{\phi oa}$ tenemos que el polinomio $\overline{\sigma}_\gamma(T) = a(T) - b(\gamma)$ tiene m raíces simples pues como $\gamma \in Z_{\phi oa}$, entonces $\phi \circ a(\gamma) = 0$, lo que significa que $h(\gamma) = \alpha$ y por lo tanto

$$\overline{\sigma}_\gamma(T) = a(T) - b(\gamma) = h(T) - \frac{h(\gamma) + \alpha f(\gamma) - \alpha}{f(\gamma)} = h(T) - \alpha,$$

que por hipótesis tiene m raíces simples.

Como se cumplen las condiciones del Teorema 2.2.1 tenemos que

$$|Split(\mathcal{F}/F_0)| \geq m.$$

Como el polo P_∞ de x_0 en F_0 es totalmente ramificado en $\mathcal{F}$, por (2.2.2) del Teorema 2.2.1 tenemos que, para todo $i \geq 0$, el número de lugares racionales de F_i/F_0 satisface

$$N(F_i) \geq m^{i+1} + 1.$$

También por el Teorema 2.2.1, tenemos que $g(F_i) \to \infty$, cuando $i \to \infty$ y por lo tanto $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ es una torre recursiva de cuerpos de funciones sobre $\mathbb{F}_q$, lo cual completa la prueba. □

Observación 2.2.9. Las cotas para el espacio de descomposición siguen siendo válidas en el caso en que $h(T) = h_1(T)/h_2(T) \in \mathbb{F}_q(T)$ sea una función racional, con h_1 y h_2 sin factores comunes, definiendo $deg\,(h) = \text{máx}\{deg\,(h_1), deg\,(h_2)\}$ y teniendo en cuenta lo considerado en la Observación 2.2.2.

Ejemplo 2.2.10. Sea q una potencia de un primo impar de manera que $T^2 + 1$ se descomponga completamente en $\mathbb{F}_q$. Consideremos los polinomios $f(T) = 2T$ y $h(T) = T^2 + 2$. Entonces la sucesión $\mathcal{F} = (F_1, F_2, \ldots)$ generada recursivamente por la ecuación

$$y^2 + 2 = \frac{x^2 + 2x + 1}{2x}$$

sobre $\mathbb{F}_q$ y satisface

$$|Split(\mathcal{F}/F_0)| \geq 2,$$

ya que se cumplen las condiciones de la Proposición 2.2.8. Observar que la ecuación que define esta sucesión puede escribirse como

$$y^2 = \frac{(x-1)^2}{2x}.$$

En el próximo Capítulo veremos que la torre generada por esta ecuación es asintóticamente óptima.

2.3. Sucesiones y torres de tipo Kummer

Ejemplo 2.3.1. Si consideramos sucesiones como en la Proposición 2.2.8 pero con $h(T) = T^m$ tenemos sucesiones de tipo Kummer. Es decir, si $m \geq 2$ y q es una potencia de un primo de manera que $\mathbb{F}_q$ contenga al cuerpo de descomposición del polinomio $T^m + 1$ y tal que $\mathrm{mcd}(m, char\, \mathbb{F}_q) = 1$, y consideramos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ definida recursivamente por la ecuación

$$y^m = \frac{x^m + \alpha f(x) - \alpha}{f(x)},$$

donde $f(T) \in \mathbb{F}_q[T]$ es un polinomio de grado $m - r$ con $\mathrm{mcd}(m, r) = 1$, entonces $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ es una torre recursiva de tipo Kummer de cuerpos de funciones sobre $\mathbb{F}_q$ y tenemos que para todo $i \geq 0$, el número de lugares racionales de F_i/F_0 satisface

$$N(F_i) \geq m^{i+1} + 1.$$

Las sucesiones del tipo del Ejemplo 2.3.1 pueden verse también como un caso particular del siguiente resultado.

Proposición 2.3.2. *Sean $m \geq 2$ y $n > k \geq 1$ tales que $\mathrm{mcd}(m, n-k) = 1$ y $\mathrm{mcd}(m, q) = 1$. Sea $\alpha \in \mathbb{F}_q^*$ y consideremos las funciones racionales*

$$a(T) = T^m \qquad y \qquad b(T) = \frac{T^n + \alpha(f(T) - 1)}{f(T)},$$

donde $f(T) \in \mathbb{F}_q[T]$ es un polinomio de grado k. Sea F_{q^t} un cuerpo de descomposición para $T^m - \alpha$. Si $Z_f \cap Z_{T^m-\alpha} = \emptyset$ entonces para la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ tenemos que

$$|Split(\mathcal{F}/F_0)| \geq m,$$

y por lo tanto

$$N(F_i) \geq m^{i+1} + 1,$$

para cualquier $i \geq 0$.

Demostración. Observar que la ecuación que define esta sucesión satisface las condiciones del Teorema 1.4.4, y por lo tanto el polinomio

$$\sigma(T) = T^m - \frac{x_i^n + \alpha(f(x_i) - 1)}{f(x_i)} \ \in F_i[T]$$

es el polinomio mínimo de x_{i+1} sobre F_i. Sea

$$\phi(T) = T - \alpha.$$

Entonces $\phi(T) \in \mathbb{F}_q[T]$ y

$$\phi(a(T)) = T^m - \alpha \qquad \text{y} \qquad \phi(b(T)) = \frac{T^n - \alpha}{f(T)}.$$

Ahora, sea $r > 0$ tal que $\alpha^{r-1} = 1$. Si $\beta^m = \alpha$ entonces

$$\beta^{mr} - \alpha = \alpha^r - \alpha = \alpha(\alpha^{r-1} - 1) = 0,$$

y por lo tanto $Z_{\phi \circ a} \subset Z_{\phi \circ b}$ si $n = mr$. Notar que si $r > 1$ entonces $Z_{\phi \circ a} \subsetneq Z_{\phi \circ b}$.

Como $T^m - \alpha$ se descompone en $\mathbb{F}_{q^t}$ entonces $Z_{\phi \circ a} \subset \mathbb{F}_{q^t}$. Además, como $\text{mcd}(m, q) = 1$ y $Z_f \cap Z_{\phi \circ a} = \emptyset$ tenemos que para cada $\gamma \in Z_{\phi \circ a}$ el polinomio $\bar{\sigma}_\gamma(T)$ es separable. Luego, se cumplen las condiciones del Teorema 2.2.1 y se obtienen las estimaciones buscadas. □

Las condiciones de la Proposición 2.3.2 son cumplidas, por ejemplo, por la sucesión recursiva $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de tipo (a, b) sobre $\mathbb{F}_9$ con

$$a(T) = T^2 \qquad \text{y} \qquad b(T) = \frac{T^2 + f(T) - 1}{f(T)},$$

donde $f(T) = T + 1$. En este caso

$$b(T) = \frac{T(T-1)}{T+1},$$

y obtenemos que $|Split(\mathcal{F}/F_0)| \geq 2$. Esta sucesión fue estudiada en [**GSR03**] obteniéndose el mismo resultado para el espacio de descomposición.

Si consideramos ahora la sucesión recursiva $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ de tipo (a, b) de cuerpos de funciones sobre $\mathbb{F}_9$ con

$$a(T) = T^2 \qquad \text{y} \qquad b(T) = \frac{T^2 - (f(T) - 1)}{f(T)},$$

donde $f(T) = T$ entonces las condiciones del Teorema 2.2.1 también se cumplen. En este caso

$$b(T) = \frac{(T+1)^2}{T},$$

y obtenemos que $|Split(\mathcal{G}/G_0)| \geq 2$. En [**GSR03**] probaron que esta sucesión es una subsucesión de la dada en el Ejemplo 2.2.6 en el sentido en que cada cuerpo G_i es un subcuerpo de algún cuerpo $E_{j(i)}$ en la sucesión $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ de cuerpos de funciones dada en el Ejemplo 2.2.6.

Veamos ahora un resultado sobre cuerpos primos.

Proposición 2.3.3. *Sea l un número primo y $r \in \mathbb{N}$. Sea p un factor primo de $l - 1$ y consideremos las ecuaciones*

$$y^p = \frac{x^{rp} + x - 1}{x},$$

y

$$y^p = \frac{x^{rp} + x}{x + 1}, \qquad \textit{para } p \geq 3.$$

Entonces ambas ecuaciones definen respectivamente sucesiones $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ y $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_l$ con tasa de descomposición positiva

$$|Split(\mathcal{F}/F_0)| \geq p \qquad y \qquad |Split(\mathcal{H}/H_0)| \geq p,$$

y se tienen las siguientes estimaciones

$$N(F_i) \geq p^{i+1} + 1 \qquad y \qquad N(H_i) \geq p^{i+1} + 1,$$

para todo $i \geq 0$.

Demostración. Para la sucesión $\mathcal{F}$ tomemos $m = p$, $n = rp$, $\alpha = 1$ y $f(T) = T$ en la Proposición 2.3.2. Entonces

$$a(T) = T^p \quad \text{y} \quad b(T) = \frac{T^{rp} + f(T) - 1}{f(T)} = \frac{T^{rp} + T - 1}{T},$$

y tenemos que $a(T)$, $b_1(T)$ y $b_2(T)$ están en $\mathbb{F}_l[T]$. Además tenemos que $\text{mcd}(p, rp-1) = 1$. Como $\text{mcd}(p, l) = 1$ y $Z_f \cap Z_{\phi \circ a} = Z_T \cap Z_{T^p-1} = \emptyset$ entonces la Proposición 2.3.2 muestra que la ecuación

$$y^p = \frac{x^{rp} + x - 1}{x},$$

define una sucesión recursiva $\mathcal{F} = (F_0, F_1, f_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_l$ con tasa de descomposición

$$|Split(\mathcal{F}/F_0)| \geq p,$$

y para la cual se verifica que

$$N(F_i) \geq p^{i+1} + 1,$$

para todo $i \geq 0$.

Ahora supongamos que p es impar y consideremos $f(T) = T + 1$. Entonces

$$a(T) = T^p \quad \text{y} \quad b(T) = \frac{T^{rp} + f(T) - 1}{F(T)} = \frac{T^{rp} + T}{T + 1},$$

y como p es impar tenemos que $Z_f \cap Z_{\phi \circ a} = Z_{T+1} \cap Z_{T^p-1} = \emptyset$. De la Proposición 2.3.2 deducimos que la ecuación

$$y^p = \frac{x^{rp} + x}{x + 1}$$

define una sucesión recursiva de cuerpos de funciones $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ sobre $\mathbb{F}_l$ con tasa de descomposición

$$|Split(\mathcal{H}/H_0)| \geq p,$$

y para la cual se verifica que

$$N(H_i) \geq p^{i+1} + 1,$$

para todo $i \geq 0$. □

CAPÍTULO 3

RAMIFICACIÓN

El estudio de la ramificación de lugares en una torre de cuerpos de funciones es de importancia central en la teoría general del comportamiento asintótico de torres de cuerpos de funciones. En particular, el grado de ramificación de los lugares determina el comportamiento asintótico del género de los cuerpos de funciones que definen una torre.

En este Capítulo damos condiciones sobre las ecuaciones que definen la sucesión para obtener torres asintóticamente buenas a través del cálculo del espacio de ramificación para torres moderadas. Utilizando los resultados obtenidos mostramos diferentes ejemplos de torres asintóticamente buenas. Además hacemos un estudio general sobre los conceptos de subtorre y de supertorre de cuerpos de funciones. Estos conceptos son importantes en cuanto a que definen si un ejemplo de torre asintóticamente buena puede considerarse nuevo o no. También son útiles para demostrar si una torre es asintóticamente buena o no a partir de ejemplos ya estudiados. Damos un método general de construcción de subtorres y mostramos que muchos ejemplos conocidos son casos particulares de esta construcción. En la Sección 3 mostramos un familia de tipo Kummer con ramificación finita sobre todo cuerpo finito con al menos tres elementos, que además es torre asintóticamente buena en ciertos casos e incluso asintóticamente óptima en algunos de éstos. Este ejemplo da una demostración alternativa a la de Garcia, Stichtenoth y Rück dada en [**GSR03**] de que $A(q^2) > 0$ si $q \geq 3$.

3.1. Torres moderadas

Sea $F/\mathbb{F}_q$ un cuerpo de funciones. Dada una extensión finita E/F y un lugar $P \in \mathbb{P}(F)$, existe una cantidad finita de lugares $P' \in \mathbb{P}(E)$ que están arriba de P. La extensión E/F se dice que es *moderada* si el índice de ramificación $e(P'|P)$ es coprimo con la característica de $\mathbb{F}_q$, para todos los lugares $P \in \mathbb{P}(F)$ y todo $P'|P$; en otro caso la extensión es *salvaje*. Decimos que una sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ es *moderada* si todas las extensiones F_n/F_0 son moderadas. En caso contrario decimos que la sucesión es *salvaje*.

Para torres moderadas se tiene el siguiente resultado debido a Garcia, Stichtenoth y Thomas.

Teorema 3.1.1. [**GST97**, Teorema 2.1] *Sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una torre de cuerpos de funciones sobre $\mathbb{F}_q$ que satisface las siguientes condiciones:*

(i) *Todas las extensiones F_{n+1}/F_n son moderadas.*

(ii) *$Ram(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) \mid P$ ramifica en F_n/F_0 para algún $n \geq 1\}$ es finito.*

(iii) *$Split(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) \mid \deg P = 1$, y P se descompone completamente en $\mathcal{F}\}$ es no vacío.*

Entonces $\mathcal{F}$ es asintóticamente buena, y se obtiene la estimación

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_0) - 2 + s} > 0,$$

donde $t := |Split(\mathcal{F}/F_0)|$ y $s := \sum_{P \in Ram(\mathcal{F}/F_0)} \deg P$.

Como ejemplos explícitos de torres que satisfacen las hipótesis del Teorema 3.1.1, Garcia, Stichtenoth y Thomas presentaron (en [**GST97**]) la siguiente familia de torres de cuerpos de funciones.

Teorema 3.1.2. *Sea $m > 1$ un entero con $q \equiv 1 \mod m$, y sea $S_0 \subseteq \mathbb{F}_q$ un subconjunto de $\mathbb{F}_q$ con $0 \in S_0$. Supongamos que $f(t) \in \mathbb{F}_q[T]$ es un polinomio cuyo coeficiente principal es una potencia m-ésima en $\mathbb{F}_q$ y que satisface las condiciones (a), (b) y (c) a continuación:*
(a) $f(t) = t^d f_1(t)$ con $F_1(t) \in \mathbb{F}_q[T]$, $f_1(0) \neq 0$ y $\mathrm{mcd}(d, m) = 1$.

(b) $deg\,(f(t)) = m$.

(c) Para cada $\gamma \in S_0$*, todas las raíces de la ecuación* $f(t) = \gamma^m$ *pertenecen a* S_0.

Definimos los cuerpos de funciones $F_n/\mathbb{F}_q$ $(n \geq 0)$ *recursivamente por* $F_0 := \mathbb{F}_q(x_0)$ *y* $F_{n+1} := F_n(x_{i+1})$ *con*

$$x_{i+1}^m = f(x_i) \qquad (para\ i \geq 0).$$

Entonces $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ *es una torre de cuerpos de funciones sobre* $\mathbb{F}_q$ *con las siguientes propiedades:*

(i) F_{i+1}/F_i *es una extensión cíclica moderada de grado* m*, para todo* $i \geq 0$.

(ii) *Si* $P \in \mathbb{P}(F_0)$ *es un lugar ramificado en* F_n/F_0*, para algún* $n \geq 1$*, entonces* P *es un cero de* $x_0 - \gamma$ *para algún* $\gamma \in S_0$.

(iii) *El polo* P_∞ *de* x_0 *en* F_0 *se descompone completamente en* F_n/F_1*, para todo* $n \geq 1$.

(iv) $\lambda(\mathcal{F}) \geq 2/(\#S_0 - 2) > 0$.

Observación 3.1.3 . Observar que el teorema también se obtiene si se reemplaza la hipótesis sobre la existencia del conjunto S_0 y la dada en la condición (c) por la siguiente:

(c') Supongamos que existe $\psi(t) \in \mathbb{F}_q[T]$ tal que

(c_1') $B := \{\gamma \in \bar{\mathbb{F}}_q | \psi(\gamma^m) = 0\} \subseteq \mathbb{F}_q$.

(c_2') $B = \{\gamma \in \bar{\mathbb{F}}_q | \psi(f(\gamma)) = 0\}$.

(c_3') $0 \in B$.

En este caso, sea $S_0 = B$. Entonces S_0 satisface que $0 \in S_0 \subseteq \mathbb{F}_q$. También se cumple la hipótesis (c) del teorema, es decir, que para cada $\gamma \in S_0$, todas las raíces de la ecuación $f(t) = \gamma^m$ pertenecen a S_0. En efecto, sea $\gamma \in S_0$ y sea β tal que $f(\beta) = \gamma^m$. Entonces $\psi(f(\beta)) = \psi(\gamma^m) = 0$ pues $\gamma \in S_0$ y por lo tanto $\beta \in S_0$.

Veamos ahora un resultado que asegura la finitud del espacio de ramificación para cierta clase de sucesiones de cuerpos de funciones de tipo Kummer. Recordemos que si $g(T) \in \mathbb{F}_q[T]$, denotamos por Z_g al conjunto de los ceros de $g(T)$ en una clausura algebraica $\bar{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Teorema 3.1.4. *Sea $m \geq 2$ un entero con $\mathrm{mcd}(m, q) = 1$. Sea $\mathcal{F} = (F_0, F_1, F_2, \dots)$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ definida recursivamente por la ecuación*

$$y^m = \frac{b_1(x)}{b_2(x)},$$

donde $b_1(T)$, $b_2(T) \in \mathbb{F}_q[T]$ con $deg\,(b_1(T)) = m$, $deg\,(b_2(T)) = m - r$ y $\mathrm{mcd}(m, r) = 1$. Supongamos que existe un subconjunto S_0 de $\mathbb{F}_q$ tal que:

(i) $0 \in S_0$;

(ii) $Z_{b_2} \subset S_0$; *y*

(iii) *para todo $\gamma \in S_0$, $Z_{H_\gamma} \subset S_0$, donde $H_\gamma(T) = b_2(T)\gamma^m - b_1(T)$.*

Entonces $\mathcal{F}$ es una sucesión moderada con espacio de ramificación finito. Más aún, si $P \in \mathbb{P}(F_0)$ es un lugar ramificado en la sucesión entonces $P = P_\infty$ es el polo de x_0 en F_0 o P es un cero de $x_0 - \gamma$ para algún $\gamma \in S_0$.

Demostración. Por la parte (ii) del Teorema 1.4.4 del Capítulo 1, sabemos que el polo P_∞ de x_0 en F_0 está totalmente ramificado en la sucesión y que $\mathbb{F}_q$ es el cuerpo total de constantes de todos los F_n. Además, cada extensión F_n/F_{n-1} es una extensión moderada de grado m (pues $F_n = F_{n-1}(y)$ con $y^m = u \in F_{n-1}$, donde $\mathrm{mcd}(m, char\,\mathbb{F}_q) = 1$, y por el Teorema 1.2.14, $e(Q|P)$ divide a m para todo $P \in \mathbb{P}(F_{n-1})$, $Q \in \mathbb{P}(F_n)$ y $Q|P$).

Sea $P \in \mathbb{P}(F_0)$ un lugar ramificado en F_n/F_0. Sea $Q \in \mathbb{P}(F_n)$ un lugar arriba de P tal que $e(Q|P) > 1$. Denotamos por $P_i = Q \cap F_i$ a la restricción del lugar Q al cuerpo F_i para todo $i = 0, \dots, n$. Como $Q|P$ está ramificado, entonces $P_{i+1}|P_i$ es ramificado para algún i.

De la ecuación

$$x_{i+1}^m = \frac{b_1(x_i)}{b_2(x_i)}, \tag{3.1.1}$$

y de la teoría de ramificación de extensiones de Kummer (Teorema 1.2.14 del Capítulo 1), se obtiene que P_{i+1} es un cero o un polo de x_{i+1}.

En efecto, si suponemos que $v_{P_{i+1}}(x_{i+1}) = 0$ entonces tenemos que

$$0 = m\, v_{P_{i+1}}(x_{i+1}) = e(P_{i+1}|P_i) v_{P_i}\left(\frac{b_1(x_i)}{b_2(x_i)}\right),$$

y por lo tanto

$$v_{P_i}\left(\frac{b_1(x_i)}{b_2(x_i)}\right) = 0.$$

Nuevamente por el Teorema 1.2.14 del Capítulo 1, tenemos que

$$e(P_{i+1}|P_i) = \frac{m}{r_{P_i}} = \frac{m}{\mathrm{mcd}(m, v_{P_i}(b_1(x_i)/b_2(x_i)))} = \frac{m}{\mathrm{mcd}(m,0)} = 1,$$

y esto contradice el hecho de que $e(P_{i+1}|P_i) > 1$. Luego, $v_{P_{i+1}}(x_{i+1}) > 0$ o $v_{P_{i+1}}(x_{i+1}) < 0$.

Si P_{i+1} es un cero de x_{i+1}, entonces denotando por $z(Q)$ a la clase de residuos de un elemento $z \in F_n$ módulo Q, obtenemos que $x_{i+1}(P_{i+1}) = 0$ y por lo tanto $x_{i+1}(Q) = 0 \in S_0$, por (i). Luego, de la ecuación (3.1.1), tenemos que

$$x_{i+1}^m b_2(x_i) = b_1(x_i),$$

y tomando la clase de residuos módulo Q,

$$0 = x_{i+1}(Q)^m b_2(x_i(Q)) = b_1(x_i(Q)),$$

y por lo tanto $x_i(Q) \in S_0$, por (iii) con $\gamma = 0$.

Si P_{i+1} es un polo de x_{i+1}, entonces

$$0 > m\, v_{P_{i+1}}(x_{i+1}) = e(P_{i+1}|P_i) v_{P_i}\left(\frac{b_1(x_i)}{b_2(x_i)}\right).$$

Aquí tenemos tres opciones:

- si $v_{P_i}(x_i) < 0$ para todo i entonces P es el polo P_∞ de x_0 en F_0;
- si $v_{P_i}(x_i) > 0$ para algún i entonces $x_i(Q) = x_i(P_i) = 0 \in S_0$, por (i);
- si $v_{P_i}(x_i) = 0$ para algún i entonces

$$v_{P_i}(b_2(x_i)) > b_1(x_i) \geq 0,$$

y esto implica que $x_i(Q) = x_i(P_i) = \gamma$ para algún γ tal que $b_2(\gamma) = 0$ y por lo tanto $x_i(Q) = \gamma \in S_0$, por (ii).

En todos los casos en que $P \neq P_\infty$, repitiendo el argumento para x_{i-1}, tenemos que

$$b_2(x_{i-1}(Q))x_i(Q) - b_1(x_{i-1}(Q)) = 0,$$

y por lo tanto $x_{i-1}(Q) \in S_0$, por (iii). Continuando de la misma manera obtenemos $x_{i-2}(Q) \in S_0$, ..., $x_1(Q) \in S_0$, y finalmente $x_0(Q) \in S_0$. Luego la sucesión $\mathcal{F}$ tiene un

espacio de ramificación finito. Más aún, si $P \in \mathbb{P}(F_0)$ es un lugar ramificado en $\mathcal{F}$ y $P \neq P_\infty$ entonces P es un cero de $x_0 - \gamma$ para algún $\gamma \in S_0$.

□

Observación 3.1.5. Observar que el teorema también se obtiene si se reemplazan las hipótesis sobre el conjunto S_0 por las siguientes:

- Supongamos que existe $\psi(t) \in \mathbb{F}_q[T]$ tal que
  - (i) $0 \in B$.
  - (ii) $B := \{\gamma \in \bar{\mathbb{F}}_q | \psi(\gamma^m) = 0\} \subseteq \mathbb{F}_q$.
  - (iii) $B = \{\gamma \in \bar{\mathbb{F}}_q | \psi(b_2(\gamma)) = 0\}$.
  - (iv) $B = \{\gamma \in \bar{\mathbb{F}}_q | \psi\left(\frac{b_1(\gamma)}{b_2(\gamma)}\right) = 0\}$.

  En este caso, $S_0 = B$ satisface las hipótesis del Teorema.

Ejemplo 3.1.6. Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_4$ generada recursivamente por

$$y^3 = \frac{x^3 + 1}{x^2 + x}.$$

En este caso, el conjunto $S_0 = \mathbb{F}_4$ cumple las condiciones del Teorema 3.1.4, y por lo tanto la sucesión tiene un espacio de ramificación finito. En efecto, el cuerpo finito $\mathbb{F}_4$ puede representarse como $\mathbb{F}_4 = \{0, 1, \delta, \delta + 1\}$ donde δ satisface $\delta^2 + \delta + 1 = 0$. Entonces tenemos que

(i) $0 \in S_0$.

(ii) Si $\beta \in \bar{\mathbb{F}}_4$ satisface $b_2(\beta) = \beta^2 + \beta = 0$ entonces $\beta \in S_0$; pues las raíces de $x^2 + x$ son 0 y 1 y ambos están en S_0.

(iii) Para todo $\gamma \in S_0$, si $\beta \in \bar{\mathbb{F}}_4$, satisface $b_2(\beta)\gamma^3 = b_1(\beta)$, es decir, $\gamma^3(\beta^2+\beta) = \beta^3+1$, entonces $\beta \in S_0$. En efecto:

- si $\gamma = 0$ y $0 = \beta^3 + 1 = (\beta + 1)(\beta^2 + \beta + 1)$ entonces $\beta = 1, \delta, \delta + 1 \in S_0$.
- Si $\gamma = 1$ y $\beta^2 + \beta = \beta^3 + 1$ entonces $\beta = 1 \in S_0$, es una raíz triple.
- Si $\gamma = \delta$ y $\delta^3(\beta^2 + \beta) = \beta^3 + 1$ entonces $\beta = 1 \in S_0$, es una raíz triple.
- Si $\gamma = \delta + 1$ y $(\delta + 1)^3(\beta^2 + \beta) = \beta^3 + 1$ entonces $\beta = 1 \in S_0$, es una raíz triple.

Luego, el Teorema 3.1.4 nos asegura que el espacio de ramificación es finito y está contenido en el conjunto $\mathbb{F}_4$.

Ejemplo 3.1.7(Continuación del Ejemplo 2.3.1)**.** En el Ejemplo 2.3.1 consideramos la torre de cuerpos de funciones $\mathcal{F}$ definida sobre $\mathbb{F}_q$ por la ecuación

$$y^m = \frac{x^m + \alpha f(x) - \alpha}{f(x)},$$

donde $\mathbb{F}_q$ contiene al cuerpo de descomposición de $T^m - \alpha$ para algún $\alpha \in \mathbb{F}_q$ y $f(T)$ es un polinomio en $\mathbb{F}_q[T]$, de grado $m-r$ con m y r coprimos. Allí probamos que $|Split(\mathcal{F}/F_0)| \geq m$.

Ahora, si existe un conjunto S_0 con las propiedades del Teorema 3.1.4, entonces tenemos que el espacio de ramificación de la torre es finito, más aún, $Ram(\mathcal{F}/F_0) \subseteq S_0 \subseteq \mathbb{F}_q$.

En este caso, el Teorema 3.1.1 nos asegura que si $t = \nu(\mathcal{F}/F_0)$ y $s = \sum_{P \in Ram\mathcal{F}} deg\, P$ entonces

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_0) - 2 + s} \geq \frac{2m}{s-2}.$$

En particular si consideramos $m = 2$, $q = 9$, $\alpha = -1$ y $f(x) = x$ tenemos que $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ es una torre sobre $\mathbb{F}_9$ definida recursivamente por la ecuación

$$y^2 = \frac{x^2 - x + 1}{x}.$$

En este caso, consideremos $S_0 = \{0, 1, 2\} \subset \mathbb{F}_9$ donde $\mathbb{F}_9 = \mathbb{F}_3(\delta)$ con $\delta^2 + \delta + 2$. Entonces tenemos que

(i) $0 \in S_0$.

(ii) Si $\beta \in \bar{\mathbb{F}}_9$ satisface $b_2(\beta) = \beta = 0$ entonces $\beta \in S_0$.

(iii) Para todo $\gamma \in S_0$ si $\beta \in \bar{\mathbb{F}}_9$ satisface $\beta\,\gamma^2 = \beta^2 - \beta + 1$ entonces $\beta \in S_0$; en efecto:

- si $\gamma = 0$ y $\beta^2 - \beta + 1 = 0$ entonces $\beta = 2 \in S_0$, es una raíz doble.
- Si $\gamma = 1$ y $\beta = \beta^2 - \beta + 1$ entonces $\beta = 1 \in S_0$, es una raíz doble.
- Si $\gamma = 2$ y $\beta\, 2^2 = \beta^2 - \beta + 1$ entonces $\beta = 1 \in S_0$, es una raíz doble.

Luego, por el Teorema 3.1.4 tenemos que el espacio de ramificación de la torre $\mathcal{G}$ es finito y está contenido en el conjunto $\{P_{x_0}, P_{x_0-1}, P_{x_0-2}, P_\infty\}$. Utilizando el Teorema 3.1.1,

tenemos que

$$\lambda(\mathcal{G}) \geq \frac{4}{4-2} = 2,$$

y como sabemos que

$$\lambda(\mathcal{G}) \leq \sqrt{9} - 1 = 2,$$

entonces la torre $\mathcal{G}$ es asintóticamente óptima sobre $\mathbb{F}_9$ y $\lambda(\mathcal{G}) = 2$.

Si consideramos $m = 2$, $q = 9$, $\mathbb{F}_9 = \mathbb{F}_3(\delta)$ con $\delta^2 + \delta + 2 = 0$, $\alpha = -1$ y $f(x) = x + 1$ tenemos que $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ es una torre de cuerpos de funciones sobre $\mathbb{F}_9$ definida recursivamente por la ecuación

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

En este caso,

$$S_0 = \{0, 1, 2, \delta, \delta^3, \delta^5, \delta^7\},$$

satisface las hipótesis del Teorema 3.1.4. Luego, $\mathcal{H}$ es una torre asintóticamente buena sobre $\mathbb{F}_9$ y tenemos que

$$\lambda(\mathcal{H}) \geq \frac{2}{3}.$$

3.2. Subsucesiones y supersucesiones

Definición 3.2.1. Sean $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ y $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ sucesiones de cuerpos de funciones sobre el cuerpo finito $\mathbb{F}_q$. Decimos que $\mathcal{G}$ es una *subsucesión* de $\mathcal{F}$ si para cada $i \geq 0$ existe un índice $j = j(i)$ y una aplicación $\varphi_i : G_i \to F_j$ sobre $\mathbb{F}_q$. En este caso decimos también que F es una *supersucesión* de $\mathcal{G}$.

Cuando las sucesiones son en realidad torres de cuerpos de funciones, decimos que $\mathcal{G}$ es una *subtorre* de $\mathcal{F}$ o que F es una *supertorre* de $\mathcal{G}$.

El siguiente resultado es útil en el trabajo de torres y subtorres.

Proposición 3.2.2. [**Sti09**, Proposición 7.2.8] *Sea $\mathcal{G}$ una subtorre de $\mathcal{F}$. Entonces $\lambda(\mathcal{G}) \geq \lambda(\mathcal{F})$. En particular se tiene que:*

(a) Si $\mathcal{F}$ es asintóticamente buena, entonces $\mathcal{G}$ es asintóticamente buena.

(b) Si $\mathcal{G}$ es asintóticamente mala, entonces $\mathcal{F}$ es asintóticamente mala.

Observación 3.2.3. Otra prueba de optimalidad de la torre $\mathcal{G}$ del Ejemplo 3.1.7 sobre $\mathbb{F}_9$ se da en [**GSR03**], utilizando el hecho de que es una subtorre de la torre $\mathcal{H}$ definida recursivamente por la ecuación

$$z_{i+1}^2 = \frac{z_i^2 + 1}{2z_i},$$

sobre $\mathbb{F}_{p^2}$ con característica $p \geq 3$. Para probar este hecho debemos observar que en un cuerpo de característica 3

$$\frac{x^2 - x + 1}{x} = \frac{(x+1)^2}{4x},$$

utilizando esto y el cambio de variables $x_i = z_{i+1}^2$ podemos probar que la torre definida recursivamente por la ecuación

$$x_{i+1}^2 = \frac{x_i^2 - x_i + 1}{x_i},$$

es una subtorre de la torre definida recursivamente por la ecuación

$$z_{i+1}^2 = \frac{z_i^2 + 1}{2z_i}.$$

En efecto, como

$$x_i = z_{i+1}^2 = \frac{z_i^2 + 1}{2z_i},$$

entonces

$$x_i^2 = z_{i+1}^4 = \frac{(z_i^2+1)^2}{4z_i^2} = \frac{(x_{i-1}+1)^2}{4x_{i-1}} = \frac{x_{i-1}^2 - x_{i-1} + 1}{x_{i-1}}.$$

En el mismo trabajo, [**GSR03**], se prueba que la torre $\mathcal{H}$ sobre $\mathbb{F}_9$ es asintóticamente buena obteniéndose la misma cota para su límite.

Ejemplo 3.2.4. Consideremos la torre $\mathcal{G} = (G_0, G_1, \ldots)$ recursiva generada por

$$y^2 = \frac{(x-1)^2}{2x}$$

sobre $\mathbb{F}_9$. En este caso, si $S_0 = \{0, 1, 2\} \subset \mathbb{F}_9$ entonces tenemos que

(i) $0 \in S_0$.

(ii) Si $\beta \in \bar{\mathbb{F}}_9$ satisface $b_2(\beta) = \beta = 0$ entonces $\beta \in S_0$.

(iii) Para todo $\gamma \in S_0$ si $\beta \in \bar{\mathbb{F}}_9$ satisface $2\beta\gamma^2 = \beta^2 - 2\beta + 1$ entonces $\beta \in S_0$; en efecto:

- si $\gamma = 0$ y $\beta^2 - 2\beta + 1 = 0$ entonces $\beta = 1 \in S_0$, es una raíz doble.

- Si $\gamma = 1$ y $2\beta = \beta^2 - 2\beta + 1$ entonces $\beta = 2 \in S_0$, es una raíz doble.
- Si $\gamma = 2$ y $2\beta\, 2^2 = \beta^2 - \beta + 1$ entonces $\beta = 2 \in S_0$, es una raíz doble.

Luego, por el Teorema 3.1.4 tenemos que el espacio de ramificación de la torre $\mathcal{G}$ es finito y está contenido en el conjunto $\{P_{x_0}, P_{x_0-1}, P_{x_0-2}, P_\infty\}$. Observar que esta torre puede escribirse como

$$h(y) = \frac{h(x) + f(x) - 1}{f(x)},$$

con $h(T) = T^2 + 2$ y $f(T) = 2T$ y coincide con la del Ejemplo 2.2.10, por lo tanto $|Split(\,G/G_0)| \geq 2$. Utilizando el Teorema 3.1.1, tenemos que

$$\lambda(\mathcal{G}) \geq \frac{4}{4-2} = 2,$$

y como sabemos que

$$\lambda(\mathcal{G}) \leq \sqrt{9} - 1 = 2,$$

entonces la torre $\mathcal{G}$ es asintóticamente óptima sobre $\mathbb{F}_9$ y $\lambda(\mathcal{G}) = 2$.

Observación 3.2.5. Observar que la torre del Ejemplo 3.2.4 es una supertorre de la torre $\mathcal{F}$ de [**GSR03**], definida recursivamente por la ecuación

$$z_{i+1}^2 = \frac{z_i^2}{z_i - 1},$$

sobre $\mathbb{F}_9$ (ver Ejemplo 2.2.6). Utilizando el cambio de variables $z_i = x_i^2 + 1$ podemos probar que la torre definida recursivamente por la ecuación

$$z_{i+1}^2 = \frac{z_i^2}{z_i - 1},$$

es una subtorre de la torre definida recursivamente por la ecuación

$$x_{i+1}^2 = \frac{(x_i - 1)^2}{2x_i}.$$

En efecto, como

$$z_{i+1} = x_{i+1}^2 + 1 = \frac{(x_i - 1)^2}{2x_i} + 1 = \frac{x_i^2 + 1}{2x_i},$$

entonces

$$z_{i+1}^2 = \left(\frac{x_i^2 + 1}{2x_i}\right)^2 = \frac{(x_i^2 + 1)^2}{4x_i^2} = \frac{z_i^2}{z_i - 1}.$$

Luego, el Ejemplo 3.2.4 da otra prueba de la optimalidad de la torre $\mathcal{F}$ sobre $\mathbb{F}_9$.

Supongamos que $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ en una sucesión recursiva de tipo (a, b) sobre $\mathbb{F}_q$. Sean f, $\tilde{a}$ y $\tilde{b}$ funciones racionales con coeficientes en $\mathbb{F}_q$ tales que

$$\tilde{a} \circ f \circ b = \tilde{b} \circ f \circ a.$$

Para $i \geq 0$ sea $z_i = f(a(x_i))$. Entonces, como $a(x_{i+1}) = b(x_i)$, tenemos que

$$\tilde{a}(z_{i+1}) = \tilde{a}(f(a(x_{i+1}))) = \tilde{a}(f(b(x_i))) = \tilde{b}(f(a(x_i))) = \tilde{b}(z_i). \tag{3.2.1}$$

Por lo tanto, $z_0 = f(a(x_0))$ también es trascendente sobre $\mathbb{F}_q$ y definiendo $E_0 = \mathbb{F}_q(z_0)$ y $E_{i+1} = E_i(z_{i+1})$ para $i \geq 0$ tenemos una sucesión recursiva $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$, de tipo $(\tilde{a}, \tilde{b})$ pues $E_i \subset F_i$ para todo $i \geq 0$. Obviamente, estamos interesados en el caso $E_i \subsetneq F_i$ para una cantidad infinita de $i \geq 0$ para que $\mathcal{E}$ sea esencialmente diferente de $\mathcal{F}$. Si $E_i \subsetneq F_i$ para infinitos $i \geq 0$ decimos que $\mathcal{E}$ es una *subsucesión propia* de $\mathcal{F}$ y si $\mathcal{F}$ y $\mathcal{E}$ son torres diremos que $\mathcal{E}$ es una *subtorre propia* de $\mathcal{F}$.

A continuación damos condiciones sencillas de verificar para garantizar que una subsucesión de $\mathcal{F}$ construida usando (3.2.1) sea una subsucesión propia. Recordar que el grado de una función racional $a \in \mathbb{F}_q(T)$ se define como $deg\,(a) = \max\{deg\,(a_1), deg\,(a_2)\}$ donde a_1, $a_2 \in \mathbb{F}_q[T]$ son polinomio coprimos tales que $a = a_1/a_2$.

Proposición 3.2.6. *Sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una sucesión recursiva de tipo (a, b) sobre $\mathbb{F}_q$. Sea $\{x_i\}_{i=0}^{\infty}$ una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ tales que $F_{i+1} = F_i(x_{i+1})$ y $a(x_{i+1}) = b(x_i)$ para $i \geq 0$ y $F_0 = \mathbb{F}_q(x_0)$. Sean $a_1, a_2 \in \mathbb{F}_q[T]$ polinomios coprimos tales que $a = a_1/a_2$ y $a_1(T) - a_2(T)b(x_i)$ (resp. $a_2(T) - a_1(T)(b(x_i))^{-1}$) es el polinomio mínimo de x_{i+1} sobre F_i para $i \geq 0$ con $deg\,(a_1) \geq 2$ (resp. $deg\,(a_2) \geq 2$). Sea $f \in \mathbb{F}_q(T)$ una función racional tal que* (3.2.1) *vale. Para $i \geq 0$ sea $E_{i+1} = E_i(z_{i+1})$ donde $z_i = f(a(x_i))$ y $E_0 = \mathbb{F}_q(z_0)$. Supongamos que $\tilde{a}_1, \tilde{a}_2 \in \mathbb{F}_q[T]$ son polinomios coprimos tales que $\tilde{a} = \tilde{a}_1/\tilde{a}_2$ y $\tilde{a}_1(T) - \tilde{a}_2(T)\tilde{b}(z_i)$ (resp. $\tilde{a}_2(T) - \tilde{a}_1(T)(\tilde{b}(z_i))^{-1}$) es el polinomio mínimo de z_{i+1} sobre E_i para $i \geq 0$ con $deg\,(\tilde{a}_1) \geq 2$ (resp. $deg\,(\tilde{a}_2) \geq 2$). Si tenemos que:*

$$deg\,(a) \geq deg\,(\tilde{a}), \qquad \text{ó} \qquad \text{mcd}(deg\,(a), deg\,(\tilde{a})) = 1,$$

entonces $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ *es una subsucesión recursiva de* $\mathcal{F}$ *de tipo* $(\tilde{a},\ \tilde{b})$ *tal que* $E_i \subsetneq F_i$, *para todo* $i \geq 0$.

Demostración. Vamos a probar este resultado para el caso en que $a_1(T) - a_2(T)b(x_i)$ es el polinomio mínimo de x_{i+1} sobre F_i ya que la prueba para el otro caso es similar. De esta suposición tenemos que $deg\,(a) = deg\,(a_1)$ y $deg\,(\tilde{a}) = deg\,(\tilde{a}_1)$. Sea $z_0 = f(a(x_0))$. Como f y a son funciones racionales existen polinomios coprimos $h_1,\ h_2 \in \mathbb{F}_q[T]$ tales que $f \circ a = h_1/h_2$. Entonces x_0 es una raíz del polinomio $h_1(T) - h_2(T)z_0 \in E_0[T]$ y $E_0(x_0) = \mathbb{F}_q(z_0, x_0) = F_0$. Luego F_0 es una extensión finita de E_0 y por lo tanto $[F_i : E_0] < \infty$ para $i \geq 0$. Como $E_0 \subset E_i \subset F_i$ tenemos que $[F_i : E_i] < \infty$ para $i \geq 0$. Sea $d_i = [F_i : E_i]$. Tenemos que mostrar que $d_i > 1$ para $i \geq 0$. Supongamos que $d_0 = 1$. Entonces existen polinomios $r_1,\ r_2 \in \mathbb{F}_q[T]$ tales que $x_0 = r_1(z_0)/r_2(z_0)$. Como $z_0 = h_1(x_0)/h_2(x_0)$ y h_1 y h_2 tienen coeficientes en $\mathbb{F}_q$ tendríamos que x_0 es una raíz de un polinomio con coeficientes en $\mathbb{F}_q$ lo cual es imposible pues x_0 es trascendente sobre $\mathbb{F}_q$. Por lo tanto $d_0 > 1$. Ahora, supongamos que $d_i > 1$ y que $d_{i+1} = 1$. Por hipótesis, tenemos que $[E_{i+1} : E_i] = \tilde{d} = deg\,(\tilde{a}_1) = deg\,(\tilde{a})$ y $[F_{i+1} : F_i] = d = deg\,(a_1) = deg\,(a)$. Entonces $\tilde{d} = \tilde{d}d_{i+1} = dd_i$ que contradice el hecho de que o bien $d \geq \tilde{d}$ o bien $\text{mcd}(d, \tilde{d}) = 1$. Luego, $d_{i+1} > 1$. □

Consideremos ahora el caso en que $\mathcal{F}$ es en realidad una torre recursiva de tipo (a, b). En esta situación es natural preguntarse cuándo una subsucesión recursiva $\mathcal{E}$ de $\mathcal{F}$ de tipo $(\tilde{a},\ \tilde{b})$ construida usando (3.2.1) es una torre de cuerpos de funciones (y por lo tanto una subtorre de $\mathcal{F}$). En otras palabras, una serie de preguntas interesantes para responder son las siguientes:

- ¿En qué casos, las extensiones E_{i+1}/E_i son separables y $g(E_i) \longrightarrow \infty$ cuando $i \to \infty$?
- ¿Cuán grande es $g(F_i)$ comparado con $g(E_i)$?
- ¿Cuál es la relación entre $Split(\mathcal{F}/F_0)$ y $Split(\mathcal{E}/E_0)$?
- Si las extensiones F_{i+1}/F_i son de tipo Kummer o Artin-Schreier, ¿las extensiones E_{i+1}/E_i serán del mismo tipo?

Veamos algunos ejemplos en los cuáles podemos responder algunas de estas cuestiones.

Ejemplo 3.2.7. Sea $q = p^{2n}$ donde p es un primo impar. La ecuación de Kummer

$$y^2 = \frac{x^2+1}{2x},$$

define una torre recursiva $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ de tipo (a, b) y fue estudiada en [**GSR03**]. En este caso

$$F_{i+1} = F_i(x_{i+1}) \quad \text{con} \quad x_{i+1}^2 = \frac{x_i^2+1}{2x_i} \quad \text{para } i \geq 0.$$

Tenemos además que $a(T) = T^2$ y $b(T) = (T^2+1)/2T$.

Si consideramos $f(T) = 2T$, $\tilde{a}(T) = T^2$ y $\tilde{b}(T) = (T+2)^2/2T$ entonces se ve fácilmente que

$$(\tilde{a} \circ f \circ b)(T) = \frac{(T^2+1)^2}{T^2} = (\tilde{b} \circ f \circ a)(T)\,,$$

y por lo tanto, la ecuación

$$y^2 = \frac{(x+2)^2}{2x}\,,$$

define una subsucesión propia $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ de tipo $(\tilde{a}, \tilde{b})$ de $\mathcal{F}$ sobre $\mathbb{F}_q$ por la Proposición 3.2.6, donde

$$E_{i+1} = E_i(z_{i+1}) \quad \text{con} \quad z_{i+1}^2 = \frac{(z_i+2)^2}{2z_i} \quad \text{y } z_i = 2x_i^2 \text{ para } i \geq 0\,.$$

Más aún, $\mathcal{E}$ es en realidad una subtorre propia de $\mathcal{F}$ sobre $\mathbb{F}_q$. Esta subtorre fue obtenida en [**MW05**] usando un método debido a Elkies.

Consideremos la torre anterior $\mathcal{E}$ sobre $\mathbb{F}_9$. Sea $f(T) = T+1$, $\hat{a}(T) = T^2$ y $\hat{b}(T) = T^2/(T-1)$. Sobre $\mathbb{F}_9$ tenemos que

$$(\hat{a} \circ f \circ \tilde{b})(T) = \frac{(T^2+1)^2}{T^2} = (\hat{b} \circ f \circ \tilde{a})(T)\,,$$

y por lo tanto la ecuación

$$y^2 = \frac{x^2}{x-1}\,,$$

define una subsucesión recursiva propia $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ de tipo $(\hat{a}, \hat{b})$ de $\mathcal{E}$ sobre $\mathbb{F}_9$ por la Proposición 3.2.6, donde

$$G_{i+i} = G_i(w_{i+1}) \quad \text{con} \quad w_{i+1}^2 = \frac{w_i^2}{w_i - 1} \quad \text{y } w_i = z_i^2 + 1 \text{ para } i \geq 0\,.$$

Más aún, $\mathcal{G}$ es una subtorre propia de $\mathcal{E}$ sobre $\mathbb{F}_9$. La torre $\mathcal{G}$ fue estudiada en [**GSR03**] pero no se menciona que $\mathcal{G}$ es una subtorre de $\mathcal{E}$ sobre $\mathbb{F}_9$.

En los ejemplos anteriores tenemos que las subsucesiones obtenidas utilizando (3.2.1) son en realidad subtorres. Y además tenemos que tanto las torres originales como las subtorres son todas de tipo Kummer.

En el siguiente ejemplo partimos de una torre de cuerpos de funciones sobre $\mathbb{F}_8$ de tipo Artin-Schreier pero la subsucesión que obtenemos a partir de (3.2.1) no es de tipo Artin-Schreier.

Ejemplo 3.2.8. La ecuación de tipo Artin-Schreier

$$y^2 + y = \frac{x^2 + x + 1}{x}\,, \tag{3.2.2}$$

define una torre recursiva $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de tipo (a, b) de cuerpos de funciones sobre $\mathbb{F}_8$ y fue estudiada en [**vdGvdV02**]. En este caso

$$F_{i+1} = F_i(x_{i+1}) \quad \text{con} \quad x_{i+1}^2 + x_{i+1} = \frac{x_i^2 + x_i + 1}{x_i} \quad \text{para } i \geq 0\,,$$

y tenemos que $a(T) = T^2 + T$ y $b(T) = (T^2 + T + 1)/T$. Si $f(T) = 1/T$, $\tilde{a}(T) = T^3 + T^2$ y $\tilde{b}(T) = T/(T^3 + T^2 + T + 1)$ entonces se puede probar que

$$(\tilde{a} \circ f \circ b)(T) = \frac{T^4 + T^2}{T^6 + T^5 + T^3 + T + 1} = (\tilde{b} \circ f \circ a)(T)\,,$$

por lo que la ecuación

$$y^3 + y^2 = \frac{x}{x^3 + x^2 + x + 1}\,,$$

define una subsucesión propia recursiva $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ de tipo $(\tilde{a}, \tilde{b})$ de $\mathcal{F}$ sobre $\mathbb{F}_8$ por la Proposición 3.2.6, donde

$$E_{i+1} = E_i(z_{i+1}) \quad \text{con} \quad z_{i+1}^3 + z_{i+1}^2 = \frac{z_i}{z_i^3 + z_i^2 + z_i + 1}\,,$$

y

$$z_i = \frac{1}{x_i^2 + x_i} \quad \text{para } i \geq 0\,.$$

3.3. Más ejemplos

Utilizando los teoremas de la Sección 3.1 veamos ahora cómo obtener cotas inferiores del límite de torres definidas recursivamente sobre $\mathbb{F}_q$ por una ecuación de la forma

$$y^m = \frac{b_1(x)}{b_2(x)},$$

con $m \geq 2$, $b_1(T), b_2(T) \in \mathbb{F}_q[T] \setminus \mathbb{F}_p[T]$, si $q = p^r$ y $r > 1$.

Ejemplo 3.3.1. El cuerpo $\mathbb{F}_{25}$ se puede representar como $\mathbb{F}_{25} = \mathbb{F}_5(\delta)$ con $\delta^2 + \delta + 2 = 0$. Consideremos la sucesión $\mathcal{I} = (I_0, I_1, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_{25}$ definida recursivamente por

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)}, \tag{3.3.1}$$

con $f(x) = \delta^9 x + 1$. Como $\mathbb{F}_{25}$ contiene al cuerpo de descomposición de $T^2 + 1$, utilizando los resultados del Ejemplo 2.3.1 tenemos que $\mathcal{I}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_{25}$ y además tenemos que

$$\nu(\mathcal{I}/I_0) \geq 2.$$

Consideremos el conjunto $S_0 = \{0, \delta^3, \delta^9, \delta^{15}, \delta^{21}\} \subset \mathbb{F}_{25}$. Veamos que S_0 satisface las condiciones del Teorema 3.1.4. Tenemos que

(i) $0 \in S_0$.

(ii) Si $\beta \in \bar{\mathbb{F}}_{25}$ satisface $f(\beta) = 0$ entonces $\beta = \delta^3 \in S_0$.

(iii) Para todo $\gamma \in S_0$ si $\beta \in \bar{\mathbb{F}}_{25}$ satisface $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta \in S_0$; en efecto:

- Si $\gamma = 0$ y $0 = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^9 \in S_0$ o $\beta = 0 \in S_0$.
- Si $\gamma = \delta^3$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{21} \in S_0$, es una raíz doble.
- Si $\gamma = \delta^9$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{15} \in S_0$, es una raíz doble.
- Si $\gamma = \delta^{15}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{21} \in S_0$, es una raíz doble.
- Si $\gamma = \delta^{21}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{15} \in S_0$, es una raíz doble.

Luego, el Teorema 3.1.4 nos asegura que el espacio de ramificación es finito y está contenido en el conjunto

$$\{P_\infty, P_{x_0}, P_{x_0 - \delta^3}, P_{x_0 - \delta^9}, P_{x_0 - \delta^{15}}, P_{x_0 - \delta^{21}}\}.$$

Entonces $|Ram(\mathcal{I}/I_0)| \leq 6$ y por el Teorema 3.1.1 tenemos que

$$\lambda(\mathcal{I}) \geq \frac{2 \cdot 2}{6-2} = 1,$$

y por lo tanto la torre $\mathcal{I}$ es asintóticamente buena sobre $\mathbb{F}_{25}$.

Observación 3.3.2. Observar que la torre $\mathcal{I}$ puede escribirse también como la torre recursiva sobre $\mathbb{F}_{25}$ generada por la ecuación

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)},$$

con $f(x) = \delta^{21}x + 1$, utilizando el cambio de variables $X = 2x$, $Y = 2y$. En ambos casos se obtiene el mismo conjunto S_0 y por lo tanto el Teorema 3.1.4 arroja los mismos resultados.

Si utilizamos el cambio de variables $X = \delta^3 x$, $Y = \delta^3 Y$ vemos que otra ecuación que define la misma torre es la ecuación

$$y^2 = \frac{x^2 - \tilde{\alpha} f(x) + \tilde{\alpha}}{f(x)},$$

con $f(x) = 2x + 1$ y $\tilde{\alpha} = 2$. En este caso, tenemos una ecuación con coeficientes en $\mathbb{F}_5$. El conjunto S_0 correspondiente es $S_0 = \{0, 1, 2, 3, 4\}$; por lo tanto se obtiene la misma cota para el límite de la torre.

Utilizando el cambio de variables $X = \delta^{18}x$, $Y = \delta^{18}y$, la ecuación anterior se transforma en

$$y^2 = \frac{x(x+2)}{x+1}.$$

Utilizando esta ecuación, A. Garcia, H. Stichtenoth y H. Rück probaron, en [**GSR03**], que la torre era asintóticamente buena y que su límite es 1.

Ejemplo 3.3.3. El cuerpo $\mathbb{F}_{81}$ se puede representar como $\mathbb{F}_{81} = \mathbb{F}_3(\delta)$ con $\delta^4 + 2\delta + 2 = 0$. Consideremos la sucesión $\mathcal{J} = (J_0, J_1, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_{81}$ definida recursivamente por

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)}, \tag{3.3.2}$$

con $f(x) = \delta^5 x + \delta^{10}$. Como $\mathbb{F}_{81}$ contiene al cuerpo de descomposición de T^2+1, utilizando los resultados del Ejemplo 2.3.1 tenemos que $\mathcal{J}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_{81}$ y además tenemos que

$$\nu(\mathcal{J}/J_0) \geq 2.$$

Consideremos el conjunto $S_0 = \{0, \delta^5, \delta^{15}, \delta^{25}, \delta^{35}, \delta^{45}, \delta^{55}, \delta^{65}, \delta^{75}, \} \subset \mathbb{F}_{81}$. Veamos que S_0 satisface las condiciones del Teorema 3.1.4. Tenemos que

(i) $0 \in S_0$.

(ii) Si $\beta \in \bar{\mathbb{F}}_{81}$ satisface $f(\beta) = 0$ entonces $\beta = \delta^{45} \in S_0$.

(iii) Para todo $\gamma \in S_0$ si $\beta \in \bar{\mathbb{F}}_{81}$ satisface $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta \in S_0$; en efecto:

- Si $\gamma = 0$ y $0 = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{35} \in S_0$ o $\beta = \delta^{65} \in S_0$.
- Si $\gamma = \delta^5$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{75} \in S_0$ o $\beta = 0 \in S_0$.
- Si $\gamma = \delta^{15}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{15} \in S_0$, es una raíz doble.
- Si $\gamma = \delta^{25}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^5 \in S_0$ o $\beta = \delta^{55} \in S_0$.
- Si $\gamma = \delta^{35}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{25} \in S_0$, es una raíz doble.
- Si $\gamma = \delta^{45}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{75} \in S_0$ o $\beta = 0 \in S_0$.
- Si $\gamma = \delta^{55}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{15} \in S_0$, es una raíz doble.
- Si $\gamma = \delta^{65}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^5 \in S_0$ o $\beta = \delta^{55} \in S_0$.
- Si $\gamma = \delta^{75}$ y $\gamma^2 f(\beta) = \beta^2 - f(\beta) + 1$ entonces $\beta = \delta^{25} \in S_0$, es una raíz doble.

Luego, el Teorema 3.1.4 nos asegura que el espacio de ramificación es finito y está contenido en el conjunto

$$\{P_\infty, P_{x_0}, P_{x_0-\delta^5}, P_{x_0-\delta^{15}}, P_{x_0-\delta^{25}}, P_{x_0-\delta^{35}}, P_{x_0-\delta^{45}}, P_{x_0-\delta^{55}}, P_{x_0-\delta^{65}}, P_{x_0-\delta^{75}}\}.$$

Entonces $|Ram(\mathcal{J}/J_0)| \leq 10$ y por el Teorema 3.1.1 tenemos que

$$\lambda(\mathcal{J}) \geq \frac{2 \cdot 2}{10 - 2} = \frac{1}{2}$$

y por lo tanto la torre $\mathcal{J}$ es asintóticamente buena sobre $\mathbb{F}_{81}$.

Observación 3.3.4. La torre $\mathcal{J}$ puede definirse también utilizando $f(x) = \delta^{45}x + \delta^{10}$. Utilizando el cambio de variables $X = 2x$, $Y = 2y$ se muestra que ambas ecuaciones definen la misma torre sobre $\mathbb{F}_{81}$.

Ejemplo 3.3.5. Consideremos $\mathbb{F}_{81} = \mathbb{F}_3(\delta)$ con $\delta^4+2\delta+2 = 0$ y la torre $\mathcal{K} = (K_0, K_1, \ldots)$ de cuerpos de funciones $K_n/\mathbb{F}_{81}$ definida recursivamente por la ecuación

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)},$$

donde $f(x) = \delta^{15}x + \delta^{30}$.

Como $\mathbb{F}_{81}$ contiene al cuerpo de descomposición de $T^2 + 1$, utilizando los resultados del Ejemplo 2.3.1 tenemos que $\mathcal{K}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_{81}$ y además, el espacio de descomposición satisface

$$\nu(\mathcal{K}/K_0) \geq 2.$$

Utilizando el conjunto $S_0 = \{0, \delta^5, \delta^{15}, \delta^{25}, \delta^{35}, \delta^{45}, \delta^{55}, \delta^{65}, \delta^{75}, \} \subset \mathbb{F}_{81}$ y los resultados de los teoremas anteriores tenemos que

$$|Ram(\mathcal{K}/K_0)| \leq 10.$$

Por lo tanto, la torre es asintóticamente buena sobre $\mathbb{F}_{81}$ y tenemos que

$$\lambda(\mathcal{K}) \geq \frac{2 \cdot 2}{10 - 2} = \frac{1}{2}.$$

Observación 3.3.6. La torre $\mathcal{K}$ puede definirse también utilizando $f(x) = \delta^{55}x + \delta^{30}$. Utilizando el cambio de variables $X = 2x$, $Y = 2y$ se muestra que ambas ecuaciones definen la misma torre sobre $\mathbb{F}_{81}$.

Ejemplo 3.3.7. Consideramos la torre $\mathcal{L} = (L_0, L_1, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_9$, con $\mathbb{F}_9 = \mathbb{F}_3(\delta)$ y $\delta^2 + \delta + 1 = 0$; definida recursivamente por la ecuación

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)},$$

con $f(x) = 2x + 1$.

En este caso, utilizando los resultados del Ejemplo 2.3.1, tenemos que $\mathcal{L}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_9$ y además $\mathrm{Split}(\mathcal{L}/L_0) \supseteq \{P_{x_0-\delta^2}, P_{x_0-\delta^6}\}$, y por lo tanto

$$\nu(\mathcal{L}/L_0) \geq 2.$$

El conjunto $S_0 = \{0, 1, 2, \delta, \delta^3, \delta^5, \delta^7\}$ satisface las condiciones del Teorema 3.1.4, y por lo tanto tenemos que

$$\lambda(\mathcal{L}) \geq \frac{2 \cdot 2}{8-2} = \frac{2}{3}.$$

Luego, la torre $\mathcal{L}$ es asintóticamente buena sobre $\mathbb{F}_9$.

A continuación estudiamos una familia de torres de cuerpos de funciones sobre $\mathbb{F}_q$ de tipo Kummer que satisfacen las condiciones del Teorema 3.1.1.

Teorema 3.3.8. *Sea $m \geq 2$ un entero con $\mathrm{mcd}(m, q) = 1$ y sea β en $\mathbb{F}_q^*$. Supongamos que $h(t) \in \mathbb{F}_q[t]$ es un polinomio separable de grado $m - r$ con $\mathrm{mcd}(m, r) = 1$, $1 \leq r \leq m-1$ y $h(0) = h_0 \neq 0$, que el polinomio $T^m - (\beta/h_0)$ se descompone completamente en $\mathbb{F}_q$ y que existe un subconjunto S_0 de $\mathbb{F}_q$ que satisface:*

(a) $0 \in S_0$;

(b) $Z_h \subset S_0$;

(c) para cada $\delta \in S_0$, $Z_{H_\gamma} \subset S_0$, donde $H_\delta(t) = h(t)\gamma^m - \beta\, t^m$.

Definimos cuerpos de funciones $F_n/\mathbb{F}_q$ $(n \geq 0)$ recursivamente por $F_0 := \mathbb{F}_q(x_0)$ y $F_{n+1} := F_n(x_{i+1})$ con

$$x_{i+1}^m = \frac{\beta\, x_i^m}{h(x_i)} \qquad (\text{para } i \geq 0).$$

Entonces $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ es una torre de cuerpos de funciones sobre $\mathbb{F}_q$ con las siguientes propiedades:

(i) *F_{i+1}/F_i es una extensión moderada de grado m, para todo $i \geq 0$. Si además β es una potencia m-ésima en $\mathbb{F}_q$ entonces F_{i+1}/F_i es una extensión cíclica.*

(ii) *Sea $P \in \mathbb{P}(F_0)$ un lugar ramificado en F_n/F_0, para algún $n \geq 1$. Entonces P es el polo de x_0 en F_0 o es un cero de $x_0 - \gamma$ para algún $\gamma \in S_0 \setminus \{0\}$.*

(iii) *El cero P_0 de x_0 en F_0 se descompone completamente en F_n/F_1, para todo $n \geq 1$.*

(iv) $\lambda(\mathcal{F}) \geq 2/(\#S_0 - 2) > 0$.

Demostración. Como la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ satisface las condiciones del Teorema 1.4.4 tenemos que $\mathcal{F}$ es una sucesión recursiva de cuerpos de funciones sobre $\mathbb{F}_q$. Más aún, sabemos que el polo P_∞ de x_0 en F_0 es totalmente ramificado en todas las extensiones. Como F_{n+1}/F_n es una extensión cíclica de grado m (esto se obtiene de la ecuación definitoria y del hecho que $\mathrm{mcd}(m, q) = 1$, ya que si $P_n \in \mathbb{P}(F_n)$ y $P_n | P_\infty$ entonces $F_{n+1} = F_n(y)$ con $y^m = u$ y $v_{P_n}(u) = v_{P_n}(\beta\, x_n^m / h(x_n)) = -r^{n+1}$ con $\mathrm{mcd}(m, -r^{n+1}) = 1$), entonces la extensión F_{n+1}/F_n es moderada.

Mostremos ahora por inducción que el cero P_0 de x_0 en F_0 se descompone completamente. Sea $Q \in \mathbb{P}(F_n)$ un cero de x_0. Entonces Q es un cero de $x_0, x_1, \ldots, x_n$, pues si suponemos que es cierto para algún x_k entonces tenemos que

$$m v_Q(x_{k+1}) = v_Q\left(\frac{\beta\, x_k^m}{h(x_k)}\right) = m v_Q(x_k) > 0,$$

y por lo tanto Q es un cero de x_{k+1}.

Dividiendo por x_n^m la ecuación

$$x_{n+1}^m = \frac{\beta\, x_n^m}{h(x_n)},$$

y llamando $u := x_{n+1}/x_n$ obtenemos

$$u^m = \frac{\beta}{z}, \tag{3.3.3}$$

donde la función z satisface $z \in \mathcal{O}_Q^*$ (pues $v_Q(z) = v_Q(h(x_n)) = 0$) y por lo tanto $z(Q) \in \mathbb{F}_q^*$. (Observar que si $h(T) = h_{m-r}T^{m-r} + \cdots + h_1 T + h_0$ entonces $z(Q) = h_0 \in \mathbb{F}_q^*$).

La reducción módulo Q de la ecuación 3.3.3 es

$$u^m = \frac{\beta}{z(Q)},$$

y como la ecuación $T^m = \beta / z(Q)$ tiene m raíces distintas en $\mathbb{F}_q$, entonces (usando el Teorema de Kummer 1.2.8) tenemos que el lugar Q se descompone completamente en F_{n+1}/F_n.

Por lo tanto, el lugar $P_0 = P_{x_0}$ se descompone completamente en la sucesión.

Tenemos que la ecuación

$$x_{n+1}^m = \frac{\beta\, x_n^m}{h(x_n)},$$

define una sucesión recursiva de cuerpos de funciones. Para probar que es torre debemos mostrar que el género satisface $g(F_n) \to \infty$ cuando $n \to \infty$.

Como sabemos que P_0 se descompone completamente en todas las extensiones entonces tenemos que

$$N(F_n) \geq [F_n : F_0] = m^n.$$

Usando este resultado y el teorema de Hasse-Weil tenemos que $g(F_n) \to \infty$ cuando $n \to \infty$.

Hasta aquí hemos probado que $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ es una torre de cuerpos de funciones con las propiedades (i) y (iii) del Teorema 3.3.8.

Observar que con las hipótesis pedidas sobre el conjunto S_0 se cumplen las hipótesis del Teorema 3.1.4 y por lo tanto, todo lugar de F_0 que ramifica en la torre es o bien el polo de x_0 en F_0 o es un cero de $x_0 - \gamma$ para algún $\gamma \in S_0$. Pero $0 \in S_0$ y ya sabemos que P_{x_0} se descompone completamente en la torre, por lo tanto tenemos que la propiedad (ii) vale. Ahora podemos aplicar el Teorema 3.1.1. Sean

$$S = \{P \in \mathbb{P}(F_0) | P \text{ es un cero de } x_0 - \gamma \text{ para algún } \gamma \in S_0 \setminus \{0\}\} \cup \{P_\infty\},$$

y

$$T = \{P_0, \text{ el cero de } x_0 \text{ en } F_0\}.$$

El Teorema 3.1.1 nos da directamente que

$$\lambda(\mathcal{F}) \geq \frac{2}{\#S_0 - 2}.$$

□

Observación 3.3.9. Observar que el teorema también se obtiene si se reemplazan las hipótesis sobre la existencia del conjunto S_0 y sus propiedades por las siguientes:

- Supongamos que existe $\psi(t) \in \mathbb{F}_q[T]$ tal que
  (a) $B := \{\gamma \in \bar{\mathbb{F}_q} | \psi(\frac{1}{\gamma^m}) = 0\} \subseteq \mathbb{F}_q$.
  (b) $B = \{\gamma \in \bar{\mathbb{F}_q} | \psi(\frac{h(\gamma)}{\beta\, \gamma^m}) = 0\}$.
  (c) $\psi(0) = 0$.

En efecto, sea $S_0 = B \cup \{0\}$. Entonces S_0 satisface que $0 \in S_0 \subseteq \mathbb{F}_q$. Veamos que cumple la hipótesis del Teorema 3.3.8, es decir, que para cada $\gamma \in S_0$, todas las raíces de las ecuaciones $h(t) = 0$ y $h(t) - \beta \left(\frac{t}{\gamma}\right)^m = 0$, para $\gamma \neq 0$, pertenecen a S_0.

Sea $\delta \in \bar{\mathbb{F}}_q$ tal que $h(\delta) = 0$. Entonces como $h(0) \neq 0$ tenemos que $\frac{h(\delta)}{\beta\,\delta^m} = 0$ y como $\psi(0) = 0$ entonces

$$\psi\left(\frac{h(\delta)}{\beta\,\delta^m}\right) = 0,$$

y por lo tanto $\delta \in S_0$.

Si $0 \neq \gamma \in S_0$, entonces $\gamma \in B$. Sea $\delta \in \bar{\mathbb{F}}_q$ tal que $\frac{h(\delta)}{\beta\,\delta^m} = \frac{1}{\gamma^m}$. Entonces

$$\psi\left(\frac{h(\delta)}{\beta\,\delta^m}\right) = \psi\left(\frac{1}{\gamma^m}\right) = 0,$$

pues $\gamma \in B$. Luego, tenemos que $\delta \in S_0$ y por lo tanto el teorema vale.

Ejemplo 3.3.10. Considerar la torre de funciones sobre $\mathbb{F}_9 = \mathbb{F}_3(\delta)$ con $\delta^2 + \delta + 2 = 0$ definida recursivamente por la ecuación

$$y^2 = \frac{\delta^i x^2}{\delta^j x + \delta^{i+4}},$$

para algún $i = 2, 4, 6, 8$ y algún $1 \leq j \leq 8$.

Utilizando el conjunto $S_0^k = \{0, \delta^k, \delta^{k+4}\}$ para algún k adecuado con $1 \leq k \leq 8$ y los resultados del Teorema 3.3.8, tenemos que la torre es asintóticamente óptima ya que el límite de la torre satisface

$$2 = \sqrt{9} - 1 \geq A(9) \geq \lambda(\mathcal{F}) \geq \frac{2}{3-2} = 2.$$

Se puede probar que todas estas ecuaciones definen la misma torre sobre $\mathbb{F}_9$ utilizando la transformación lineal $X = \delta^k x$, $Y = \delta^k y$ para algún k adecuado con $1 \leq k \leq 8$. En particular se obtiene que son todas equivalentes a la torre

$$y^2 = \frac{x^2}{x-1},$$

presentada en [**GSR03**].

Ejemplo 3.3.11. Sea $q > 2$ y consideremos ahora la sucesión $\mathcal{F} = (F_0, F_1, \ldots)$ sobre $\mathbb{F}_q$ generada recursivamente por la ecuación

$$y^{q-1} = \frac{x^{q-1}}{x^{q-1} - (x-\alpha)^{q-1}},$$

con $\alpha \in \mathbb{F}_q^*$. Entonces, $f(x) = x^{q-1} - (x-\alpha)^{q-1}$ tiene todas sus raíces en $\mathbb{F}_q$. En efecto, sea $\beta \in \mathbb{F}_q^* \setminus \{\alpha\}$, entonces como $\beta \in \mathbb{F}_q^*$ sabemos que $\beta^{q-1} = 1$ y por lo tanto $f(\beta) = \beta^{q-1} - (\beta - \alpha)^{q-1} = 1 - 1 = 0$. Es decir, tenemos $q-2$ raíces distintas de $f(x)$ en $\mathbb{F}_q$, y como $deg(f(x)) = q-2$ tenemos que $f(x)$ se descompone linealmente en $\mathbb{F}_q$. Sea $S_0 = \mathbb{F}_q$. Como S_0 satisface las condiciones

(a) $0 \in S_0$ pues $0 \in \mathbb{F}_q$;

(b) $Z_f \subset S_0$ pues por hipótesis $f(x)$ tiene todas sus raíces en $\mathbb{F}_q$;

(c) para cada $\alpha \in S_0$, $Z_{H_\gamma} \subset S_0$, donde $Z_{H_\gamma} = f(t)\alpha^m - \beta\, t^m = 0$. En efecto, si $\gamma \in \mathbb{F}_q$ entonces $\gamma^{q-1} = 1$ y por lo tanto tenemos que $t^{q-1} - f(t) = (t+1)^{q-1}$ que tiene todas sus raíces en $\mathbb{F}_q$;

entonces la sucesión $\mathcal{F}$ tiene ramificación finita para todo $q > 2$.

Ahora, si $\mathbb{F}_q$ es un cuerpo de característica 2 con $q > 2$ entonces el polinomio $T^{q-1} + 1$ se descompone completamente en $\mathbb{F}_q$ y por lo tanto la sucesión que se obtiene en este caso es una torre de cuerpos de funciones asintóticamente buena cuyo límite satisface

$$\lambda(\mathcal{F}) \geq \frac{2}{q-2} > 0.$$

Si la característica de $\mathbb{F}_q$ es impar, entonces $T^{q-1} + 1$ se descompone completamente en $\mathbb{F}_{q^2}$, y así la sucesión que obtenemos en este caso es una torre asintóticamente buena sobre $\mathbb{F}_{q^2}$.

En definitiva, tenemos que

$$A(2^n) \geq \frac{2}{2^n - 2} \qquad \text{para } n \geq 2, \text{ y}$$
$$A(p^{2n}) \geq \frac{2}{p^n - 2} \qquad \text{para } p \text{ primo impar.}$$

Observación 3.3.12. Haciendo el cambio de variables $X = \frac{1}{x}$, e $Y = \frac{1}{y}$ obtenemos que la ecuación que define la torre del Ejemplo 3.3.11 se transforma en la ecuación

$$Y^{q-1} = 1 - (X + b)^{q-1} \qquad \text{con } b \in \mathbb{F}_q^*. \tag{3.3.4}$$

La torre definida por la ecuación anterior fue estudiada en [**GSR03**, Teorema 3.11] donde los autores obtienen la misma cota inferior para el límite de la torre. Observar que esta torre no puede ser estudiada con el Teorema 3.3.8 si se usa la ecuación (3.3.4).

Ejemplo 3.3.13. En particular si consideramos la torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_4$ generada recursivamente por la ecuación

$$y^3 = \frac{x^3}{x^2 + x + 1},$$

tenemos que el límite de la torre es exactamente 1, y por lo tanto la torre es asintóticamente óptima. En efecto, como $\mathbb{F}_4 = \{0, 1, \delta, \delta + 1\}$ donde $\delta^2 + \delta + 1 = 0$ entonces el polinomio $t^2 + t + 1$ tiene sus raíces (δ y $\delta + 1$) en $\mathbb{F}_4$. Luego, tenemos que la torre tiene límite $\lambda(\mathcal{F}) \geq \frac{2}{4-2} = 1$. Además, como sabemos que $A(4) = A(2^2) = 2 - 1 = 1$ y para toda torre sobre $\mathbb{F}_q$ se verifica $A(q) \geq \lambda(\mathcal{F})$ entonces, $\mathcal{F}$ es una torre asintóticamente óptima sobre $\mathbb{F}_q$.

Observación 3.3.14. El Ejemplo 3.3.13 fue presentado por Y. Qiu en [**Qiu10**].

Ejemplo 3.3.15. Si consideramos $\mathbb{F}_3$, tenemos que la sucesión $\mathcal{F} = (F_0, F_1, \ldots)$ generada recursivamente por la ecuación

$$y^2 = \frac{x^2}{2x - 1},$$

tiene ramificación finita. Sin embargo el polinomio $T^2 + 1$ no se descompone en $\mathbb{F}_3$, pero sí en $\mathbb{F}_9$. Luego, $\mathcal{F}$ es una torre asintóticamente buena sobre $\mathbb{F}_9$ y además

$$\lambda(\mathcal{F}) \geq \frac{2}{3 - 2} = 2.$$

Observar que esta torre es además, asintóticamente óptima sobre $\mathbb{F}_9$ ya que $A(9) = 3-1 = 2$.

Observación 3.3.16. Notar que en el ejemplo anterior, si utilizamos el cambio de variables $X = \frac{1}{x}$, e $Y = \frac{1}{y}$ obtenemos la ecuación

$$Y^2 = \frac{X^2}{X-1},$$

que ya fue estudiada en el Ejemplo 3.2.7 donde se demuestra que define (sobre $\mathbb{F}_9$) una subtorre de la torre $\mathcal{F}'$ definida por la ecuación

$$y^2 = \frac{x^2+1}{2x}.$$

Por lo tanto la torre $\mathcal{F}$ del Ejemplo 3.3.15 es subtorre de $\mathcal{F}'$, lo que da otra demostración de la optimalidad de $\mathcal{F}$ sobre $\mathbb{F}_9$.

CAPÍTULO 4

TORRES ASINTÓTICAMENTE MALAS

En este Capítulo damos condiciones suficientes para determinar si una sucesión dada de cuerpos de funciones es asintóticamente mala. Como consecuencia de estos resultados, probamos que para una cierta clase de sucesiones la infinitud del espacio de ramificación implica que la sucesión es asintóticamente mala. Mostramos también, que la mayoría de los ejemplos conocidos de torres asintóticamente malas se obtienen como casos particulares de estos resultados.

4.1. Sucesiones y torres asintóticamente malas

Una pregunta básica y muy interesante en la teoría de sucesiones y torres recursivas de cuerpos de funciones es la siguiente: ¿Qué propiedades debe tener un polinomio $f \in \mathbb{F}_q[X, Y]$ que define recursivamente una sucesión de cuerpos de funciones para que la sucesión obtenida resulte asintóticamente buena? Una condición necesaria simple es que la sucesión sea *admisible*. Esto significa que el grado del polinomio que la define es el mismo en las dos variables, es decir $deg_X(f) = deg_Y(f)$. En el caso de sucesiones *no admisibles*, si $deg_X(f) > deg_Y(f)$ entonces la tasa de descomposición $\nu(\mathcal{F}/F_0)$ es cero y si $deg_X(f) < deg_Y(f)$ entonces el género $\gamma(\mathcal{F}/F_0)$ no es finito (ver [**GS07**]). Por lo tanto se tiene una condición suficiente sencilla para ver que una sucesión recursiva es asintóticamente mala y la búsqueda de condiciones para obtener un comportamiento asintótico bueno debe concentrarse en sucesiones admisibles. Lamentablemente, existen muchos ejemplos

de sucesiones y torres admisibles y asintóticamente malas, por lo tanto esta condición no es suficiente. Es interesante notar que en el caso de sucesiones admisibles, parece ser igualmente complicado probar que una sucesión es asintóticamente buena o mala.

Como no está claro qué otras condiciones sobre el polinomio f, además de la admisibilidad, podrían ayudar a decidir si la sucesión definida por f es asintóticamente mala, un paso natural en la búsqueda de condiciones para deducir un comportamiento asintótico malo o bueno, es estudiar directamente al diferente $\mathrm{Diff}(F_m/F_n)$ para $m > n$. El punto de partida de muchos resultados conocidos en la dirección de comportamiento asintótico malo es la siguiente proposición.

En todos los enunciados asumimos que K es un cuerpo perfecto y que es el cuerpo total de constantes de cada F_i en la sucesión $\mathcal{F}$ dada.

Proposición 4.1.1. *Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una sucesión de cuerpos de funciones sobre K. Supongamos que existe una subsucesión $\{F_{r_i}\}_{i=1}^{\infty}$ tal que la serie*

$$\sum_{i=1}^{\infty} \frac{deg\ \mathrm{Diff}(F_{r_i}/F_{r_{i-1}})}{[F_{r_i} : F_0]}$$

diverge. Entonces $\gamma(\mathcal{F}/F_0) = \infty$. En particular, $\mathcal{F}$ es asintóticamente mala. El recíproco vale cuando $\mathcal{F}$ es una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ con tasa de descomposición $\nu(\mathcal{F}/F_0)$ positiva. Es decir, si $\mathcal{F}$ es una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ asintóticamente mala y $\nu(\mathcal{F}/F_0) > 0$, entonces para cualquier subsucesión $\{F_{r_i}\}_{i=1}^{\infty}$ la serie

$$\sum_{i=1}^{\infty} \frac{deg\ \mathrm{Diff}(F_{r_i}/F_{r_{i-1}})}{[F_{r_i} : F_0]}$$

diverge.

Demostración. El teorema se obtiene del hecho de que el género de la sucesión $\gamma(\mathcal{F}/F_0) = \lim_{n\to\infty} g(F_n)/[F_n : F_0]$ se puede escribir como

$$\gamma(\mathcal{F}/F_0) = \lim_{i\to\infty} \frac{g(F_{r_i})}{[F_{r_i} : F_0]} = g(F_0) - 1 + \frac{1}{2}\sum_{i=1}^{\infty} \frac{deg\ \mathrm{Diff}(F_{r_i}/F_{r_{i-1}})}{[F_{r_i} : F_0]}. \tag{4.1.1}$$

En efecto, utilizando la fórmula del género de Hurwitz (Teorema 1.2.11) para la extensión F_{r_1}/F_0, tenemos que

$$2(g(F_{r_1})-1) = [F_{r_1}:F_0](2g(F_0)-2) + deg\ \mathrm{Diff}(F_{r_1}/F_0)$$

y por lo tanto

$$\frac{g(F_{r_1})-1}{[F_{r_1}:F_0]} = g(F_0) - 1 + \frac{1}{2}\frac{deg\ \mathrm{Diff}(F_{r_1}/F_0)}{[F_{r_1}:F_0]}.$$

Supongamos ahora que

$$\frac{g(F_{r_i})-1}{[F_{r_i}:F_0]} = g(F_0) - 1 + \frac{1}{2}\sum_{j=1}^{i}\frac{deg\ \mathrm{Diff}(F_{r_j}/F_{r_{j-1}})}{[F_{r_j}:F_0]},$$

donde F_{r_0} denota a F_0. Entonces para la extensión $F_{r_{i+1}}/F_{r_i}$ tenemos que

$$2(g(F_{r_{i+1}})-1) = [F_{r_{i+1}}:F_{r_i}](2g(F_{r_i})-2) + deg\ \mathrm{Diff}(F_{r_{i+1}}/F_{r_i})$$

y por lo tanto

$$\begin{aligned}
\frac{g(F_{r_{i+1}})-1}{[F_{r_{i+1}}:F_0]} &= \frac{g(F_{r_i})-1}{[F_{r_i}:F_0]} + \frac{1}{2}\frac{deg\ \mathrm{Diff}(F_{r_{i+1}}/F_{r_i})}{[F_{r_{i+1}}:F_0]} \\
&= g(F_0) - 1 + \frac{1}{2}\sum_{j=1}^{i}\frac{deg\ \mathrm{Diff}(F_{r_j}/F_{r_{j-1}})}{[F_{r_j}:F_0]} + \frac{1}{2}\frac{deg\ \mathrm{Diff}(F_{r_{i+1}}/F_{r_i})}{[F_{r_{i+1}}:F_0]} \\
&= g(F_0) - 1 + \frac{1}{2}\sum_{j=1}^{i+1}\frac{deg\ \mathrm{Diff}(F_{r_j}/F_{r_{j-1}})}{[F_{r_j}:F_0]}.
\end{aligned}$$

Luego, como sabemos que el límite $g(F_n)/[F_n:F_0]$ siempre existe tenemos que

$$\begin{aligned}
\gamma(\mathcal{F}/F_0) &= \lim_{n\to\infty}\frac{g(F_n)}{[F_n:F_0]} \\
&= \lim_{n\to\infty}\frac{g(F_n)-1}{[F_n:F_0]} \\
&= \lim_{i\to\infty}\frac{g(F_{r_i})-1}{[F_{r_i}:F_0]} \\
&= g(F_0) - 1 + \frac{1}{2}\lim_{i\to\infty}\sum_{j=1}^{i+1}\frac{deg\ \mathrm{Diff}(F_{r_j}/F_{r_{j-1}})}{[F_{r_j}:F_0]} \\
&= g(F_0) - 1 + \frac{1}{2}\sum_{j=1}^{\infty}\frac{deg\ \mathrm{Diff}(F_{r_j}/F_{r_{j-1}})}{[F_{r_j}:F_0]}.
\end{aligned}$$

Finalmente, si $\mathcal{F}$ es una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ asintóticamente mala y $\nu(\mathcal{F}/F_0) > 0$ el resultado recíproco se obtiene fácilmente de la ecuación (4.1.1). $\square$

La idea en la Proposición 4.1.1 fue usada en [**GS96**], [**MW05**], [**BGS04**] y [**BGS05a**]; en donde los autores dan condiciones suficientes para obtener torres asintóticamente malas. A primera vista pareciera que los ejemplos que aparecen en los artículos mencionados representan casos con poca relación entre ellos. Sin embargo, vamos a mostrar que estos resultados se pueden deducir del siguiente resultado general.

Proposición 4.1.2. *Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una sucesión recursiva admisible de cuerpos de funciones sobre K definida por un polinomio $f \in K[X, Y]$. Sea $\{x_i\}_{i=0}^{\infty}$ una sucesión de elementos trascendentes sobre K tales que*

$$F_0 = K(x_0) \qquad y \qquad F_{i+1} = F_i(x_{i+1}),$$

donde $f(x_i, x_{i+1}) = 0$ para $i \geq 0$. Sea $b \in K(T)$ una función racional y supongamos que existe una sucesión creciente de enteros no negativos $\{r_j\}_{j=1}^{\infty}$ y funciones positivas $c_1(t)$ y $c_2(t)$ definidas para $t \geq 0$ tales que para $j \geq 1$ existe un divisor $B_{r_j} \in \mathcal{D}(F_{r_j})$ que satisface

a) $\deg B_{r_j} \geq c_1(j) \cdot \deg\left(b(x_{r_j})\right)_{\infty}^{r_j}$ (resp. $\deg B_{r_j} \geq c_1(j) \cdot \deg\left(b(x_{r_j})\right)_{0}^{r_j}$), donde $\left(b(x_{r_j})\right)_{\infty}^{r_j}$ (resp. $\left(b(x_{r_j})\right)_{\infty}^{r_j}$) denota al divisor de polos (resp. divisor de ceros) del elemento x_{r_j} en F_{r_j};

b)

$$\sum_{P \in \, supp(B_{r_j})} \sum_{P'|P} d(P'|P) \deg P' \geq c_2(j) \, [F_{r_{j+1}} : F_{r_j}] \deg B_{r_j}$$

donde la suma interior recorre todos los lugares P' de $F_{r_{j+1}}$ arriba de P.

Si se cumple una de las siguientes:

c) la serie $\sum_{j=1}^{\infty} c(j)$ diverge;

d) existe una función no negativa ψ y una constante positiva M tales que

(i) $\psi(c(1)) \leq Mc(1)$;

(ii) $\psi(c(j)) - \psi(c(j-1)) \leq Mc(j)$;

(iii) $\psi(c(t)) \to \infty$ cuando $t \to \infty$;

donde $c(j) = c_1(j)c_2(j)$, entonces $\gamma(\mathcal{F}/F_0) = \infty$. En particular una sucesión $\mathcal{F}$ que satisface a), b) y c) o d), define una torre asintóticamente mala (pues $\gamma(\mathcal{F}/F_0) = \infty$ implica que $g(F_i) \to \infty$ cuando $t \to \infty$).

Demostración. Por el Teorema 1.1.16 del Capítulo 1 tenemos que

$$deg\,(b(x_{r_j}))_\infty^{r_j} = [F_{r_j} : K(b(x_{r_j}))]$$

y por lo tanto

$$deg\, B_{r_j} \geq c_1(j)[F_{r_j} : K(b(x_{r_j}))] \geq c_1(j)[F_{r_j} : K(x_{r_j})].$$

Como $\mathcal{F}$ es admisible, entonces $[F_{r_j} : F_0] = [F_{r_j} : K(x_{r_j})]$ y por lo tanto

$$deg\, B_{r_j} \geq c_1(j)\,[F_{r_j} : F_0] \qquad \text{para } \; j \geq 1. \tag{4.1.2}$$

Observar ahora que

$$\begin{aligned} deg\ \mathrm{Diff}(F_{r_{j+1}}/F_{r_j}) &= \sum_{P\in\mathbb{P}(F_{r_j})} \sum_{P'|P} d(P'|P)\, deg\, P' \\ &\geq \sum_{P\in\, supp(B_{r_j})} \sum_{P'|P} d(P'|P)\, deg\, P' \\ &\geq c_2(j)[F_{r_{j+1}} : F_{r_j}]\, deg\, B_{r_j} \qquad (\text{por } \; b)) \\ &\geq c(j)\,[F_{r_{j+1}} : F_0], \end{aligned}$$

donde $c(j) = c_1(j)c_2(j)$.

Por lo tanto

$$\sum_{j=1}^{\infty} \frac{deg\ \mathrm{Diff}(F_{r_{j+1}}/F_{r_j})}{[F_{r_{j+1}} : F_0]} \geq \sum_{j=1}^{\infty} c(j)$$

y usando la hipótesis en *c)* y la Proposición 4.1.1 obtenemos que $\gamma(\mathcal{F}/F_0) = \infty$.

Supongamos ahora que se cumple la hipótesis en *d)*. Usando la transitividad del exponente diferente podemos probar por inducción que

$$deg\ \mathrm{Diff}(F_{r_{s+1}}/F_{r_1}) \geq M'\,\psi(c(s))\,[F_{r_{s+1}} : F_0] \qquad \forall\, s \geq 1,$$

donde $M' = 1/M$. En efecto, para $s = 1$ usando *(i)* de *d)* tenemos que

$$deg\ \mathrm{Diff}(F_{r_2}/F_{r_1}) \geq c(1)\,[F_{r_2} : F_0] \geq M'\,\psi(c(1))\,[F_{r_2} : F_0].$$

Supongamos ahora que vale

$$deg\ \mathrm{Diff}(F_{r_s}/F_{r_1}) \geq M'\,\psi(c(s-1))\,[F_{r_s} : F_0].$$

Entonces

$$\begin{aligned}
deg\ \mathrm{Diff}(F_{r_{s+1}}/F_{r_1}) &= \sum_{P\in\mathbb{P}(F_{r_1})} \sum_{\substack{P''|P \\ P''\in\mathbb{P}\left(F_{r_{s+1}}\right)}} d(P''|P)\, deg\, P'' \\
&= \sum_{P\in\mathbb{P}(F_{r_1})} \sum_{\substack{P\subset P'\subset P'' \\ P''\in\mathbb{P}\left(F_{r_{s+1}}\right),\, P'\in\mathbb{P}(F_{r_s})}} \left(e(P''|P')\, d(P'|P) + d(P''|P')\right) deg\, P'' \\
&\geq \sum_{P\in\mathbb{P}(F_{r_1})} \sum_{\substack{P'|P \\ P'\in\mathbb{P}(F_{r_s})}} \sum_{P''\in\mathbb{P}(F_{r_{s+1}})} e(P''|P')\, d(P'|P)\, f(P''|P')\, deg\, P' \\
&\quad + \sum_{P'\in\mathbb{P}(F_{r_s})} \sum_{\substack{P'''|P' \\ P''\in\mathbb{P}\left(F_{r_{s+1}}\right)}} d(P'''|P')\, deg\, P'' \\
&= [F_{r_{s+1}} : F_{r_s}]\, deg\ \mathrm{Diff}(F_{r_s}/F_{r_1}) + deg\ \mathrm{Diff}(F_{r_{s+1}}/F_{r_s}) \\
&\geq [F_{r_{s+1}} : F_{r_s}] M'\, \psi(c(s-1))\, [F_{r_s} : F_0] + k\, c(s)\, [F_{r_{s+1}} : F_0] \\
&= M'\, [F_{r_{s+1}} : F_0] \Big(\psi(c(s-1)) + M\, c(s)\Big) \\
&\geq M'\psi(c(s))[F_{r_{s+1}} : F_0] \qquad (\text{por } \textit{(ii)} \text{ de } \textit{d)}).
\end{aligned}$$

Sin pérdida de generalidad podemos suponer que el género del cuerpo de funciones F_{r_1} satisface $g(F_{r_1}) > 0$ y por lo tanto la fórmula del género de Hurwitz para la extensión $F_{r_{s+1}}/F_{r_1}$ implica que

$$g(F_{r_{s+1}}) \geq \frac{M'}{2}\, \psi(c(s))\, [F_{r_{s+1}} : F_0],$$

para todos los índices s.

Entonces

$$\frac{g(F_{r_{s+1}})}{[F_{r_{s+1}} : F_0]} \geq \frac{M'}{2}\, \psi(c(s))$$

que tiende a infinito por *(iii)* de *d)* y por lo tanto, $\gamma(\mathcal{F}/F_0) = \infty$. □

Observación 4.1.3. Si en la parte *a)* de la Proposición 4.1.2 la desigualdad

$$deg\, B_{r_j} \geq c_1(j) \cdot deg\, (b(x_{r_j}))_\infty^{r_j} \quad \text{ó} \quad deg\, B_{r_j} \geq c_1(j) \cdot deg\, (b(x_{r_j}))_0^{r_j},$$

se reemplaza por la siguiente desigualdad más fuerte

$$deg\, B_{r_j} \geq c_1(j)[F_{r_j} : F_0], \tag{4.1.3}$$

obtenida en (4.1.2), de la prueba de la Proposición 4.1.2 tenemos nuevamente el mismo resultado para sucesiones en general (es decir, sin que sea necesariamente recursiva o admisible).

Probemos ahora un resultado que usaremos más adelante cuando estudiemos la relación entre el espacio de ramificación de una sucesión de cuerpos de funciones y el comportamiento asintótico de la sucesión. Usaremos el siguiente resultado que es consecuencia de la teoría de extensiones de cuerpos constantes: sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$. Si consideramos las extensiones de cuerpos constantes $F_i' = F_i \cdot K$ donde K es un cuerpo perfecto obtenemos la sucesión de extensiones constantes $\mathcal{F}' = (F_0', F_1', F_2', \ldots)$ de cuerpos de funciones sobre K. Entonces

$$\nu(\mathcal{F}/F_0) \leq \nu(\mathcal{F}'/F_0') \quad \text{y} \quad \gamma(\mathcal{F}/F_0) = \gamma(\mathcal{F}'/F_0')\,,$$

y por lo tanto, si $\mathcal{F}'$ es asintóticamente mala entonces $\mathcal{F}$ es asintóticamente mala.

Teorema 4.1.4. *Sea K un cuerpo perfecto y sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una sucesión de cuerpos de funciones sobre K. Supongamos que existe una sucesión creciente de enteros no negativos $\{r_j\}_{j=1}^{\infty}$ tales que se cumple una de las siguientes*

(i) para cada índice r_j hay un número positivo m_j y un divisor $B_{r_j} = \sum m_P P$ de F_{r_j} de grado al menos $d_j[F_{r_j} : F_0]$ donde $d_j > 0$, para todo $P \in supp(B_{r_j})$ se tiene que $m_P \leq m_j$ y que $e(Q|P) > 1$ para cada lugar Q de $F_{r_{j+1}}$ arriba de P, y $c(j) = d_j/m_j$ satisface c) ó d) del Teorema 4.1.2, o

(ii) para cada índice r_j existe un lugar P_j de F_0 que no ramifica en F_{r_j} y tal que cada lugar Q de $F_{r_{j+1}}$ arriba de P_j satisface $e(Q|P_j) > 1$.

Entonces $\gamma(\mathcal{F}/F_0) = \infty$ y $\mathcal{F}$ es en realidad una torre asintóticamente mala. Notar que en el caso (ii), $\mathcal{F}$ es una torre asintóticamente mala con espacio de ramificación $Ram(\mathcal{F}/F_0)$ infinito.

Supongamos ahora que la sucesión es una sucesión recursiva admisible de cuerpos de funciones sobre K. Entonces existe un polinomio en dos variables $f \in H \in K[X, Y]$ y una sucesión $\{x_i\}_{i=0}^{\infty}$ de elementos trascendentes sobre K tales que

$$F_0 = K(x_0) \quad y \quad F_{i+1} = F_i(x_{i+1}),$$

donde $f(x_i, x_{i+1}) = 0$ *para* $i \geq 0$. *Supongamos que existe una sucesión creciente de enteros no negativos* $\{r_j\}_{j=1}^{\infty}$ *tales que*

(iii) para cada índice r_j *existe un lugar* P_j *de* $K(x_{r_j})$ *que no ramifica en* F_{r_j} *y tal que cada lugar* Q *de* $F_{r_{j+1}}$ *arriba de* P_j *satisface* $e(Q|P_j) > 1$.

Entonces $\gamma(\mathcal{F}/F_0) = \infty$ *y* $\mathcal{F}$ *es en realidad una torre asintóticamente mala.*

Demostración. Supongamos que vale *(i)*. Por hipótesis tenemos que

$$deg\, B_{r_j} \geq d_j\, [F_{r_j} : F_0],$$

por lo que la desigualdad (4.1.3) de la Observación 4.1.3 vale con $c_1(j) = d_j$ para todo $j \geq 1$. Por otra parte, *b)* de la Proposición 4.1.2 vale con $c_2(j) = 1/2m_j$ para todo $j \geq 1$ pues por el Teorema del diferente de Dedekind (Teorema 1.2.9 del Capítulo 1) tenemos que

$$\begin{aligned}
\sum_{P \in\, supp(B_{r_j})} \sum_{Q|P} d(Q|P) deg\, Q &\geq \sum_{P \in\, supp(B_{r_j})} \sum_{Q|P} (e(Q|P) - 1) deg\, Q \\
&\geq \frac{1}{2} \sum_{P \in\, supp(B_{r_j})} \sum_{Q|P} e(Q|P) deg\, Q \\
&= \frac{1}{2} \sum_{P \in\, supp(B_{r_j})} \sum_{Q|Q} e(Q|P) f(Q|P) deg\, P \\
&= \frac{1}{2} [F_{r_{j+1}} : F_{r_j}] \sum_{P \in\, supp(B_{r_j})} deg\, P \\
&\geq \frac{1}{2m_j} [F_{r_{j+1}} : F_{r_j}]\, deg\, B_{r_j}\,,
\end{aligned}$$

donde las sumas interiores anteriores recorren todos los lugares Q de $F_{r_{j+1}}$ arriba de P. Luego, la parte *c)* o *d)* de la Proposición 4.1.2 vale y como decimos en la Observación 4.1.3 todo esto implica que $\gamma(\mathcal{F}/F_0) = \infty$.

Supongamos ahora que la parte *(ii)* vale y consideremos la sucesión de extensiones constantes $\mathcal{F}' = (F_0', F_1', F_2', \ldots)$ con $F_i' = F_i \cdot \bar{K}$ donde $\bar{K}$ es una clausura algebraica de K. Por hipótesis tenemos que existe una sucesión $\{r_j\}_{j=1}^{\infty}$ tal que para $j \geq 1$ existe un lugar P_j' de F_0' que se descompone completamente en F_{r_j}' y tal que cada lugar Q' de $F_{r_{j+1}}'$

arriba de P'_j satisface $e(Q'|P'_j) > 1$. En particular, si escribimos $P' = Q' \cap F_{r_j}$, tenemos que $e(Q'|P') > 1$ y $e(P'|P'_j) = 1$. Consideremos ahora el divisor B_{r_j} de F'_{r_j} definido por

$$B_{r_j} = \sum_{P' \in L(P'_j)} P',$$

donde $L(P'_j) = \{P' \in \mathbb{P}(F'_{r_j}) : P'|P'_j\}$. Entonces

$$deg\, B_{r_j} \geq [F'_{r_j} : F'_0],$$

y vemos que estamos en la situación del item *(i)* arriba con $d_j = m_j = 1$. Luego $\gamma(\mathcal{F}'/F'_0) = \infty$ y por lo tanto $\gamma(\mathcal{F}/F_0) = \infty$. Es claro, de la definición $Ram(\mathcal{F}/F_0)$, que *(ii)* implica que $Ram(\mathcal{F}/F_0)$ es infinito.

Finalmente supongamos que vale *(iii)*. Consideramos nuevamente la sucesión de extensiones constantes $\mathcal{F}' = (F'_0, F'_1, F'_2, \ldots)$ con $F'_i = F_i \cdot \bar{K}$ donde $\bar{K}$ es una clausura algebraica de K. Como $\mathcal{F}$ es admisible, entonces $\mathcal{F}'$ es admisible y por lo tanto

$$[F'_i : F'_0] = [F'_i : \bar{K}(x_i)],$$

para todo $i \geq 0$. Ahora consideremos el divisor B_{r_j} de F'_{r_j} definido por

$$B_{r_j} = \sum_{P' \in L(P'_j)} P',$$

donde $L(P'_j) = \{P' \in \mathbb{P}(F'_{r_j}) : P'|P'_j\}$. El mismo argumento usado en *(ii)* arriba muestra que

$$deg\, B_{r_j} \geq [F'_{r_j} : \bar{K}(x_{r_j})] = [F'_i : F'_0],$$

y concluimos que estamos en la misma situación de la prueba de la parte *(ii)* arriba. Luego $\gamma(\mathcal{F}/F_0) = \gamma(\mathcal{F}'/F'_0) = \infty$.

□

4.2. Una conjetura de Beelen, Garcia y Stichtenoth

En el contexto del comportamiento asintótico de una torre de cuerpos de funciones $\mathcal{F} = (F_0, F_1, \ldots)$, la finitud o no del espacio de ramificación $Ram(\mathcal{F}/F_0)$ de la torre, es decir, del conjunto de lugares de F_0 que están ramificados en la torre, es una propiedad

clave, en particular cuando se trabaja con torres recursivas. Como vimos en el Capítulo anterior, la finitud del espacio de ramificación es esencial en el estudio del comportamiento asintótico de torres recursivas moderadas. De hecho, si una torre moderada $\mathcal{F}$ tiene tasa de descomposición positiva y $Ram(\mathcal{F}/F_0)$ es un conjunto finito entonces $\mathcal{F}$ es asintóticamente buena (ver Capítulo 3). Sin embargo, hasta el momento se desconoce si una torre asintóticamente buena (recursiva o no) puede tener espacio de ramificación infinito. Sabemos que existen ejemplos (ver [**DPZ04**]) de torres no recursivas con espacio de ramificación infinito y tasa de descomposición positiva o género finito, pero el comportamiento asintótico de estas torres se desconoce. También hay ejemplos de torres recursivas asintóticamente malas con espacio de ramificación finito (ver [**BGS05a**]).

En este contexto, parece natural preguntarse cuán esencial es la finitud del espacio de ramificación en el comportamiento asintótico de una torre. Más precisamente, hay una pregunta que hasta el momento permanece sin respuesta en el caso general: ¿cuándo la infinitud del espacio de ramificación de una torre $\mathcal{F}$ es responsable del comportamiento asintótico malo de $\mathcal{F}$? Para torres recursivas, se conjetura (ver [**BGS05b**, Conjetura 2]) que espacio de ramificación infinito implica género infinito y por lo tanto que la torre será asintóticamente mala.

Por otro lado, se sabe que si $\mathcal{F}$ es una sucesión de cuerpos de funciones asintóticamente buena sobre $\mathbb{F}_q$ donde todas las extensiones F_i/F_0 son Galois (las llamaremos *sucesiones de Galois de tipo II*), entonces no sólo $Ram(\mathcal{F}/F_0)$ es un conjunto finito sino que además $\nu(\mathcal{F}/F_0) > 0$ (ver [**GSR03**, Teorema 2.26]). Relacionados a estos problemas, tenemos el siguiente resultado recíproco parcial de la parte *(ii)* del Teorema 4.1.4, que a su vez redemuestra que una sucesión de cuerpos de funciones sobre un cuerpo perfecto K de Galois de tipo II con espacio de ramificación infinito es necesariamente asintóticamente mala.

Teorema 4.2.1. *Sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una sucesión de cuerpos de funciones sobre un cuerpo perfecto K de Galois de tipo II con espacio de ramificación infinito. Existe una sucesión creciente de enteros no negativos $\{r_j\}_{j=1}^{\infty}$ tales que para cada índice r_j hay un lugar P_j de F_0 que es no ramificado en F_{r_j} y tal que cada lugar Q de F_{r_j} arriba de P_j*

ramifica en $F_{r_{j+1}}$. En particular $\gamma(\mathcal{F}/F_0) = \infty$. Por lo tanto, toda sucesión de Galois de tipo II con espacio de ramificación infinito es una torre de Galois de tipo II que es asintóticamente mala.

Demostración. Sea S el conjunto de lugares de F_0 que ramifican en F_1. Entonces S es un conjunto finito (que puede ser vacío). Sea $N_1 = \mathbb{P}(F_0) \setminus S$. Entonces $N_1 \neq \emptyset$. Si todo lugar $P \in N_1$ no ramifica en cada F_i entonces $Ram(\mathcal{F}/F_0) \subset S$, y por lo tanto $Ram(\mathcal{F}/F_0)$ es un conjunto finito, lo cuál es una contradicción. Entonces existe un menor entero positivo $r_1 \geq 2$ tal que hay un lugar $P_1 \in N_1$ que no ramifica en F_{r_1} pero ramifica en F_{r_1+1}. Como las extensiones F_{r_1+1}/F_0 y F_{r_1}/F_0 son extensiones de Galois, cada lugar Q de F_{r_1} arriba de P_1 es ramificado en F_{r_1+1}. Sea S_1 el conjunto de lugares de N_1 que no ramifican en F_{r_1} pero ramifican en F_{r_1+1}. Entonces S_1 es un conjunto finito. Sea $N_2 = N_1 \setminus S_1$. Tenemos entonces que $N_2 \neq \emptyset$. Si todo lugar $P \in N_2$ es no ramificado en cada F_i entonces $Ram(\mathcal{F}/F_0) \subset S \cup S_1$. Luego $Ram(\mathcal{F}/F_0)$ es un conjunto finito, y nuevamente tenemos una contradicción. Entonces tiene que existir un menor entero positivo $r_2 > r_1$ tal que hay un lugar $P_2 \in N_2$ que no ramifica en F_{r_2} y sí ramifica en F_{r_2+1}. Como las extensiones F_{r_2+1}/F_0 y F_{r_2}/F_0 son extensiones de Galois, todo Q de F_{r_2} arriba de P_2 ramifica en F_{r_2+1}. Por construcción, tenemos además que P_1 no ramifica en F_{r_1} y que cada lugar Q de F_{r_1} arriba de P_1 ramifica en F_{r_2}. Continuando de esta manera, encontramos una sucesión de enteros positivos $\{r_j\}_{j=1}^{\infty}$ que satisface la propiedad buscada. En otras palabras, tenemos que la parte *(ii)* del Teorema 4.1.4 vale. Luego $\gamma(\mathcal{F}/F_0) = \infty$ y por lo tanto $\mathcal{F}$ es asintóticamente mala. □

Este resultado, a su vez, da una nueva demostración de que la Conjetura 2 en [**BGS05a**] es verdadera para sucesiones de Galois de tipo II. A una sucesión donde todas las extensiones F_{i+1}/F_i son Galois la llamaremos *sucesión de Galois de tipo I*. Hasta el momento no se conoce si la Conjetura 2 en [**BGS05a**] es verdadera para este tipo de sucesiones.

4.3. Ejemplos

Veamos ahora que los resultados en los trabajos [**GS96**], [**MW05**], [**BGS04**] y [**BGS05a**] se pueden tratar de una manera unificada, viendo que en todos los casos existe un divisor con las propiedades de la Proposición 4.1.2. Vale la pena destacar que en varios de estos ejemplos la existencia de tal divisor no es para nada obvia.

Usaremos la siguiente notación: un lugar definido por un polinomio mónico e irreducible $f \in \mathbb{F}_q[x]$ en el cuerpo de funciones racionales $\mathbb{F}_q(x)$ será denotado por P_f.

Ejemplo 4.3.1. Este ejemplo fue presentado en [**GS96**]. Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una torre recursiva de cuerpos de funciones sobre un cuerpo finito $\mathbb{F}_q$ de característica 2, donde $F_0 = \mathbb{F}_q(x_0)$ y

$$F_n = F_{n-1}(x_n) \qquad \text{con} \qquad x_n^3 - x_n = \frac{x_{n-1}^3}{x_{n-1}+1}, \qquad \text{para } n \geq 1.$$

La Proposición 4.1.2 nos permitirá probar que la torre $\mathcal{F}$ es asintóticamente mala.

Si miramos la ramificación en el cuerpo básico, tenemos que si Q es un lugar de $\mathbb{F}_q(x,y)$ tal que Q es un cero de $y+1$ en $\mathbb{F}_q(x,y)$ entonces Q es un cero de x y está arriba del lugar P_x que es el cero de x en $\mathbb{F}_q(x)$. En efecto, si $P = Q \cap \mathbb{F}_q(x)$ tenemos que

$$0 < v_Q(y+1) = v_Q(y^3 - y) = e(Q|P) v_P\left(\frac{x^3}{x+1}\right) = e(Q|P)(3v_P(x) - v_P(x+1)),$$

es decir que

$$3v_P(x) > v_P(x+1),$$

y por lo tanto $P = P_x$ es el cero de x en $\mathbb{F}_q(x)$. Además

$$2v_Q(y+1) = 3e(Q|P_x),$$

y como $[\mathbb{F}_q(x,y) : \mathbb{F}_q(x)] = 3$ entonces $e(Q|P_x) = 2$.

Por otro lado, sea R el cero de y en $\mathbb{F}_q(x,y)$. Al igual que antes se puede ver que R está arriba del lugar P_x y como

$$\sum_{P|P_x} e(P|P_x) f(P|P_x) = 3,$$

entonces debe ser que $e(R|P_x) = f(R|P_x) = f(Q|P_x) = 1$. Luego, la ramificación del lugar P_x de $\mathbb{F}_q(x)$ en $\mathbb{F}_q(x,y)$ es como se describe en la siguiente figura.

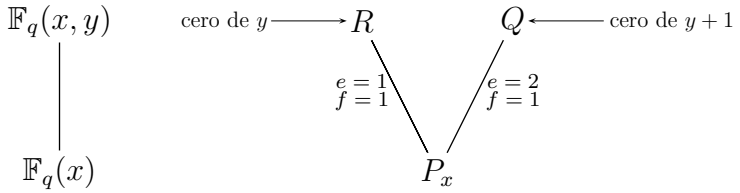

FIGURA 1. Ramificación de P_x en $\mathbb{F}_q(x,y)$.

Notar ahora que R, que es un cero de y en $\mathbb{F}_q(x,y)$, también es un cero de y en $\mathbb{F}_q(y)$, pues si $P = \mathbb{F}_q(y) \cap R$ entonces

$$0 < v_R(y) = e(R|P)v_P(y)$$

y por lo tanto $P = P_y$. Entonces $v_{P_y} = 1$ y tenemos que

$$0 < e(R|P_y) = v_R(y) = 3v_R(x) - v_R(x+1),$$

y por lo tanto

$$3v_R(x) > v_R(x+1).$$

Como las suposiciones $v_R(x) < 0$ y $v_R(x) = 0$ conducen a absurdos concluimos que $v_R(x) > 0$ y en este caso $v_R(x+1) = 0$. Luego, $3|e(R|P_y)$ y como $e(R|P_y) \leq 3$ tenemos que $e(R|P_y) = 3$, es decir, el lugar P_y de $\mathbb{F}_q(y)$ es totalmente ramificado en $\mathbb{F}_q(x,y)$.

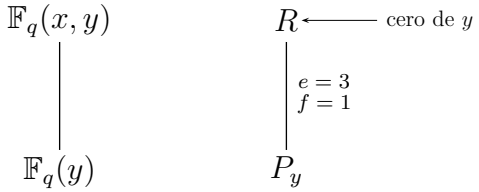

FIGURA 2. Ramificación de P_y en $\mathbb{F}_q(x,y)$.

Sea P' un lugar de F_{n+1} que es un cero de $x_{n+1}+1$. Entonces tenemos que P' es un cero de $x_{n-1}, x_{n-2}, \ldots, x_1, x_0$. Más aún, utilizando los resultados de las Figuras 1 y 2 y el Lema de Abhyankar (Proposición 1.2.13) tenemos el siguiente diagrama.

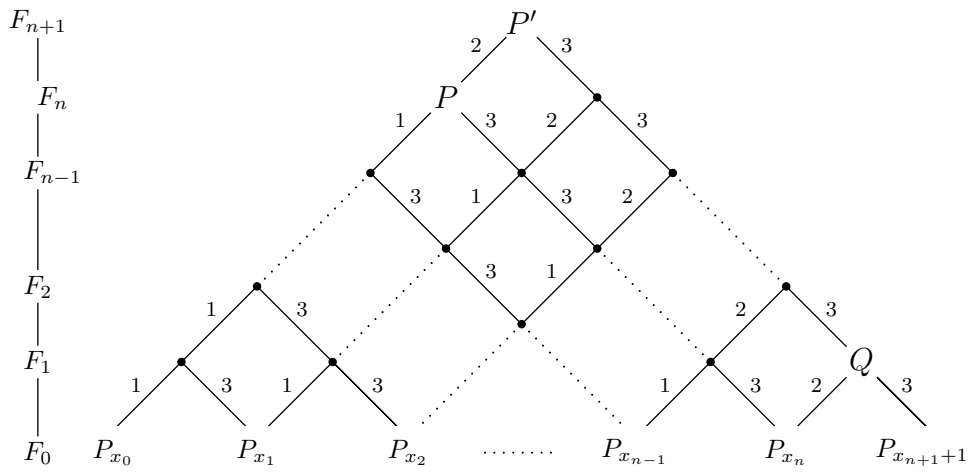

FIGURA 3. Ramificación de P'.

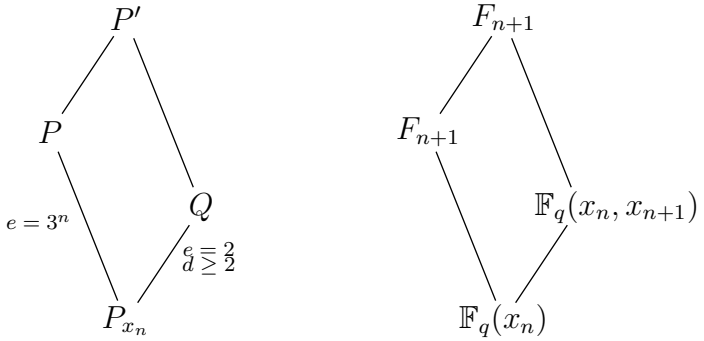

FIGURA 4. Ramificación de $P_{x_{n-1}}$.

Sea P la restricción de P' a F_n y Q la restricción de P' a $\mathbb{F}_q(x_n, x_{n+1})$, es decir, $P = P' \cap F_n$ y $Q = P' \cap \mathbb{F}_q(x_n, x_{n+1})$ como en la Figura 4.

Usando la transitividad del exponente diferente tenemos que

$$\begin{aligned} d(P'|P) &= e(P'|P)\, d(Q|P_{x_n}) + d(P'|Q) - e(P'|P)\, d(P|P_{x_n}) \\ &= 3^n\, d(Q|P_{x_n}) + (3^n - 1) - 2(3^n - 1) \\ &\geq 3^n + 1. \end{aligned}$$

Ahora, para cada $j \geq 1$ denotamos por P'_j al lugar de F_j que es un cero de $x_j + 1$ y por P_j a la restricción de P'_j a F_{j-1}. Definimos el divisor

$$B_n := 3^n P_{n+1} \in \mathcal{D}(F_n) \qquad \text{para} \qquad n \geq 0.$$

Notar que el argumento anterior implica que $deg\, P_j = 1$ para $j \geq 1$. Observar que en la Figura 5 a continuación $\tilde{P}_{n+1}$ es un cero de x_{n+1} en F_{n+1}, mientras que P'_{n+1} es un cero de $x_{n+1}+1$ en F_{n+1}.

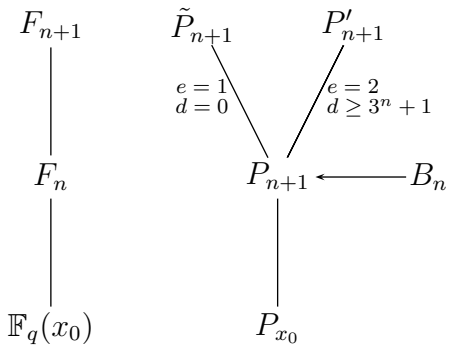

FIGURA 5. Descripción del divisor B_j.

Como sabemos que $[F_n : \mathbb{F}_q(x_n)] = 3^n$ entonces

$$deg\, B_n = 3^n deg\, P_{n+1} = 3^n = [F_n : \mathbb{F}_q(x_n)] = deg\, (x_n)^n_\infty.$$

Además,

$$\begin{aligned}\sum_{P \in\, supp(B_n)} \sum_{P'|P} d(P'|P) deg\, P' &\geq d(P'_{n+1}|P_{n+1}) deg\, P'_{n+1} \\ &\geq 3^n + 1 \\ &\geq \frac{1}{3} 3^{n+1} \\ &= \frac{1}{3}[F_{n+1} : F_n] deg\, B_n.\end{aligned}$$

Luego, se cumplen las hipótesis de la Proposición 4.1.2 con $c_1(j) = 1$ y $c_2(j) = 1/3$ y por lo tanto la torre $\mathcal{F}$ es asintóticamente mala.

Ejemplo 4.3.2 . Veamos ahora que el resultado probado en [**BGS04**, Teorema 2.1] sobre torres asintóticamente malas de tipo Artin-Schreier puede deducirse de la Proposición 4.1.2. Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una torre recursiva de cuerpos de funciones de tipo Artin-Schreier sobre el cuerpo finito $\mathbb{F}_q$ de característica p. Supongamos que $F_0 = \mathbb{F}_q(x_0)$ y para todo $n \geq 1$ tenemos que

$$F_n = F_{n-1}(x_n), \qquad \text{con} \qquad x_n^p - x_n = b(x_{n-1})$$

donde $b(T) = b_1(T)/b_2(T) \in \mathbb{F}_q(T)$ es una función racional donde $b_1(T)$ y $b_2(T)$ son polinomios coprimos con $deg\,(b_1(T)) = p$ y $deg\,(b_2(T)) = r < p$. Supongamos que el conjunto

$$L_0 = \{P \in\ supp((b(x_0))^0_\infty) : (v_P(b(x_0)), p) = 1\} \subset \mathbb{P}(F_0),$$

es no vacío y sea $L_j = \{P' \in \mathbb{P}(F_j) : P'|P$ para algún $P \in L_0\}$, para $j \geq 1$. Finalmente supongamos que existe una constante $C > 0$ tal que para una cantidad infinita de índices $0 \leq r_1 < r_2 < \cdots$ tenemos que

$$deg\, B_{r_j} \geq C \cdot deg\,(b(x_{r_j}))^{r_j}_\infty,$$

donde

$$B_{r_j} := \sum_{P \in L_{r_j}} -v_P(b(x_{r_j}))P \quad \in \mathcal{D}(F_{r_j}).$$

Entonces $\mathcal{F}$ es asintóticamente mala.

Para obtener el resultado deseado como consecuencia de la Proposición 4.1.2 probemos primero que para todo $j \geq 0$ tenemos que

$$L_j \subset \{P \in \mathbb{P}(F_j) : v_P(b(x_j)) < 0 \text{ y } (v_P(b(x_j)), p) = 1\}.$$

Por definición tenemos que

$$L_0 = \{P \in\ supp((b(x_0))^0_\infty) : (v_P(b(x_0)), p) = 1\} \subset \mathbb{P}(F_0).$$

Sea P un lugar de L_0 y Q un lugar de F_1 arriba de P y escribamos $z_j = b(x_{j-1})$ para todo $j \geq 1$. Entonces

$$v_Q(x_1^p - x_1) = e(Q|P)v_P(b(x_0)) = e(Q|P)v_P(z_1) < 0,$$

pues P es un polo de $b(x_0)$. Luego, $v_Q(x_1) < 0$ ya que por el Lemma 1.4.1 sabemos que si $v_Q(x_1) \geq 0$ entonces $v_Q(x_1^p - x_1) \geq 0$. Entonces

$$v_Q(z_2) = v_Q(b(x_1)) = v_Q(b_1(x_1)) - v_Q(b_2(x_1)) = (p - r)v_Q(x_1) < 0,$$

y

$$(v_Q(z_2), p) = ((p - r)v_Q(x_1), p) = 1.$$

Procedemos ahora por inducción. Supongamos que para $j \leq k$ tenemos que

$$L_j \subset \{P \in \mathbb{P}(F_j) : v_P(z_{j+1}) < 0 \text{ y } (v_P(z_{j+1}), p) = 1\}.$$

Sea Q un lugar en L_k y sea R un lugar de F_{k+1} arriba de Q. Entonces

$$v_R(x_{k+1}^p - x_{k+1}) = e(R|Q)v_Q(b(x_k)) = e(R|Q)v_Q(z_{k+1}) < 0,$$

y de la misma manera que antes obtenemos que $v_R(x_{k+1}) < 0$. Luego

$$v_Q(z_{k+2}) = (p - r)v_Q(x_{k+1}) < 0,$$

y

$$(v_Q(z_{k+2}), p) = 1.$$

Observar ahora que si $P \in L_j$ entonces para algún $u \in F_j$ tenemos que

$$v_P(z_{j+1} - (u^p - u)) = -m < 0 \qquad \text{con} \qquad m \not\equiv 0 \mod p.$$

Esto es así ya que si existiera $u \in F_j$ tal que $v_P(u^p - u) = v_P(z_{j+1})$ entonces $0 > v_P(u^p - u)$ y por lo tanto $v_P(u) < 0$. En este caso, tendríamos que $v_P(z_{j+1}) = v_P(u^p - u) = p\, v_P(u)$ contradiciendo el hecho de que $(v_P(z_{j+1}), p) = 1$. Luego, para todo $u \in F_j$ tenemos que $v_P(z_{j+1}) \neq v_P(u^p - u)$ y por la desigualdad triangular estricta para valuaciones (Teorema 1.1.6) tenemos que

$$v_P(z_{j+1} - (u^p - u)) = \min\{v_P(z_{j+1}), v_P(u^p - u)\} \leq v_P(z_{j+1}) < 0,$$

para todo $u \in F_j$. Con esta desigualdad, el Lema 1.2.18 del Capítulo 1 nos asegura que existe $u \in F_j$ tal que

$$v_P(z_{j+1} - (u^p - u)) = -m < 0 \qquad \text{con} \qquad m \not\equiv 0 \mod p.$$

Ahora, afirmamos que si $P \in L_{r_j}$, $Q \in L_{r_{j+1}}$ y $Q|P$ entonces

$$d(Q|P) \geq \frac{1}{2}(-v_P(b(x_{r_j}))[F_{r_{j+1}} : F_{r_j}] \tag{4.3.1}$$

para todo i. Para probar esto, notar que si $L_{r_{j+1}}/L_{r_j}$ es una extensión de Artin-Schreier, entonces

$$d(Q|P) \geq (-v_P(b(x_{r_j})) + 1)([F_{r_{j+1}} : F_{r_j}] - 1)\,,$$

$$\geq \frac{1}{2}(-v_P(b(x_{r_j})))[F_{r_{j+1}} : F_{r_j}]\,.$$

por la teoría general de extensiones de tipo Artin-Schreier (ver Teorema 1.2.19 ítem (c)). En otro caso, tenemos que L_{r_j+2}/L_{r_j+1} y L_{r_j+1}/L_{r_j} sí son extensiones de Artin-Schreier, y por lo tanto si if $P^1 = Q \cap F_{r_j+1}$ y $P^2 = Q \cap F_{r_j+2}$ entonces tenemos que

$$d(P^1|P) \geq \frac{1}{2}(-v_P(b(x_{r_j})))[F_{r_j+1} : F_{r_j}]\,,$$

y que

$$e(P^2|P^1) = [F_{r_j+2} : F_{r_j+1}].$$

Por la transitividad del exponente diferente obtenemos

$$\begin{aligned} d(P^2|P) &\geq e(P^2|P^1)d(P^1|P) \\ &\geq [F_{r_j+2} : F_{r_j+1}]\frac{1}{2}(-v_P(b(x_{r_j})))[F_{r_j+1} : F_{r_j}] \\ &= \frac{1}{2}(-v_P(b(x_{r_j})))[F_{r_j+2} : F_{r_j}]\,. \end{aligned}$$

Luego, si $L_{r_j+1} = L_{r_j+2}$ listo. En caso contrario, como L_{r_j+3}/L_{r_j+2} es una extensión de Artin-Schreier tenemos que

$$e(P^3|P^2) = [F_{r_j+3} : F_{r_j+2}]\,,$$

donde $P^3 = Q \cap F_{r_j+3}$. Por lo tanto,

$$\begin{aligned} d(P^3|P) &\geq e(P^2|P^1)d(P^1|P) \\ &= \frac{1}{2}(-v_P(b(x_{r_j})))[F_{r_j+3} : F_{r_j}]\,. \end{aligned}$$

Ahora, si $L_{r_j+1} = L_{r_j+3}$ listo. En otro caso, continuando con un argumento inductivo se prueba que la afirmación vale. Luego, usando (4.3.1), tenemos que

$$\begin{aligned} \sum_{P \in\, supp(B_{r_j})} \sum_{P'|P} d(P'|P) deg\, P' &\geq \frac{1}{2}[F_{r_{j+1}} : F_{r_j}] \sum_{P \in\, supp(B_{r_j})} -v_P(b(x_{r_j}))deg\, P \\ &= \frac{1}{2}[F_{r_{j+1}} : F_{r_j}] deg\, B_{r_j}\,, \end{aligned}$$

y por lo tanto concluimos que $\mathcal{F}$ es asintóticamente mala por la Proposición 4.1.2, ya que en este caso se cumplen las condiciones con $c_1(j) = C$ y $c_2(j) = 1/2$ para todo $j \geq 0$.

Vamos a ver ahora que el resultado en [**MW05**, Lema 3.2] sobre torres asintóticamente malas se puede deducir del Teorema 4.1.4. En realidad demostraremos una versión ligeramente diferente siguiendo las mismas ideas que en [**MW05**].

Proposición 4.3.3. *Sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una sucesión recursiva de cuerpos de funciones sobre $\mathbb{F}_q$ donde $\mathbb{F}_q$ es el cuerpo total de constantes de cada cuerpo F_i. Supongamos que $\mathcal{F}$ está definida por un polinomio $f \in \mathbb{F}_q[X, Y]$ con el mismo grado m en las dos variables y supongamos que* $\mathrm{mcd}(m, q) = 1$. *Sea $F = \mathbb{F}_q(x, y)$ el correspondiente cuerpo de funciones básico asociado y supongamos que las extensiones $F/\mathbb{F}_q(x)$ y $F/\mathbb{F}_q(y)$ son ambas extensiones de Galois. Sea*

$$N = \{R \in \mathbb{P}(\mathbb{F}_q(y)) : R \text{ ramifica en } F\},$$

y supongamos que existe un lugar P de $\mathbb{F}_q(x)$ con las siguientes propiedades:

(a) P ramifica en F,

(b) $\mathrm{mcd}(\deg P, m) = 1$ *y*

(c) $\deg P$ no divide al grado de ningún lugar R en N.

Entonces $\mathcal{F}$ es asintóticamente mala. Más aún, $\mathcal{F}$ es una torre de cuerpos de funciones asintóticamente mala.

Demostración. Para ver esto, consideremos una sucesión $\{x_n\}_{n=0}^{\infty}$ de elementos trascendentes sobre $\mathbb{F}_q$ tales que

$$F_0 = \mathbb{F}_q(x_0) \quad \text{y} \quad F_{n+1} = F_n(x_{n+1}),$$

donde $f(x_n, x_{n+1}) = 0$ para $n \geq 0$. Sea $n \geq 1$. Por las hipótesis anteriores, existe un lugar P de $\mathbb{F}_q(x_n)$ que ramifica en la extensión $F_q(x_n, x_{n+1})/\mathbb{F}_q(x_n)$ con $\deg P$ coprimo con m y que además no divide a $\deg R$ para ningún lugar R de $\mathbb{F}_q(x_n)$ que ramifica en $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_n)$.

Sea P' un lugar de F_n arriba de P. Sean $P_0, P_1, \ldots, P_n = P$ las restricciones de P' a $\mathbb{F}_q(x_0), \mathbb{F}_q(x_1), \ldots, \mathbb{F}_q(x_n)$ respectivamente (ver Figura 6 a continuación).

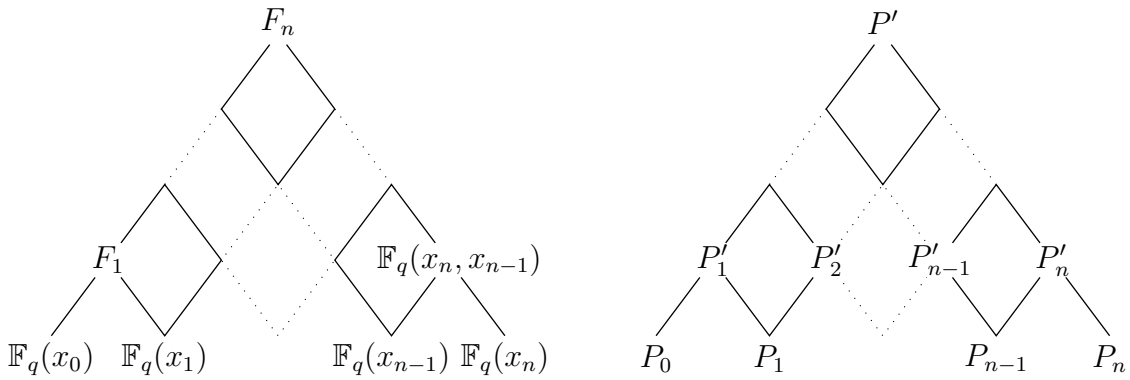

FIGURA 6. Pirámide definida por $P_0, P_1, \ldots, P_n = P$.

Se puede probar que el grado de cada P_i es divisible por el grado de P. En efecto, sea P'_n la restricción de P' a $\mathbb{F}_q(x_{n-1}, x_n)$. Observemos que

$$f(P'_n|P)deg\, P = deg\, P'_n = f(P'_n|P_{n-1})deg\, P_{n-1}$$

donde $f(P'_n|P)$ y $f(P'_n|P_{n-1})$ son los grados relativos del lugar P en las extensiones $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_{n-1})$ y $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_n)$ respectivamente. Como estas extensiones son de Galois, los grados de inercia son divisores de m y como $deg\, P$ es coprimo con m entonces $deg\, P$ divide a $deg\, P_{n-1}$. Ahora, sea P'_{n-1} la restricción de P' a $\mathbb{F}_q(x_{n-2}, x_{n-1})$. Observemos ahora que

$$f(P'_{n-1}|P_{n-1})deg\, P_{n-1} = deg\, P'_{n-1} = f(P'_{n-1}|P_{n-2})deg\, P_{n-2}.$$

Como $deg\, P$ divide al lado izquierdo de la ecuación anterior tenemos que $deg\, P$ divide también a

$$f(P'_{n-1}|P_{n-2})deg\, P_{n-2}$$

y por lo tanto también a $deg\, P_{n-2}$, usando el hecho de que m y $deg\, P$ son coprimos y que la extensión $\mathbb{F}_q(x_{n-2}, x_{n-1})/\mathbb{F}_q(x_{n-2})$ es una extensión de Galois. Continuando de esta manera, vemos que $deg\, P$ divide a $deg\, P_i$ para $i = 1, \ldots, n-1$, y entonces, por hipótesis, tenemos que ninguno de los lugares P_i puede ramificar en la extensión $\mathbb{F}_q(x_{i-1}, x_i)/\mathbb{F}_q(x_i)$.

Por el Lemma de Abhyankar (Proposición 1.2.13), tenemos que $e(P'|P) = 1$ (ver Figura 7 a continuación), y por lo tanto, usando nuevamente el Lema de Abhyankar, tenemos que P' está ramificado en la extensión F_{n+1}/F_n.

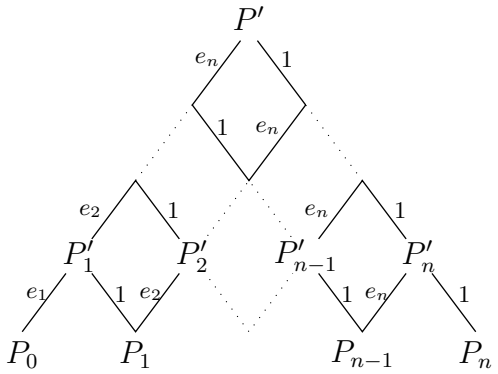

FIGURA 7. Ramificación de P a P'.

Hemos probado entonces que, para cada $n \geq 1$, existe un lugar P en $\mathbb{F}_q(x_n)$ que es no ramificado en F_n y tal que cada lugar Q de F_n arriba de P ramifica en F_{n+1}. Entonces del Teorema 4.1.4 obtenemos que $\mathcal{F}$ es asintóticamente mala. □

Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una sucesión recursiva de cuerpos de funciones sobre K. Supongamos que $\mathcal{F}$ es de tipo Kummer definida por un polinomio $f \in K[x, y]$ de la forma $f(x, y) = y^m b_2(x) - b_1(x)$ donde b_1 y b_2 son polinomios con coeficientes en K tales que $deg\,(b_1) = n - k$ y $deg\,(b_2) = n$. Supongamos que $\mathrm{mcd}(m, k) = 1$ y sea $\{x_i\}_{i=0}^{\infty}$ una sucesión de elementos trascendentes sobre K tales que $F_0 = K(x_0)$ y $F_{i+1} = F_i(x_{i+1})$ con $x_{i+1}^m = b_1(x_i)/b_2(x_i)$. Se puede probar que el lugar P_i, el polo de x_i en F_i, es totalmente ramificado en F_{i+1}/F_i por lo que K es el cuerpo total de constantes de cada cuerpo F_i. Usaremos este hecho en el siguiente ejemplo.

Ejemplo 4.3.4. Sea q una potencia de un primo p, y sea m un número primo impar tal que $q \equiv 1 \mod m$. Consideremos el polinomio

$$f(x, y) = (cx + d)^m y^m + (ax + b)^m - r(cx + d)^m \in \mathbb{F}_q[x, y]\,,$$

donde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)\,,$$

con $c \neq 0$ y $r = a^m c^{-m}$. Este polinomio define una sucesión $\mathcal{F} = (F_0, F_1, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$, donde todas las extensiones F_i/F_{i-1} son de extensiones de Kummer,

para $i \geq 1$. Por la elección de r tenemos que

$$f(x,y) = (cx+d)^m y^m - f(x)\,,$$

donde $f(x) = r(cx+d)^m - (ax+b)^m \in \mathbb{F}_q[x]$ es un polinomio de grado $m-1$. Luego $\mathbb{F}_q$ es el cuerpo total de constantes de cada cuerpo F_i por los comentarios anteriores. El cuerpo de funciones básico asociado es $\mathbb{F}_q(x,y)$ con

$$y^m = r - \left(\frac{ax+b}{cx+d}\right)^m . \tag{4.3.2}$$

Sea $\{x_i\}_{i=0}^{\infty}$ una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ tales que $F_0 = \mathbb{F}_q(x_0)$ y $F_{i+1} = F_i(x_{i+1})$ con

$$x_{i+1}^m = r - \left(\frac{ax_i+b}{cx_i+d}\right)^m = \frac{f(x_i)}{(cx_i+d)^m}\,.$$

Como consecuencia de la Proposición 4.3.3, vamos a mostrar que si el polinomio f, de grado $m-1$, tiene al menos un factor $g \in \mathbb{F}_q[x]$ mónico e irreducible de grado $d \geq 2$ entonces $\mathcal{F}$ es una torre asintóticamente mala sobre $\mathbb{F}_q$. Primero observemos que las extensiones $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ y $\mathbb{F}_q(x,y)/\mathbb{F}_q(y)$ son ambas extensiones de Galois de grado m. Esto es claro en el caso $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ pues esta extensión es una extensión de Kummer. Para el otro caso, consideremos el siguiente cambio de variables:

$$u = \frac{ax+b}{cx+d} \quad \text{y} \quad v = \frac{ay+b}{cy+d}\,.$$

Entonces

$$y = \frac{dv-b}{a-cv}\,,$$

y esto implica que $\mathbb{F}_q(y) = \mathbb{F}_q(v)$ y $\mathbb{F}_q(x,y) = \mathbb{F}_q(v,u)$ con

$$u^m = r - \left(\frac{dv-b}{a-cv}\right)^m .$$

Entonces $\mathbb{F}_q(v,u)/\mathbb{F}_q(v)$ es una extensión de Kummer y por lo tanto $\mathbb{F}_q(x,y)/\mathbb{F}_q(y)$ es una extensión de Galois de grado m.

Simplificando (4.3.2) tenemos que la extensión $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ puede definirse también por la ecuación

$$y^m = \frac{f(x)}{(cx+d)^m}\,.$$

Por la teoría de extensiones de Kummer tenemos que el lugar P_g de $\mathbb{F}_q(x)$ definida por $g(x)$ está (totalmente) ramificado en $\mathbb{F}_q(x,y)$ y es de grado $d \geq 2$ pues $g(x)$ es mónico e irreducible en $\mathbb{F}_q[x]$ y de grado $d \geq 2$. Luego $\text{mcd}(deg\, P_g, m) = 1$. Entonces *(a)* y *(b)* de la Proposición 4.3.3 valen para el lugar P_g.

Falta probar que *(c)* vale. Sea R un lugar de $\mathbb{F}_q(y)$ que ramifica en $\mathbb{F}_q(x,y)$. Notar que la extensión $\mathbb{F}_q(x,y)/\mathbb{F}_q(y)$ está definida por el polinomio mónico

$$\sigma(T) = (T + dc^{-1})^m - f(T)(cy)^{-m} \in \mathbb{F}_q(y)[T]\,,$$

pues $\sigma(x) = 0$. En otras palabras $\sigma(T)$ es el polinomio mínimo de x sobre $\mathbb{F}_q(y)$. Sea $y(R)$ la clase de residuos módulo R de y y consideremos el polinomio

$$\overline{\sigma}_R(T) = (T + dc^{-1})^m - f(T)\alpha \in \overline{\mathbb{F}}_q[T]\,,$$

donde $\overline{\mathbb{F}}_q$ denota una clausura algebraica de $\mathbb{F}_q$ y $\alpha = (cy(R))^{-m}$. Por la Proposición 2.1.1 del Capítulo 2 sabemos que el conjunto de lugares de $\mathbb{F}_q(y)$ que ramifican en $\mathbb{F}_q(x,y)$ está contenido en el conjunto

$$\{Q \in \mathbb{P}(\mathbb{F}_q(y)) \,:\, v_Q(y) = 0 \quad \text{y } \overline{\sigma}_Q(T) \text{ no es separable}\} \cup \{P_\infty\} \cup \{P_y\}\,,$$

donde P_∞ (resp. P_y) es el polo (resp. el cero) de y en $\mathbb{F}_q(y)$. Si R es P_∞ ó P_y entonces *(c)* vale pues en este caso $deg\, R = 1$. Supongamos que $\overline{\sigma}_R(T)$ no es separable. Entonces $\overline{\sigma}_R(T)$ debe tener un factor de la forma $(T-\beta)^j$ con $j \geq 2$ para algún $\beta \in \overline{\mathbb{F}}_q$. Por el Teorema de Kummer hay un lugar Q de $\mathbb{F}_q(x,y)$ arriba de R con grado de inercia al menos 2. Como la extensión $\mathbb{F}_q(x,y)/\mathbb{F}_q(y)$ es de Galois, todo lugar de $\mathbb{F}_q(x,y)$ arriba de R debe tener grado de inercia al menos 2. Pero $[\mathbb{F}_q(x,y) : \mathbb{F}_q(y)] = m$ y m es primo. Esto implica que existe un único lugar en $\mathbb{F}_q(x,y)$ arriba de R y que el grado de inercia de este lugar es m. Entonces R no ramifica en $\mathbb{F}_q(x,y)$ y por lo tanto *(c)* de la Proposición 4.3.3 vale. Luego, $\mathcal{F}$ es una torre asintóticamente mala sobre $\mathbb{F}_q$.

4.4. La torre dual

Supongamos que la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ está definida recursivamente por el polinomio $f(x,y) \in \mathbb{F}_q[x,y]$. La *sucesión dual* $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ se define como la

sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ dada recursivamente por el polinomio $f(y,x)$. Para ello, se identifican los cuerpos de funciones racionales $F_0 = \mathbb{F}_q(x_0)$ y $G_0 = \mathbb{F}_q(y_0)$ poniendo $x_0 = y_0$. Entonces se tiene que $F_0 = G_0$ y

$$F_n = \mathbb{F}_q(x_0, \ldots, x_n) \quad \text{con} \quad f(x_i, x_{i+1}) = 0, \text{ y}$$
$$G_n = \mathbb{F}_q(y_0, \ldots, y_n) \quad \text{con} \quad f(y_{i+1}, y_i) = 0$$

para todo $n \geq 2$ y $1 \leq i \leq n-1$.

Notar que los cuerpos de funciones F_n y G_n son $\mathbb{F}_q$-isomorfos para todo $n \geq 0$.

Para $P \in \mathbb{P}(F_0)$ se define el conjunto

$$\epsilon(P, \mathcal{F}) := \sup_{n \geq 1} \{e(Q_n|P) : Q_n \in \mathbb{P}(F_n) \text{ y } Q_n|P\}.$$

Ejemplo 4.4.1. Sea $\mathcal{F} = (F_0, F_1, \ldots)$ una sucesión recursiva de cuerpos de funciones sobre $\mathbb{F}_q$, definida por un polinomio $f(x,y) \in \mathbb{F}_q[x,y]$ separable en las dos variables y con el mismo grado $deg\,(f_X) = deg\,(f_Y) = m$. Sea $\mathcal{G} = (G_0, G_1, \ldots)$ la sucesión dual de $\mathcal{F}$ y sea $P \in \mathbb{P}(F_0) = \mathbb{P}(G_0)$. Se puede ver que si

$$\epsilon(P, \mathcal{F}) \neq \epsilon(P, \mathcal{G})\,,$$

entonces $\mathcal{F}$ es una torre de cuerpos de funciones y es asintóticamente mala. En efecto, para ver esto seguimos la prueba dada en [**BGS05a**] considerando que $\mathcal{F}$ es una sucesión sobre una clausura algebraica $K = \overline{\mathbb{F}}_q$ de $\mathbb{F}_q$ (recordar que el género de una sucesión y los índices de ramificación no cambian por extensiones de cuerpos constantes). Por lo tanto todos los lugares de F_i son racionales (de grado uno) para cualquier i. Además,

$$[F_{n+1} : F_n] = [G_{n+1} : G_n] = m\,,$$

para todo $n \geq 1$.

Sin pérdida de generalidad, podemos suponer que $\epsilon(P, \mathcal{F}) > \epsilon(P, \mathcal{G})$. Entonces $e_1 := \epsilon(P, \mathcal{G})$ es un entero positivo. Por definición de $\epsilon(P, \mathcal{G})$ tenemos que existe un entero positivo n y un lugar $Q_1 \in \mathbb{P}(G_n)$ tales que

(I) $e(Q_1|P) = e_1$.

(II) Q_1 se descompone completamente en G_l/G_n para todo $l \geq n$.

Como $\epsilon(P,\mathcal{F}) > \epsilon(P,\mathcal{G})$ existe un entero positivo k tal que hay algún lugar $Q_2 \in \mathbb{P}(F_k)$ arriba de P con

$$e_2 = e(Q_2|P) > e_1\,.$$

Sea $l \geq n$ y sea $H_l := F_k \cdot G_l$ (resp. $H_n := F_k \cdot G_n$) la composición del cuerpo F_k con G_l (resp. con G_n). Consideremos un lugar $R_1 \in \mathbb{P}(G_l)$ arriba del lugar Q_1 (ver Figura 8).

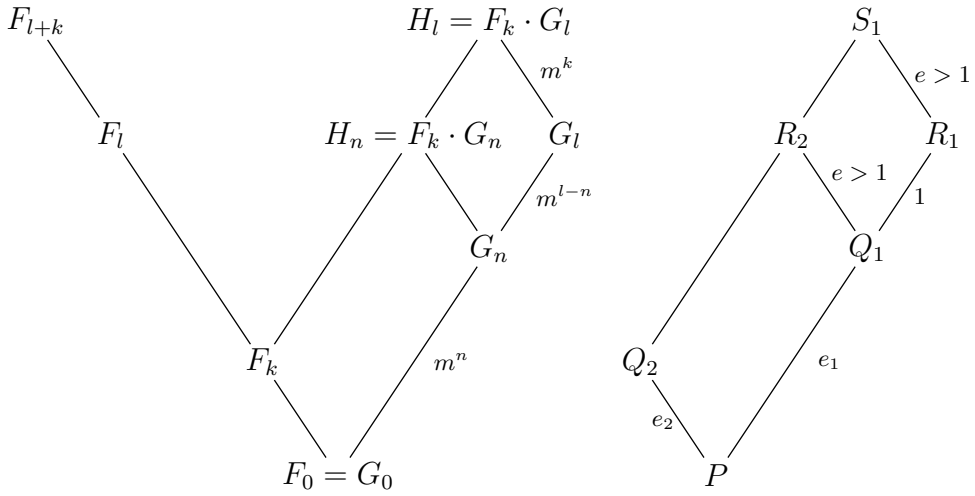

FIGURA 8. Ramificación de P en $\mathcal{F}$ y $\mathcal{G}$.

Por [**MW05**, Lema 2.1] tenemos que existe un lugar $R_2 \in \mathbb{P}(H_n)$ que está arriba de Q_1 y de Q_2. Como $e_2 > e_1$ entonces $e(R_2|Q_1) > 1$. Nuevamente por [**MW05**, Lema 2.1] tenemos que existe un lugar $S_1 \in \mathbb{P}(H_l)$ que está arriba de R_1 y de R_2. Entonces $e(S_1|R_1) = e(R_2|Q_1) > 1$. Como

$$\#\{R_1 \in \mathbb{P}(G_l) : R_1|Q_1\} = [G_l : G_n] = m^{l-n}$$

concluimos que hay, al menos, m^{l-n} lugares de G_l que ramifican en H_l. Por otro lado, como $H_l = \mathbb{F}_q(x_k, \ldots, x_1, x_0, y_1, \ldots, y_l)$, tenemos que H_l es isomorfo a F_{l+k} por medio de la aplicación que manda x_i en x_{l+i} para $0 \leq i \leq k$ y y_i en x_{l-i} para $1 \leq i \leq l$. Luego, como hay al menos m^{l-n} lugares de G_l que ramifican en H_l y la aplicación anterior restringida a G_l transforma G_l en F_l, también hay, al menos, m^{l-n} lugares de F_l que ramifican en F_{l+k}, (ver Lema 1.2.3 del Capítulo 1).

Consideremos ahora la sucesión $\{r_j\}_{j\geq 0}$ donde $r_j = n + jk$. Sabemos que en cada extensión F_{r_j} hay al menos

$$m^{r_j - n} = m^{n+jk-n} = m^{jk}$$

lugares, $P_1, P_2, \ldots, P_{m^{jk}}$, que ramifican en la extensión $F_{r_{j+1}}$. Sea

$$B_{r_j} = \sum_{i=1}^{m^{jk}} P_i.$$

Entonces

$$deg\, B_{r_j} = \sum_{i=1}^{m^{jk}} deg\, P_i = m^{jk} \geq [F_{r_j} : F_0]\,,$$

que es (4.1.2) de la Proposición 4.1.2 con $c_1(j) = 1$. Además

$$\begin{aligned} \sum_{P \in\, supp B_{r_j}} \sum_{P'|P} d(P'|P) deg\, P' &\geq \sum_{i=1}^{m^{jk}} (e(P'|P) - 1) \\ &\geq m^{jk} \\ &= \frac{1}{m^k} [F_{r_{j+1}} : F_{r_j}] deg\, B_{r_j}\,, \end{aligned}$$

y entonces $c_2(j) = m^{-k}$ en *(b)* de la Proposición 4.1.2, y por lo tanto $\mathcal{F}$ es una sucesión sobre K con género infinito. Luego, $\mathcal{F}$ tiene género infinito como sucesión sobre $\mathbb{F}_q$ y con esto tenemos que $\mathcal{F}$ es una torre sobre $\mathbb{F}_q$ que es asintóticamente mala.

CONCLUSIONES Y TRABAJO FUTURO

En esta Tesis hemos obtenido resultados estructurales generales sobre el comportamiento asintótico de torres recursivas de cuerpos de funciones sobre cuerpos finitos. Específicamente, en el Capítulo 1 dimos condiciones suficientes para que diversos tipos de ecuaciones polinómicas con coeficientes en un cuerpo perfecto definan sucesiones de cuerpos de funciones que sean torres. En el Capítulo 2 dimos condiciones suficientes para estimar la cantidad de lugares racionales en cada paso de una sucesión de cuerpos de funciones definida por una ecuación de la forma $a(x) = b(y)$. Estos resultados probaron su utilidad ya que nos permitieron dar un tratamiento unificado tanto de ejemplos ya conocidos como de nuevos ejemplos. En el Capítulo 3 estudiamos el problema del comportamiento del género de una sucesión recursiva de cuerpos de funciones a través de la finitud de su espacio de ramificación. Dimos condiciones suficientes para que ecuaciones de tipo Kummer definan torres asintóticamente buenas. Además de obtener varios ejemplos de torres de tipo Kummer asintóticamente buenas y óptimas en algunos casos, dimos un demostración alternativa de la no trivialidad de la función de Ihara para potencias pares de primos. Paralelamente estudiamos el problema de la generación de subsucesiones y supersucesiones de una sucesión recursiva de cuerpos de funciones dada. Dimos condiciones suficientes para la construcción efectiva de subsucesiones y supersucesiones mostrando que varios ejemplos conocidos son casos particulares de esta construcción permitiendo dar demostraciones alternativas del buen o mal comportamiento asintótico de esta clase de sucesiones. Finalmente en el Capítulo 4 abordamos el problema del mal comportamiento asintótico de sucesiones recursivas de cuerpos de funciones. Obtuvimos varios resultados que establecen condiciones suficientes para que una sucesión recursiva de cuerpos de funciones defina una torre asintóticamente mala. Mostramos que la mayoría de los ejemplos conocidos son casos particulares de nuestros resultados. Además,

este enfoque general nos permitió redemostrar que la infinitud del espacio de ramificación de una sucesión recursiva de cuerpos de funciones garantiza su mal comportamiento asintótico siempre que todas las extensiones F_{i+1}/F_0 de la sucesión en cuestión sean de Galois.

En vista de los resultados obtenidos en esta Tesis, han surgido nuevos interrogantes que consideramos lo suficientemente interesantes como para haber sido abordados en la misma pero que, por falta de tiempo principalmente, quedarían para ser estudiados en una etapa posdoctoral. Concretamente, en el Capítulo 2 dimos ejemplos de torres de tipo Kummer con tasa de descomposición positiva sobre cuerpos primos. Estudiar el comportamiento del género en estas sucesiones podría resultar en los primeros ejemplos de torres recursivas asintóticamente buenas sobre cuerpos primos. Hasta el momento los únicos ejemplos conocidos de torres asintóticamente buenas sobre cuerpos primos son de tipo no recursivo y están construidas de manera no explícita utilizando la existencia del cuerpo de clases de Hilbert de un cuerpo global. En el Capítulo 3 definimos una manera para construir subsucesiones y supersucesiones de una sucesión recursiva de cuerpos de funciones dada. En este contexto quedaron planteadas varias preguntas con respecto a la relación que puede haber con el género, número de lugares racionales, espacio de ramificación y tasa de descomposición de la sucesión dada y las respectivas subsucesiones y supersucesiones construidas con este método. Finalmente en el Capítulo 4 dimos un tratamiento unificado al problema de la determinación del mal comportamiento asintótico de sucesiones de cuerpos de funciones sobre un cuerpo perfecto K. En particular dimos una nueva demostración de que ramificación infinita en sucesiones de Galois de tipo II implica mal comportamiento asintótico. En este aspecto es natural ver si nuestros resultados generales nos permiten abordar el caso de sucesiones de Galois de tipo I con ramificación infinita. Esto implicaría que la ramificación infinita es esencial en el comportamiento asintótico de sucesiones de tipo Kummer o Artin-Schreier y, en consecuencia, llevaría a plantearse bajo qué condiciones se puede garantizar ramificación infinita en este tipo de sucesiones. Estas condiciones podrían contribuir a abordar el problema, aún no resuelto, de clasificar en términos de comportamiento asintótico a las ecuaciones polinomiales que definen sucesiones de tipo Kummer.

BIBLIOGRAFÍA

[BGS04] P. Beelen, A. Garcia, and H. Stichtenoth. On towers of function fields of Artin-Schreier type. *Bull. Braz. Math. Soc. (N.S.)*, 35(2):151–164, 2004.

[BGS05a] P. Beelen, A. Garcia, and H. Stichtenoth. On ramification and genus of recursive towers. *Port. Math. (N.S.)*, 62(2):231–243, 2005.

[BGS05b] P. Beelen, A. Garcia, and H. Stichtenoth. On towers of function fields over finite fields. In *Arithmetic, geometry and coding theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 1–20. Soc. Math. France, Paris, 2005.

[BGS05c] J. Bezerra, A. Garcia, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *J. Reine Angew. Math.*, 589:159–199, 2005.

[BS07] A. Bassa and H. Stichtenoth. A simplified proof for the limit of a tower over a cubic finite field. *Journal of Number Theory*, 123(1):154 – 169, 2007.

[CT11] M. Chara and R. Toledano. Rational places in extensions and sequences of function fields of kummer type. *Journal of Pure and Applied Algebra*, 215(11):2603 – 2614, 2011.

[DPZ04] E. Duursma, B. Poonen, and M. Zieve. Everywhere ramified towers of global function fields. In *Finite fields and applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 148–153. Springer, Berlin, 2004.

[GG03] A. Garcia and A. Garzon. On Kummer covers with many rational points over finite fields. *J. Pure Appl. Algebra*, 185(1-3):177–192, 2003.

[Gop81] V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981.

[GS96] A. Garcia and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996.

[GS07] A. Garcia and H. Stichtenoth. Explicit towers of function fields over finite fields. In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 1–58. Springer, Dordrecht, 2007.

[GSR03] A. Garcia, H. Stichtenoth, and H.G. Rück. On tame towers over finite fields. *J. Reine Angew. Math.*, 557:53–80, 2003.

[GST97] A. Garcia, H. Stichtenoth, and M. Thomas. On towers and composita of towers of function fields over finite fields. *Finite Fields Appl.*, 3(3):257–274, 1997.

[Has34] H. Hasse. Theorie der relativ-zyklischen algebraischen funktionenkörper, insbesondere bei endlichem konstantenkörper. *J. Reine Angew. Math.*, 172:37–54, 1934.

[Hil86] R. Hill. *A first course in coding theory*. Oxford Applied Mathematics and Computing Science Series. The Clarendon Press Oxford University Press, New York, 1986.

[HK03] T. Hiramatsu and G. Köhler. *Coding theory and number theory*, volume 554 of *Mathematics and its Applications*. Kluwer Academic Publishers Group, Dordrecht, 2003.

[Iha81] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[Man81] Y. Manin. What is the maximum number of points on a curve over $\mathbf{F}_2$? *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):715–720 (1982), 1981.

[MW05] H. Maharaj and J. Wulftange. On the construction of tame towers over finite fields. *J. Pure Appl. Algebra*, 199(1-3):197–218, 2005.

[Qiu10] Y. Qiu. On a link between towers of function field and groups theory. Eindhoven University of Technology, 2010.

[Ser83] J. P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.

[Ser85] J.P. Serre. Rational points on curves over finite fields. Unpublished lecture notes by F. Q. Gouvea, Harvard University, 1985.

[Sti09] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[TV91] M. A. Tsfasman and S. G. Vladut. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991. Translated from the Russian by the authors.

[TVZ82] M. Tsfasman, S. Vladut, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

[VD83] S. G. Vladut and V. G. Drinfeld. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.

[vdGvdV] G. van der Geer and M. van der Vlugt. Table of curves with many points. http://www.manypoints.org.

[vdGvdV00] G. van der Geer and M. van der Vlugt. Kummer covers with many points. *Finite Fields Appl.*, 6(4):327–341, 2000.

[vdGvdV02] G. van der Geer and M. van der Vlugt. An asymptotically good tower of curves over the field with eight elements. *Bull. London Math. Soc.*, 34(3):291–300, 2002.

[Wei48] A. Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[Zin85] T. Zink. Degeneration of Shimura surfaces and a problem in coding theory. In *Fundamentals of computation theory (Cottbus, 1985)*, volume 199 of *Lecture Notes in Comput. Sci.*, pages 503–511. Springer, Berlin, 1985.

ÍNDICE ALFABÉTICO