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 asintótico de torres y subtorres de cuerpos de funciones

Autor:
Horacio Navarro Oyola

Institución donde se realizó la investigación:

Instituto de Matemática Aplicada del Litoral (IMAL)
CONICET–UNL

Director de Tesis: Dr. Ricardo Toledano
Codirectora de Tesis: Dra. María Chara

Tesis defendida ante el jurado compuesto por:

Dra. Manuela Busaniche
Dr. Guillermo Matera
Dr. Ariel Pacetti

Año de presentación: 2018

Índice general

RESUMEN

Esta tesis tiene como finalidad el estudio asintótico de sucesiones y subsucesiones recursivas de cuerpos de funciones sobre cuerpos finitos, entre ellas, se destaca la sucesión $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ definida por la ecuación de tipo Artin-Schreier

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

sobre un cuerpo finito $\mathbb{F}_{2^s}$ con 2^s elementos. Determinar el comportamiento asintótico de esta torre sobre tales cuerpos finitos fue un problema propuesto por Beelen, Garcia y Stichtenoth [2].

El trabajo está dividido en tres capítulos. En el primero introducimos conceptos fundamentales de la teoría de torres de cuerpos de funciones sobre cuerpos finitos. El segundo está dedicado a la resolución del problema planteado líneas arriba; en este sentido, demostramos que la sucesión $\mathcal{H}$ es una torre de género finito sobre $\mathbb{F}_{2^s}$ para cualquier entero positivo s y probamos que el comportamiento de la tasa de descomposición depende de la paridad de s. Adicionalmente, calculamos de forma precisa el número de lugares racionales y el género de cada cuerpo de funciones F_i sobre $\mathbb{F}_4$, deduciendo que la torre $\mathcal{H}$ sobre $\mathbb{F}_4$ es una torre asintóticamente óptima. El tercer capítulo se enfoca en la construcción de subsucesiones y supersucesiones de cuerpos de funciones y a la generalización de algunos resultados conocidos.

INTRODUCCIÓN

El problema de cuántos lugares (puntos) racionales puede tener un cuerpo de funciones (curva) de género g definido sobre un cuerpo finito $\mathbb{F}_q$ ha sido objeto de estudio durante muchos años en teoría de números. En 1948 Weil [23] demostró la hipótesis de Riemann para cuerpos de funciones sobre cuerpos finitos y como consecuencia obtuvo el siguiente resultado: dado un cuerpo de funciones F sobre $\mathbb{F}_q$ de género g, el número de lugares racionales $N(F)$ satisface la desigualdad

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

La cota anterior es conocida como cota de Hasse-Weil. En 1981 Ihara [16] y Manin [18] notaron que esta cota puede ser mejorada si el género es grande en comparación con la cardinalidad del cuerpo finito sobre el cual se considere el cuerpo de funciones. De hecho, en ese mismo artículo Ihara introdujo la función

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g} \tag{2}$$

donde $N_q(g)$ es el máximo número de lugares racionales de un cuerpo de funciones sobre $\mathbb{F}_q$ de género g y probó que $A(q) \leq \sqrt{2q}$, mejorando la cota para $A(q)$ que se obtiene de (1). También demostró que $A(q^2) \geq q-1$ y conjeturó que en realidad vale la igualdad. En 1983 Drinfeld y Vlâdut [9] probaron, para todo q, que

$$A(q) \leq \sqrt{q} - 1$$

y en particular concluyeron que $A(q^2) = q-1$. Si q no es un cuadrado el valor exacto de $A(q)$ no se conoce, sólo se conocen cotas inferiores; algunas de ellas se han obtenido usando torres de cuerpos de clases. Serre [19] demostró que existe una constante $c > 0$ tal que $A(q^n) \geq c\, n \log(q)$ para todo q y todo entero $n > 0$ y Temkine [22] en 2001 probó que existe una constante $c > 0$ tal que para todo q y todo entero $n > 0$

$$A(q^n) \geq c\, n^2 \log(q) \frac{\log(q)}{\log(n) + \log(q)}.$$

Esta es una generalización de la cota de Serre que resulta ser mejor para todo q no primo. Anteriormente Zink [24] había usado superficies de Shimura degeneradas para probar que si p es primo entonces

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

Motivados por potenciales aplicaciones a la teoría de códigos, Garcia y Stichtenoth en [11] introducen la noción de torres recursivas en las que los cuerpos de funciones que la componen son definidos explícitamente mediante una única ecuación. Un resultado clave en ese trabajo es que la torre $\mathcal{F}$ definida recursivamente por la ecuación

$$y^q + y = \frac{x^q}{1+x^{q-1}} \tag{3}$$

es asintóticamente óptima sobre $\mathbb{F}_{q^2}$, esto es, el límite $\lambda(\mathcal{F})$ de la torre $\mathcal{F}$ satisface

$$\lambda(\mathcal{F}) = q - 1 = A(q^2).$$

De esta manera, los autores dieron una prueba alternativa a la conjetura de Ihara. La ventaja que tienen las torres de cuerpos de funciones frente a los métodos que se habían usado previamente para obtener cotas de $A(q)$ radica en que cada cuerpo de funciones de la torre está definido en términos de ecuaciones y generadores y esto resulta ser de gran utilidad al momento de trabajar en aplicaciones concretas, como es el caso de la teoría de códigos. Un ejemplo de esto se ve en [21] en donde, a partir de la torre recursiva definida por la ecuación (3), se construye una sucesión de códigos asintóticamente buena que mejora la cota inferior clásica Gilbert-Varshamov para la función de Manin en teoría de códigos, considerada por mucho tiempo como inmejorable. También usando torres recursivas de cuerpos de funciones, ver [4], se obtuvo una generalización de la cota inferior de Zink: para todo q se satisface que

$$A(q^3) \geq \frac{2q^2-1}{q+2}.$$

En el año 2006 Beelen, García y Stichtenoth [2] dieron los primeros pasos hacia la clasificación de torres recursivas sobre un cuerpo finito $\mathbb{F}_q$ con q elementos, de acuerdo a su comportamiento asintótico. Los autores se enfocaron en torres recursivas definidas por ecuaciones de la forma $a(y) = b(x)$, donde a y b son funciones racionales adecuadas sobre $\mathbb{F}_q$. Este tipo de torres son llamadas (a,b)-torres sobre $\mathbb{F}_q$. En particular, observaron que muchas (a,b)-torres pueden definirse recursivamente por ecuaciones de la forma $h(y) = A \cdot h(B \cdot x)$ para algún polinomio h sobre $\mathbb{F}_q$

y A, $B \in \mathrm{GL}_2(\mathbb{F}_q)$. En este caso el símbolo $A \cdot u$ se usa para denotar la acción de elementos de $\mathrm{GL}_2(\mathbb{F}_q)$ como una transformación de Möbius, esto es,

$$\begin{pmatrix} c & d \\ e & f \end{pmatrix} \cdot u := \frac{cu+d}{eu+f}.$$

Esta observación fue clave y les permitió obtener resultados en la clasificación de torres de tipo Kummer y Artin-Schreier que son de gran importancia en la teoría. Como una aplicación de esos resultados dieron una lista de todas las (a,b)-torres de tipo Artin-Schreier con $\deg a = \deg b = 2$ sobre el cuerpo finito $\mathbb{F}_2$ y verificaron que todos los posibles casos se habían considerado en trabajos previos, excepto la sucesión de tipo Artin-Schreier $\mathcal{H}$ sobre $\mathbb{F}_2$ definida recursivamente por la ecuación

$$y^2 + y = \frac{x}{x^2+x+1}. \tag{4}$$

En este sentido, Beelen, Garcia y Stichtenoth plantearon, en ese mismo artículo, como un problema abierto determinar si existe algún entero positivo $s \geq 1$ tal que la sucesión recursiva $\mathcal{H}$ definida por (4) sea una torre asintóticamente buena sobre $\mathbb{F}_{2^s}$. Este problema es resuelto en esta tesis y de esta forma completamos la clasificación de las (a,b)-torres de tipo Artin-Schreier con $\deg a = \deg b = 2$ sobre $\mathbb{F}_2$ iniciado por dichos autores.

Esta tesis se divide en tres capítulos. En el capítulo uno damos las definiciones básicas y algunos resultados conocidos de la teoría de cuerpos de funciones y de torres de cuerpos de funciones. En el capítulo dos demostramos que para cualquier entero positivo s la sucesión $\mathcal{H}$ es en realidad una torre sobre $\mathbb{F}_{2^s}$, que es 2-acotada y de espacio de ramificación finito lo que implica que $\mathcal{H}$ es de género finito. Por otra parte, probamos que el comportamiento de la tasa de descomposición depende de la paridad de s: cuando s es par la torre $\mathcal{H}$ tiene tasa de descomposición positiva lo cual, junto con la finitud del género, implica que la torre $\mathcal{H}$ es asintóticamente buena; cuando s es impar la tasa de descomposición es cero lo que implica que $\mathcal{H}$ es asintóticamente mala. Debemos destacar la importancia de la prueba para $s = 2$ pues la ramificación o no de algunos lugares de la torre depende de la existencia de ciertos elementos, que denominamos de tipo 1 o tipo 2, que se construyen a partir de manipulaciones de carácter técnico de la ecuación (4). Por un lado, lo anterior nos permite afirmar que los lugares racionales de $\mathcal{H}$ siempre ramifican en algún paso de la torre e inmediatamente después se descomponen completamente y, por otro lado, nos permite calcular de forma precisa el número de lugares racionales y el género de cada cuerpo de funciones de la torre. De lo que se concluye que la torre $\mathcal{H}$ sobre $\mathbb{F}_4$

es asintóticamente óptima.

Finalmente, el capítulo tres lo dedicamos a la construcción de subsucesiones y supersucesiones de cuerpos de funciones. En este orden, formulamos un método para obtener una subsucesión propia a partir de una (a, b)-sucesión recusiva no trivial, el cual puede implementarse computacionalmente de forma sencilla; además, constatamos que varias de las subtorres conocidas en la literatura pueden obtenerse por la aplicación del método descrito y, adicionalmente, probamos que el método dado en [6] es un caso particular del nuestro. Por otra parte, generalizamos un resultado dado en el artículo [14] relacionado con la obtención de una supertorre asíntoticamente buena a partir de una torre asintóticamente buena. Finalmente, extendimos el resultado de [8] en el que se dan condiciones suficientes para que una (a, b)-sucesión recursiva no trivial tenga espacio de descomposición no vacío a sucesiones recursivas definidas por ecuaciones reducibles.

CAPÍTULO 1
PRELIMINARES

En este capítulo introducimos conceptos y resultados fundamentales de la teoría de cuerpos de funciones y torres de cuerpos de funciones sobre cuerpos finitos necesarios para el desarrollo de la tesis. Las demostraciones se pueden consultar en las secciones $1, 3$ y 7 del texto [20].

1.1. Extensiones algebraicas de cuerpos de funciones

Una extensión de cuerpos F/k se dice un **cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre k tal que F es una extensión finita del cuerpo de funciones racionales $k(x)$ sobre k. Por simplicidad diremos que F/k es un cuerpo de funciones.

Dado un cuerpo de funciones F/k, la clausura algebraica de k en F es un subcuerpo de F y lo denotaremos por $\overline{k}_F$. Es claro que $F/\overline{k}_F$ también es un cuerpo de funciones y en caso de que $k = \overline{k}_F$ diremos que k es el **cuerpo total de constantes** de F/k.

Sea F/k un cuerpo de funciones. Un **anillo de valuación discreta** $\mathcal{O}$ de F/k es un anillo intermedio propio de F/k, esto es, $k \subsetneq \mathcal{O} \subsetneq F$ tal que para todo $z \in F$ se tiene que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$. Se puede probar que los anillos de valuación discreta de un cuerpo de funciones son anillos locales, es decir, tienen un único ideal maximal. ([20, Proposición 1.1.15]).

Un **lugar** P de un cuerpo de funciones F/k es un ideal maximal de algún anillo de valuación discreta de F/k. Al conjunto de lugares de F/k lo denotamos por $\mathbb{P}(F)$.

Una **valuación discreta** de un cuerpo de funciones F/k es una función sobreyectiva $\nu : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ que satisface las siguientes condiciones:

i. $\nu(x) = \infty$ si y sólo si $x = 0$.

ii. $\nu(xy) = \nu(x) + \nu(y)$ para todo $x, y \in F$.

iii. $\nu(x + y) \geq \text{mín}\{\nu(x), \nu(y)\}$ para todo $x, y \in F$.

iv. $\nu(a) = 0$ para todo $a \in k^* := k \setminus \{0\}$.

Una propiedad de mucha utilidad al momento de trabajar con valuaciones es la **desigualdad triangular estricta**, la cual es consecuencia de los axiomas anteriores, y afirma que: dados $x, y \in F$ tales que $\nu(x) \neq \nu(y)$ entonces

$$\nu(x + y) = \text{mín}\{\nu(x), \nu(y)\}.$$

Se puede probar que existe una biyección entre los lugares y las valuaciones discretas de un cuerpo de funciones. También se ve que dado un lugar P de F/k entonces

$$\mathcal{O}_P = \{x \in F : \nu_P(x) \geq 0\} \quad \text{y} \quad P = \{x \in F : \nu_P(x) > 0\},$$

donde ν_P denota la valuación discreta correspondiente a P. Si x es un elemento no nulo de F tal que $\nu_P(x) > 0$ decimos que P es un **cero** de x y si $\nu_P(x) = m > 0$ decimos que P es un cero de x de **orden** m. Si $\nu_P(x) < 0$ decimos que P es un **polo** de x y si $\nu_P(x) = -m < 0$ decimos que P es un polo de x de **orden** m. Si P es un cero (resp. un polo) de orden 1 de x decimos que P es un **cero simple** (resp. **polo simple**) de x. Un elemento $x \in F$ es llamado un **elemento primo** o **parámetro local** para P si P es un cero simple de x.

Dado un lugar P de F/k, se define el **cuerpo de clases residuales** en P como $F_P := \mathcal{O}_P/P$. Si $x \in \mathcal{O}_P$ denotamos la clase residual de x módulo P como $x(P)$. La proyección canónica

$$\phi_P : \mathcal{O}_P \to F_P$$

induce una inmersión de cuerpos de $\overline{k}_F$ a F_P. Por lo tanto se puede ver a $\overline{k}_F$ y a k como subcuerpos de F_P. Se define el **grado** de P como $\deg P := [F_P : k]$. Se puede probar que cualquier lugar P tiene grado finito y que $[\overline{k}_F : k] \leq \deg P$. En particular si P es un lugar de grado uno tenemos que $\overline{k}_F = k$, es decir, k es el cuerpo total de constantes de F/k. Un lugar de grado uno es llamado racional.

En adelante F/k denotará un cuerpo de funciones con k su cuerpo total de constantes.

A continuación damos los conceptos necesarios para definir el género de un cuerpo de funciones que es un invariante de gran importancia en esta teoría.

Un **divisor** D de F/k es una suma formal $D = \sum_{P\in\mathbb{P}(F)} n_P P$ donde n_P son coeficientes enteros y $n_P \neq 0$ a lo más para un número finito de lugares $P \in \mathbb{P}(F)$. Es común escribir $\nu_P(D)$ en vez de n_P. Si D es un divisor de F/k definimos el **grado** $\deg(D)$ de D como $\deg(D) = \sum_{P\in\mathbb{P}(F)} \nu_P(D)\deg(P)$ y el **espacio de Riemann-Roch** de D como:

$$\mathcal{L}(D) := \{x \in F : \nu_P(x) \geq -\nu_P(D) \text{ para todo } P \in \mathbb{P}(F)\} \cup \{0\}.$$

Este es un espacio vectorial finito dimensional sobre k y $l(D)$ denota su dimensión. El **género** de F/k se define por:

$$g(F) := \text{máx}\{\deg(D) - l(D) + 1 : D \text{ es un divisor de } F/k\}.$$

En [20, Proposición 1.4.14] y [20, Corolario 1.4.14] se demuestra que el género de un cuerpo de funciones es un entero no negativo.

El ejemplo más sencillo de un cuerpo de funciones es el **cuerpo de funciones racionales** $k(x)/k$, donde x es un elemento trascendente sobre k. Este cuerpo de funciones tiene género 0 y una descripción muy particular de sus lugares, la cual daremos a continuación. Cada polinomio irreducible $p(x) \in k[x]$ induce un lugar en $\mathbb{P}(k(x))$ que se denota como $P_{p(x)}$. En este caso $p(x)$ es un elemento primo para $P := P_{p(x)}$ y su correspondiente valuación discreta es $\nu_P(q(x)) = n$, donde $q(x)$ es de la forma $p(x)^n r(x)$ con n un entero, $r(x) = s_1(x)/s_2(x) \in k(x)$ y $s_i(x) \in k[x]$ es un polinomio no divisible por $p(x)$ para $i = 1, 2$. Por otra parte tenemos al lugar infinito, denotado por P_∞. Un elemento primo para P_∞ es $1/x$ y su correspondiente valuación discreta está dada por $\nu_\infty(p_1(x)/p_2(x)) = \deg p_2(x) - \deg p_1(x)$. Además, si P es un lugar de $k(x)/k$ entonces $P = P_{p(x)}$ para algún $p(x) \in k[x]$ irreducible o $P = P_\infty$. Finalmente, $\deg P_{p(x)} = \deg p(x)$ y $\deg P_\infty = 1$. En particular, si k es un cuerpo finito el número de lugares racionales de $k(x)$ es $|k| + 1$.

En adelante supondremos que F'/k' (resp. F/k) es un cuerpo de funciones y que k' (resp. k) es su cuerpo total de constantes. Un cuerpo de funciones F'/k' se dice una **extensión algebraica** (resp. **extensión finita**) de un cuerpo de funciones F/k si F'/F y k'/k son extensiones algebraicas (resp. extensiones finitas) de cuerpos. Nuestro interés a lo largo del trabajo se centra en torres de cuerpos de funciones sobre cuerpos finitos así que supondremos que k es un cuerpo finito.

Ahora mencionaremos algunas definiciones y propiedades importantes de los lugares en una extensión algebraica de cuerpos de funciones F'/k' de F/k. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$. Si $P \subseteq Q$ diremos que Q **cae sobre** P o que Q **está arriba** de P o

que Q **divide** a P o que P es **la restricción** de Q a F y lo denotamos por $Q|P$. En este caso se demuestra que existe un entero positivo $e \geq 1$ tal que para todo $x \in F$ se cumple que

$$\nu_Q(x) = e\nu_P(x).$$

El entero positivo e se conoce como el **índice de ramificación** de Q sobre P y se denota por $e(Q|P)$. También se prueba que para cada lugar $Q \in \mathbb{P}(F')$ existe un único lugar $P \in \mathbb{P}(F)$ tal que Q cae sobre P, concretamente $P = Q \cap F$, y de manera recíproca que para cada lugar P de F existe al menos uno y lo más un número finito de lugares en F' arriba de P.
Se dice que un lugar $P \in \mathbb{P}(F)$ **ramifica** en F'/F si existe un lugar Q de F' arriba de P tal que $e(Q|P) > 1$. En caso contrario decimos que P **no ramifica** en F'/F. Decimos que la extensión F'/F **ramifica** si existe un lugar $P \in \mathbb{P}(F)$ que ramifica y **no ramifica** en caso contrario.
Si Q cae sobre P se prueba que la clase residual F'_Q es una extensión de cuerpos de la clase residual F_P. El grado de F'_Q/F_P, el cual puede ser infinito, se denota por $f(Q|P)$ y es llamado el **grado de inercia** o el **grado relativo** de Q sobre P. En caso de que $f(Q|P) > 1$ decimos que P es **inerte** en F'/F.

El índice de ramificación y el grado de inercia son multiplicativos, esto es, si F''/F' y F'/F son extensiones algebraicas y los lugares $R \in \mathbb{P}(F'')$, $Q \in \mathbb{P}(F')$ y $P \in \mathbb{P}(F)$ son tales que $P \subseteq Q \subseteq R$ entonces

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

El siguiente resultado muestra que el índice de ramificación y el grado de inercia están estrechamente relacionados.

Proposición 1.1. *(**Igualdad fundamental**) Sean F'/k' una extensión finita de F/k, P un lugar de F y $Q_1, \ldots, Q_r$ todos los lugares de F' arriba de P entonces:*

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

Sean F'/k' una extensión finita de F/k y $P \in \mathbb{P}(F)$. Se dice que el lugar P es **totalmente ramificado** en F'/F si existe Q un lugar de F' arriba de P tal que $e(Q|P) = [F' : F]$. La igualdad fundamental implica que Q es el único lugar arriba de P y que $f(Q|P) = 1$. Se dice que P se **descompone completamente** en F'/F si existen exactamente $[F' : F]$ lugares en F' arriba de P. Usando nuevamente la igualdad fundamental vemos que P se descompone completamente en F'/F si y sólo

si $e(Q|P) = f(Q|P) = 1$ para todo lugar Q de F' arriba de P. Ahora veamos la relación que hay entre el grado de los lugares y el grado de inercia en una extensión de cuerpos de funciones finita. Dados $Q \in \mathbb{P}(F')$ y $P \in \mathbb{P}(F)$ con Q arriba de P, se muestra fácilmente que

$$\deg Q = \frac{f(Q|P)\deg P}{[k' : k]}.$$

En particular, si $k = k'$ entonces Q es racional si y sólo si P es racional y $f(Q|P) = 1$. Ahora definimos los conceptos extensión por constantes y divisor conorma que serán necesarios para enunciar la siguiente proposición. Sea F'/k' una extensión algebraica de F/k. Si F' es la composición de los cuerpos F y k' diremos que F' es una **extensión por constantes** de F. Dado un lugar $P \in \mathbb{P}(F)$ se define su **conorma** (respecto a F'/F) como el divisor

$$\mathrm{Con}_{F'/F}(P) := \sum_{Q|P} e(Q|P) \cdot Q.$$

Proposición 1.2. *(**Extensiones por constantes**) Si F'/k' es una extensión por constantes de F/k entonces:*

i. La extensión F'/F no ramifica.

ii. Los cuerpos de funciones F y F' tienen el mismo género.

iii. $\deg(\mathrm{Con}_{F'/F}(D)) = \deg(D)$ *para cualquier divisor D de F.*

iv. Sea $Q \in \mathbb{P}(F')$ un lugar arriba de $P \in \mathbb{P}(F)$. Si $|k| = q$ y $|k'| = q^m$ entonces:

a) $\deg Q = \frac{n}{(n,m)}$, *donde* $n = \deg P$.

b) $f(Q|P) = \frac{m}{(n,m)}$.

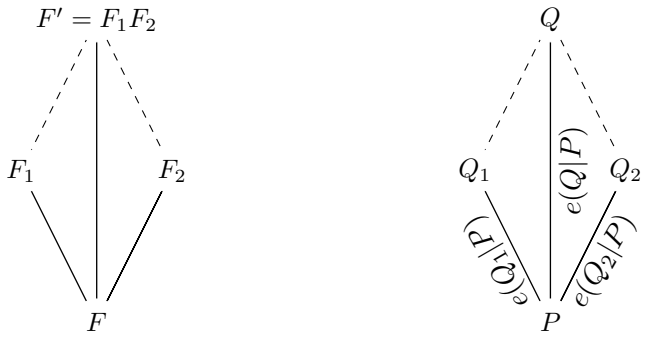
c) Hay exactamente (n, m) lugares en F' arriba de P.

El símbolo (n, m) denota el máximo común divisor entre los enteros n y m.

A continuación describiremos algunos resultados relacionados con la composición de dos cuerpos de funciones.

Proposición 1.3. *(**Lema de Abhyankar**) Sea F'/F una extensión finita y separable tal que F_1, F_2 son cuerpos intermedios y F' es la composición entre F_1 y F_2. Sean $Q \in \mathbb{P}(F')$ un lugar arriba de $P \in \mathbb{P}(F)$ y Q_i la restricción de Q a F_i con $i = 1, 2$. Supongamos que la característica de F,* $\mathrm{Car}\, F$, *no divide a $e(Q_i|P)$ para algún $i = 1, 2$, entonces*

$$e(Q|P) = \frac{e(Q_1|P)e(Q_2|P)}{(e(Q_1|P), e(Q_2|P))}.$$



Gráfica 1.1: Lema de Abhyankar

Corolario 1.4. *Sea F'/F una extensión finita y separable tal que F_1, F_2 son cuerpos intermedios y F' es la composición entre F_1 y F_2. Sean $Q \in \mathbb{P}(F')$ un lugar arriba de $P \in \mathbb{P}(F)$ y Q_i la restricción de Q a F_i con $i = 1, 2$. Si $Q|Q_1$ ramifica en F'/F_1 entonces $Q_2|P$ ramifica en F_2/F.*

Demostración. Supongamos que $Q_2|P$ no ramifica en la extensión F_2/F, es decir, $e(Q_2|P) = 1$, entonces el lema de Abhyankar implica que $e(Q|P) = e(Q_1|P)$. Ahora, de la multiplicatividad del exponente diferente y la igualdad anterior tenemos que

$$e(Q|Q_1)e(Q_1|P) = e(Q|P) = e(Q_1|P),$$

por lo tanto $e(Q|Q_1) = 1$, lo cual es una contradicción.

Proposición 1.5. *Sean F'/F una extensión finita y separable de cuerpos de funciones y E la clausura de Galois de F'/F. Si P es un lugar de F que se descompone completamente en F'/F entonces P se descompone completamente en E/F.*

Proposición 1.6. *Sea F'/F una extensión finita y separable de cuerpos de funciones tal que F_1, F_2 son cuerpos intermedios de F'/F y F' es la composición de F_1 y F_2. Consideremos $P \in \mathbb{P}(F)$.*

i. Si P se descompone completamente en F_1/F entonces cualquier lugar $Q \in \mathbb{P}(F_2)$ arriba de P se descompone completamente en F'/F_2.

ii. Si P se descompone completamente en F_i/F con $i = 1, 2$ entonces P se descompone completamente en F'/F.

Proposición 1.7. *(**Desigualdad de Castelnuovo**) Sean F'/k, F_1/k y F_2/k cuerpos de funciones con k el cuerpo total de constantes de cada uno de ellos. Supongamos que F_1 y F_2 son subcuerpos de F' tales que $F' = F_1F_2$. Entonces el género de*

F' satisface la siguiente desigualdad:

$$g(F') \leq g(F_1)[F' : F_1] + g(F_2)[F' : F_2] + ([F' : F_1] - 1)([F' : F_2] - 1).$$

Un divisor de vital importancia asociado a una extensión finita y separable F'/F es el **diferente** de F'/F que se define como

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

donde $d(Q|P)$ denota a un entero no negativo llamado el **exponente diferente** de Q sobre P (ver [20, Definición 3.4.3]). La siguiente proposición es una herramienta fundamental en el cálculo del género de una extensión finita y separable de cuerpos de funciones y como se puede ver depende del divisor diferente asociado a dicha extensión.

Teorema 1.8. *(**Fórmula del género de Hurwitz**) Sean F'/k' una extensión finita y separable de F/k. Entonces el género $g(F')$ de F'/k' y el género $g(F)$ de F/k satisfacen la siguiente relación:*

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

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

En general, el calculo del exponente diferente no es simple; sin embargo, en muchas ocasiones es suficiente acotarlo. Teniendo en mente esto, a continuación resaltamos una variedad de resultados que involucran al exponente diferente.

Proposición 1.9. *Sean F'/F una extensión finita y separable, un lugar P de F y $Q_1, \ldots, Q_r$ todos los lugares de F' arriba de P. Si $F' = F(y)$, donde y es entero sobre $\mathcal{O}_P$ y φ es el polinomio minimal de y sobre F. Entonces para $1 \leq i \leq r$ se cumple que*

$$d(Q_i|P) \leq \nu_{Q_i}(\varphi'(y)).$$

Proposición 1.10. *Sean F'/F una extensión finita y separable, $Q \in \mathbb{P}(F')$ arriba de $P \in \mathbb{P}(F)$ tal que Q sobre P es totalmente ramificado. Supongamos t es un elemento primo de Q y que φ es el polinomio minimal de t sobre F. Entonces $d(Q|P) = \nu_Q(\varphi'(t))$.*

Proposición 1.11. *(**Teorema del diferente de Dedekind**) Sean F'/F una extensión finita y separable y $P \in \mathbb{P}(F)$. Para todo lugar $Q \in \mathbb{P}(F')$ arriba de P se cumple que:*

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

ii. $d(Q|P) = e(Q|P) - 1$ *si y sólo si* $\operatorname{Car} F$ *no divide a* $e(Q|P)$.

Proposición 1.12. *(**Transitividad del exponente diferente**) Sea* $F_0 \subseteq F_1 \subseteq F_2$ *una torre de extensiones finitas y separables. Dada la sucesión de lugares* $P \subseteq Q \subseteq R$ *donde* $R \in \mathbb{P}(F_2), Q \in \mathbb{P}(F_1)$ *y* $P \in \mathbb{P}(F_0)$ *entonces*

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

Sean F'/F una extensión finita y separable, $P \in \mathbb{P}(F)$, $Q \in \mathbb{P}(F')$ y B un número real positivo. Se dice que P es un lugar de **ramificación salvaje** en F'/F si existe Q arriba de P tal que $e(Q|P)$ es divisible por $p := \operatorname{Car} F$, la característica de F. Diremos que P es de **ramificación moderada** en F'/F si para cada Q arriba de P tal que $e(Q|P) > 1$ se tiene que p no divide a $e(Q|P)$. La extensión F'/F se dice **moderada** o de **ramificación moderada** si ningún lugar $P \in \mathbb{P}(F)$ es salvaje en F'/F. Finalmente, P se dice B-**acotado** en F'/F si para todo lugar Q arriba de P el exponente diferente de $Q|P$ satisface

$$d(Q|P) \leq B(e(Q|P) - 1).$$

La extensión F'/F se dice B-**acotada** si todo lugar $P \in \mathbb{P}(F)$ es B-**acotado** en F'/F. Del Teorema del diferente de Dedekind tenemos que toda extensión moderada es 1-acotada y de la transitividad del exponente diferente se sigue que si F''/F' y F'/F son extensiones B-acotadas entonces F''/F también es B-acotada.

Algunas extensiones 2-acotadas reciben especial atención por las propiedades interesantes que poseen. Antes de mencionarlas recordemos que una p-**extensión** de cuerpos E/F, donde p es un número primo, es una extensión de Galois tal que su grupo de Galois es un p-grupo. Notar que esto implica que el grado de E/F es una potencia de p. Ahora, consideremos los cuerpos de funciones F'/k' y F/k y $p := \operatorname{Car}(F)$. Se dice que F'/k' es una p-**extensión** de F/k si F'/F es una p-extensión de cuerpos.

Sean F'/k' una p-extensión de F/k, P un lugar de F y Q un lugar de F' que cae sobre P. Por los inscisos *a*) y *e*) de [20, Proposición 3.8.5] y la fórmula del diferente de Hilbert [20, Teorema 3.8.7] se sigue que

$$d(Q|P) \geq 2(e(Q|P) - 1).$$

Por lo tanto, una p-extensión F'/k' de F/k es 2-acotada si y sólo si para todo

$Q \in \mathbb{P}(F')$ y $P := Q \cap F$ se cumple

$$d(Q|P) = 2(e(Q|P) - 1). \tag{1.1}$$

La siguiente definición generaliza la noción de p-extensión en cuerpos de funciones. Sea F'/k' una extensión finita de F/k y $p = \operatorname{Car} F$. Diremos que la extensión F'/F es **débilmente ramificada** si existe una sucesión de cuerpos intermedios $\{E_i\}_{i=0}^{n}$ tal que

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = F'$$

y para cada $0 \leq i \leq n-1$ la extensión E_{i+1}/E_i es una p-extensión 2-acotada.
Notemos que en cada extensión intermedia vale la propiedad (1.1), así por la transitividad del exponente diferente, Proposición 1.12, la extensión F'/F también cumple la propiedad (1.1). Además se sigue que el grado de F'/F es una potencia p.

Inmediatamente enunciamos dos proposiciones referentes a extensiones débilmente ramificadas.

Proposición 1.13. *Sea F''/F una extensión de cuerpos de funciones de grado una potencia de $p := \operatorname{Car} F$.*

i. Supongamos que F''/F satisface la propiedad (1.1) y que existe un cuerpo intermedio F' tal que F''/F' y F'/F son extensiones de Galois. Entonces las extensiones F''/F' y F'/F también cumplen la propiedad (1.1). En particular son extensiones débilmente ramificadas.

ii. Recíprocamente, si F' es un cuerpo intermedio tal que F''/F' y F'/F son extensiones débilmente ramificadas entonces F''/F es una extensión débilmente ramificada.

Proposición 1.14. *Sean E_1, E_2 cuerpos intermedios de una extensión finita y separable de cuerpos de funciones F'/F. Si F' es la composición entre E_1 y E_2 y cada extensión E_i/F es débilmente ramificada entonces F'/F es débilmente ramificada.*

El siguiente resultado nos da condiciones suficientes para garantizar la irreducibilidad de ciertos polinomios sobre cuerpos de funciones.

Proposición 1.15. *(**Criterio de Eisenstein**) Sea F/k un cuerpo de funciones y consideremos el polinomio*

$$\varphi(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0 \in F[T].$$

Supongamos que existe un lugar $P \in \mathbb{P}(F)$ tal que se cumple alguna de las condiciones:

E1. $\nu_P(a_n) = 0$, $\nu_P(a_i) \geq \nu_P(a_0) > 0$ *para* $i = 1, \ldots, n-1$ *y* $(n, \nu_P(a_0)) = 1$.

E2. $\nu_P(a_n) = 0$, $\nu_P(a_0) < 0$, $\nu_P(a_i) \geq 0$ *para* $i = 1, \ldots, n-1$ *y* $(n, \nu_P(a_0)) = 1$.

Entonces $\varphi(T)$ es irreducible sobre F. Si $F' = F(y)$ con $\varphi(y) = 0$ entonces F'/F es una extensión de grado n y P es totalmente ramificado en F'/F.

Ahora presentamos los resultados más relevantes de extensiones de tipo Kummer y de tipo Artin-Schreier en cuerpos de funciones.

Teorema 1.16. *(**Teorema de Kummer**) Sean P un lugar de F, $F' = F(y)$ con y entero sobre $\mathcal{O}_P$ y $\varphi \in F[T]$ el polinomio minimal de y sobre F. Sea*

$$\varphi_P := \varphi \mod P = \prod_{i=1}^{r} p_i^{n_i}$$

la descomposición en factores irreducibles de φ_P en $F_P[T]$, donde cada p_i es un polinomio mónico e irreducible en $F_P[T]$ e $i = 1, \ldots, r$; además, $p_i \neq p_j$ para $i \neq j$. Elijamos polinomios mónicos $\varphi_i \in \mathcal{O}_P[T]$ tales que $(\varphi_i)_P := \varphi_i \mod P = p_i$ y $\deg \varphi_i = \deg p_i$. Entonces, existen lugares $Q_1, \ldots, Q_r \in \mathbb{P}(F')$ tales que para $i = 1, \ldots, r$ se cumple que:

$$Q_i | P, \quad \varphi_i(y) \in Q_i \quad y \quad f(Q_i|P) \geq \deg p_i.$$

Si suponemos que $n_i = 1$ para $i = 1, \ldots, r$ entonces existe, para cada $1 \leq i \leq r$, exactamente un lugar $Q_i \in \mathbb{P}(F')$ arriba de P tal que $\varphi_i(y) \in Q_i$, $Q_i|P$ no ramifica y $f(Q_i|P) = \deg p_i$. Además $Q_1, \ldots, Q_r \in \mathbb{P}(F')$ son todos los lugares en F' arriba de P.

Sea F/k un cuerpo de funciones tal que k contiene una raíz n-ésima de la unidad y $(n, \operatorname{Car} k) = 1$. Supongamos que $u \in F$ es un elemento que satisface

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

La extensión definida por

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

es llamada una **extensión de Kummer** de F.

Teorema 1.17. *Sea F'/F una extensión de kummer como la descrita anteriormente. Entonces:*

i. El polinomio $\varphi(T) = T^n - u$ es el polinomio minimal de y sobre F (en particular, φ es irreducible sobre F). La extensión F'/F es de Galois de grado n; su grupo de Galois es cíclico y el grupo de automorfismos está dado por $\sigma(y) = \varepsilon y$, donde $\varepsilon \in k$ es una raíz n-ésima de la unidad.

ii. Sean $P \in \mathbb{P}(F)$ y $P' \in \mathbb{P}(F')$ una extensión de P. Entonces

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

donde $r_P = (n, \nu_P(u)) > 0$.

Sea F/k un cuerpo de funciones y $\operatorname{Car} k = p$. Supongamos que $u \in F$ es un elemento que satisface

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

La extensión definida por

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

es llamada una **extensión de Artin-Schreier** de F.

Teorema 1.18. *Sea F'/F una extensión de Artin-Schreier como la descrita anteriormente. Para cada $P \in \mathbb{P}(F)$ existe $z \in F$ tal que se cumple una y sólo una de las siguientes condiciones (ver [20, Lema 3.7.7])*

S1. $\nu_P(u - (z^p - z)) \geq 0$

S2. $\nu_P(u - (z^p - z)) = -m$ *con* $m > 0$ *y* $(m, p) = 1$.

Definimos al entero m_P como $m_P := -1$ si se satisface la primera condición y como $m_P := m$ si se satisface la segunda. Además, se cumplen las siguientes afirmaciones:

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

ii. P no ramifica en F'/F si y sólo si $m_P = -1$.

iii. P es totalmente ramificado en F'/F si y sólo si $m_P > 0$. Más aún, si $Q \in \mathbb{P}(F')$ es el único lugar arriba P entonces

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

Finalizamos esta sección con algunos resultados clásicos de la teoría de cuerpos. Sean F'/F una extensión finita de Galois, $G = \mathrm{Gal}(F'/F)$ y α un elemento de F'. La **traza** de α de F' a F, se define como

$$\mathrm{Tr}_{F'/F}(\alpha) := \sum_{\sigma \in G} \sigma(\alpha).$$

En particular, si $\mathrm{Gal}(F'/F) = \langle \sigma \rangle$ tenemos que

$$\mathrm{Tr}_{F'/F}(\alpha) = \sigma^{n-1}(\alpha) + \cdots + \sigma(\alpha) + \alpha.$$

Proposición 1.19. *(**versión aditiva del Teorema 90 de Hilbert**) Supongamos que F'/F es una extensión de Galois de grado n tal que $\mathrm{Gal}(F'/F) = \langle \sigma \rangle$. Un elemento $\alpha \in F'$ es de la forma*

$$\alpha = \sigma(\beta) - \beta$$

si sólo si

$$\mathrm{Tr}_{F'/F}(\alpha) = \sigma^{n-1}(\alpha) + \cdots + \sigma(\alpha) + \alpha = 0.$$

Corolario 1.20. *Sean $k = \mathbb{F}_q$, $p = \mathrm{Car}\, k$ y consideremos $\phi(T) = T^p - T - \alpha$ con $\alpha \in \mathbb{F}_q$. Si denotamos por* Tr *la función traza de k a $\mathbb{F}_p$ entonces:*

i. $\phi(T)$ es irreducible sobre k si y sólo si $\mathrm{Tr}(\alpha) \neq 0$.

ii. $\phi(T)$ se descompone completamente sobre k si y sólo si $\mathrm{Tr}(\alpha) = 0$. En este caso, si $\phi(\beta) = 0$ entonces $\{\beta + i : i \in \mathbb{F}_p\}$ es el conjunto de las raíces de $\phi(T)$.

Este criterio de irreducibilidad de trinomios será de gran utilidad en las secciones 2.3 y 2.4.

Sean F y F' dos extensiones finitas de K y supongamos que F y F' son subcuerpos de algún cuerpo E. Diremos que F y F' son cuerpos **disjuntos** o **linealmente disjuntos** sobre K si

$$[FF' : K] = [F : K][F' : K].$$

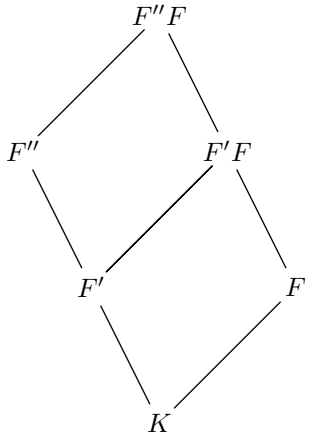
En la siguiente proposición recordamos dos propiedades relacionadas con este concepto.

Proposición 1.21. *Sean F, F' y F'' extensiones finitas de K.*

i. Si al menos una de la extensiones F/K, F'/K es de Galois entonces F y F' son linealmente disjuntos sobre K si y sólo si $K = F \cap F'$.

ii. Si los grados de F/K y F'/K son primos relativos entonces F y F' son linealmente disjuntos sobre K.

iii. Si F'' es una extensión de F' entonces F'' y F son linealmente disjuntos sobre K si y sólo si F' y F son linealmente disjuntos sobre K y F'' y $F'F$ son linealmente disjuntos sobre F'.



Gráfica 1.2: Cuerpos linealmente disjuntos

1.2. Torres de cuerpos de funciones

Una sucesión de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre k se dice una **sucesión no trivial** si $F_i \subsetneq F_{i+1}$ para cada $i \geq 0$. Diremos que la sucesión $\mathcal{F}$ es **recursiva** si existe una sucesión de elementos trascendentes $\{x_i\}_{i=0}^{\infty}$ sobre k y un polinomio en dos variables $H(X,Y) \in k[X,Y]$ tales que $F_0 = k(x_0)$ y

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

donde $H(x_i, x_{i+1}) = 0$ para todo $i \geq 0$. Un **cuerpo de funciones básico** asociado a una sucesión recursiva $\mathcal{F}$ es un cuerpo de funciones $F = k(x,y)$ con x, y elementos trascendentes sobre k que satisfacen $H(x,y) = 0$.

Se dice que una sucesión recursiva $\mathcal{F}$ sobre k es una (a,b)-**sucesión recursiva** o una **sucesión recursiva** de tipo (a,b) si $a(T) = a_1(T)/a_2(T)$ y $b(T) = b_1(T)/b_2(T)$ donde $(a_1(T), a_2(T)) = 1$ y $(b_1(T), b_2(T)) = 1$ y $\mathcal{F}$ está definida por un polinomio de la forma

$$H(X,Y) = a_1(Y)b_2(X) - a_2(Y)b_1(X).$$

En este caso se suele decir que la (a, b)-sucesión recursiva $\mathcal{F}$ está definida por la ecuación con variables separadas

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

Sean $g_1(T)$, $g_2(T) \in k[T]$ polinomios primos relativos. Se define el **grado de la función racional** $g(T) = g_1(T)/g_2(T)$ como

$$\deg(g(T)) = \text{máx}\{\deg g_1(T), \deg g_2(T)\}.$$

Diremos que una (a, b)-sucesión recursiva $\mathcal{F}$ es de grado m si m es el grado de las funciones racionales $a(T), b(T) \in k(T)$.

Una **torre** (o una **torre de cuerpos de funciones**) sobre k es una sucesión no trivial de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ que satisface las siguientes condiciones:

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

ii. El cuerpo total de constantes de F_i es k, para cada $i \geq 0$.

iii. El género $g(F_i)$ de F_i tiende a infinito cuando $i \to \infty$.

Como consecuencia de las condiciones *i.*, *ii.* y la fórmula del género de Hurwitz (Teorema 1.8) podemos reemplazar la condición *iii.* por la condición equivalente

✓ Existe $j \geq 0$ tal que $g(F_j) \geq 2$.

A continuación definiremos los conceptos más relevantes asociados a una torre de cuerpos de funciones sobre un cuerpo finito. En adelante k denotará un cuerpo finito. Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre de cuerpos de funciones sobre k.

i. El **género** de la torre $\mathcal{F}$ sobre F_j se define como

$$\gamma(\mathcal{F}/F_j) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_j]}.$$

ii. La **tasa de descomposición** de la torre $\mathcal{F}$ sobre F_j se define como

$$\nu(\mathcal{F}/F_j) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_j]},$$

donde $N(F_i)$ denota el número de lugares racionales del cuerpo de funciones F_i.

iii. El **límite** de la torre $\mathcal{F}$ se define como

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

Se puede demostrar que los límites anteriores existen y que además se cumple que

$$\gamma(\mathcal{F}/F_j) \in \mathbb{R}^+ \cup \{\infty\} \quad \text{y} \quad \nu(\mathcal{F}/F_j),\, \lambda(\mathcal{F}) \in \mathbb{R}_0^+$$

(ver [20, Lema 7.2.3]). Cuando consideramos el género (resp. la tasa de descomposición) de la torre sobre F_0 lo denotamos como $\gamma(\mathcal{F})$ (resp. $\nu(\mathcal{F})$). De las definiciones de límite de una torre y de función de Ihara (2) tenemos que

$$0 \leq \lambda(\mathcal{F}) \leq A(q) \leq \sqrt{q} - 1.$$

Ahora, una torre de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre k se dice

i. **Asintóticamente buena** si $\lambda(\mathcal{F}) > 0$.

ii. **Asintóticamente mala** si $\lambda(\mathcal{F}) = 0$.

iii. **Asintóticamente óptima** si $\lambda(\mathcal{F}) = \sqrt{q} - 1$.

Es claro que $\mathcal{F}$ es asintóticamente buena si y sólo si $\nu(\mathcal{F}) > 0$ y $\gamma(\mathcal{F}) < \infty$.

A continuación introducimos un espacio de vital importancia en el estudio del género de una torre.

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre de cuerpos de funciones sobre k. Diremos que un lugar $P \in \mathbb{P}(F_j)$ **ramifica** en la torre $\mathcal{F}$ si ramifica en F_i/F_j para algún $i > j$. Si un lugar $P \in \mathbb{P}(F_0)$ es totalmente ramificado en F_i/F_0 para cada $i \geq 1$ decimos que P es **totalmente ramificado** en la torre $\mathcal{F}$. Se dice que la torre $\mathcal{F}$ es **salvaje** si existe un lugar $P \in \mathbb{P}(F_0)$ y un índice $i \geq 1$ tal que P es salvaje en la extensión F_i/F_0. En caso contrario se dice **moderada**.
Definimos el **espacio de ramificación** de la torre $\mathcal{F}$ sobre F_j como el conjunto

$$\mathcal{R}(\mathcal{F}/F_j) = \{P \in \mathbb{P}(F_j) : P \text{ ramifica en } \mathcal{F}\}.$$

Si $\mathcal{R}(\mathcal{F}/F_j)$ es un conjunto finito definimos el **divisor ramificación** de $\mathcal{F}$ como

$$R(\mathcal{F}/F_j) = \sum_{P\in\mathcal{R}(\mathcal{F}/F_j)} P.$$

Cuando consideremos a $\mathcal{F}$ sobre F_0 simplemente escribiremos $\mathcal{R}(\mathcal{F})$ y $R(\mathcal{F})$ para el espacio de ramificación y su grado, respectivamente. Una torre de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ se dice B-**acotada** (resp. **débilmente ramificada**) si para cada $i \geq 1$ la extensión F_i/F_0 es B-acotada (resp. débilmente ramificada). Como consecuencia de la transitividad del exponente diferente, Proposición 1.12, tenemos el siguiente resultado: si $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre y cada extensión F_{i+1}/F_i es B-acotada entonces $\mathcal{F}$ es una torre B-acotada.

La siguiente proposición resalta la importancia del espacio de ramificación de una torre.

Teorema 1.22. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre B-acotada con espacio de ramificación finito sobre F_j. Entonces la torre tiene género finito, específicamente,*

$$\gamma(\mathcal{F}) \leq \frac{g(F_j) - 1 + \frac{B}{2} \deg R(\mathcal{F}/F_j)}{[F_j : F_0]}.$$

A continuación probaremos un resultado que es de utilidad en el estudio del género de cierto tipo de torres recursivas.

Corolario 1.23. *Sean $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre de cuerpos de funciones recursiva sobre k tal que cada F_{i+1}/F_i es una p-extensión y $F = k(x, y)$ el cuerpo de funciones básico asociado a $\mathcal{F}$. Si la extensión $F/k(y)$ es débilmente ramificada entonces la torre $\mathcal{F}$ es débilmente ramificada. Además $\mathcal{F}$ tiene género finito si $\mathcal{F}$ tiene espacio de ramificación finito.*

Demostración. Supongamos que F_i/F_0 es una extensión débilmente ramificada y probemos que F_{i+1}/F_0 también lo es. Como $\mathcal{F}$ es una torre recursiva de cuerpos de funciones entonces existe una sucesión de elementos trascendentes $\{x_i\}_{i=0}^{\infty}$ sobre k tal que $F_0 = k(x_0)$ y $F_{i+1} = F_i(x_{i+1}) = k(x_0, \ldots, x_{i+1})$ para $i \geq 0$. Considerando el homomorfismo que envía $x_j \to x_{j+1}$, con $j = 0, \ldots, i$, tenemos que los cuerpos F_i y $k(x_1, ..., x_{i+1})$ son k-isomorfos, luego $k(x_1, \ldots, x_i, x_{i+1})/k(x_1)$ es una extensión débilmente ramificada. Dado que F_{i+1} es la composición de los cuerpos $F_1 = k(x_0, x_1)$ y $k(x_1, \ldots, x_i, x_{i+1})$ y la extensión $F_1/k(x_1)$ es débilmente ramificada por hipótesis, entonces la Proposición 1.14 garantiza que la extensión $F_{i+1}/k(x_1)$ es débilmente ramificada; este hecho y la hipótesis F_{i+1}/F_i es una p-extensión implican que

$$d(Q|P) = 2(e(Q|P) - 1)$$

para todo $Q \in \mathbb{P}(F_{i+1})$ y $P = Q \cap F_i$, es decir, F_{i+1}/F_i es una extensión débilmente ramificada. Por lo tanto, por la Proposición 1.13 la extensión F_{i+1}/F_0 es débilmente

ramificada, como se quería probar. En particular, tenemos que $\mathcal{F}$ es una torre 2-acotada, luego la segunda afirmación se sigue directamente del Teorema 1.22. □

Ahora introducimos un espacio que es útil al momento de estudiar la tasa de descomposición de una torre $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre k. Sea $j \geq 0$, diremos que un lugar $P \in \mathbb{P}(F_j)$ **se descompone completamente** en la torre $\mathcal{F}$ si P se descompone completamente en la extensión F_i/F_j para cada $i > j$. Además, definimos el **espacio de descomposición** de la torre $\mathcal{F}$ sobre F_j como el conjunto

$$\mathcal{S}_j(\mathcal{F}) := \{P \in \mathbb{P}(F_j) : P \text{ es racional y se descompone completamente en } \mathcal{F}\}.$$

Al espacio de descomposición $\mathcal{S}_0(\mathcal{F})$ de $\mathcal{F}$ lo denotaremos simplemente por $\mathcal{S}(\mathcal{F})$.

Teorema 1.24. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre sobre k. Supongamos que el conjunto $\mathcal{S}_j(\mathcal{F})$ es no vacío para algún $j \geq 0$. Entonces $\mathcal{F}$ tiene tasa de descomposición positiva, más aún,*

$$\nu(\mathcal{F}) \geq \frac{|\mathcal{S}_j(\mathcal{F})|}{[F_j : F_0]}.$$

Corolario 1.25. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre sobre k. Supongamos que $\mathcal{S}_j(\mathcal{F})$ es un conjunto no vacío para algún $j \geq 0$, $\mathcal{R}(\mathcal{F}/F_j)$ es un conjunto finito y $\mathcal{F}$ es una torre B-acotada entonces $\mathcal{F}$ es una torre asintóticamente buena, aún más, su límite $\lambda(\mathcal{F})$ satisface*

$$\lambda(\mathcal{F}) \geq \frac{2|\mathcal{S}_j(\mathcal{F})|}{2g(F_j) - 2 + B \deg R(\mathcal{F}/F_j)}.$$

Demostración. Como $\mathcal{S}_j(\mathcal{F})$ es un conjunto no vacío el Teorema 1.24 asegura que $\mathcal{F}$ tiene tasa de descomposición positiva y que $\nu(\mathcal{F})$ satisface

$$\nu(\mathcal{F}) \geq \frac{|\mathcal{S}_j(\mathcal{F})|}{[F_j : F_0]}.$$

Por otra parte, dado que $\mathcal{R}(\mathcal{F}/F_j)$ es un conjunto finito y $\mathcal{F}$ es una torre B-acotada entonces el Teorema 1.22 afirma que $\mathcal{F}$ es una torre de género finito y que $\gamma(\mathcal{F})$ satisface

$$\gamma(\mathcal{F}) \leq \frac{g(F_j) - 1 + \frac{B}{2} \deg \mathcal{R}(\mathcal{F}/F_j)}{[F_j : F_0]}.$$

Por lo tanto, $\mathcal{F}$ es una torre asintóticamente buena y $\lambda(\mathcal{F})$ satisface la desigualdad

$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} \geq \frac{2|\mathcal{S}_j(\mathcal{F})|}{2g(F_j) - 2 + B \deg R(\mathcal{F}/F_j)}.$$

□

A partir de una torre $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre k podemos definir una torre $\mathcal{F}'$ que es muy "similar" a $\mathcal{F}$, por ejemplo, tiene el mismo género de $\mathcal{F}$. Veamos esto con detalle: sea k' una extensión algebraica de k. Para todo $i \geq 0$ consideramos a F_i' como la composición de los cuerpos F_i y k', esto es, $F_i' = F_i k'$. La sucesión $\mathcal{F}' = \{F_i'\}_{i=0}^{\infty}$ es llamada una **extensión por constantes** de $\mathcal{F}$ por k'. Se puede probar para todo $i \geq 0$ que $[F_{i+1}' : F_i'] = [F_{i+1} : F_i]$, k' es el cuerpo total de constantes de F_i' y $g(F_i') = g(F_i)$. Por lo tanto $\mathcal{F}'$ es una torre sobre k' y tiene el mismo género de $\mathcal{F}$. Además un lugar $P \in \mathbb{P}(F_i)$ ramifica en F_{i+1}/F_i si y sólo si un lugar $Q \in \mathbb{P}(F_i')$ arriba de P ramifica en F_{i+1}'/F_i', luego

$$\mathcal{R}(\mathcal{F}') = \{P' \in \mathbb{P}(F_0') : P' \cap F_0 \in \mathcal{R}(\mathcal{F})\}.$$

Notemos que $\mathcal{R}(\mathcal{F})$ es finito si y sólo si $\mathcal{R}(\mathcal{F}')$ es finito. En este caso tenemos que

$$\mathrm{Con}_{F_0'/F_0}(R(\mathcal{F})) = \sum_{P \in \mathcal{R}(\mathcal{F})} \mathrm{Con}_{F_0'/F_0}(P) = \sum_{P \in \mathcal{R}(\mathcal{F})} \sum_{P'|P} P' = \sum_{P' \in \mathcal{R}(\mathcal{F}')} P' = R(\mathcal{F}'),$$

entonces por la Proposición 1.2 *iii* se sigue que

$$\deg(R(\mathcal{F}')) = \deg(\mathrm{Con}_{F_0'/F_0}(R(\mathcal{F}))) = \deg(R(\mathcal{F})).$$

Por lo tanto la cota dada en el Teorema 1.22 se mantiene independientemente de cuál sea el cuerpo de constantes en que se considere la torre. A causa de los resultados anteriores decimos que las torres, al igual que los cuerpos de funciones, son invariantes bajo extensiones por constantes y es frecuente trabajar sobre una extensión algebraica "adecuada" de k cuando se trata de estimar el género de una torre sobre k. En caso de que k' sea un extensión finita de k, por ejemplo, $k = \mathbb{F}_q$ y $k' = \mathbb{F}_{q^n}$ para algún n entero positivo mayor que uno entonces

$$\nu(\mathcal{F}') \geq \nu(\mathcal{F}) \qquad \text{y} \qquad \lambda(\mathcal{F}') \geq \lambda(\mathcal{F}).$$

En efecto, si P es un lugar racional de F_i por la Proposición 1.2 existe exactamente un lugar racional Q en F_i' arriba de P, luego $N(F_i') \geq N(F_i)$ para cada $i \geq 0$ y concluimos que

$$\nu(\mathcal{F}') = \lim_{i \to \infty} \frac{\nu(\mathcal{F}')}{[F_i' : F_0']} \geq \lim_{i \to \infty} \frac{\nu(\mathcal{F})}{[F_i : F_0]} = \nu(\mathcal{F}).$$

Podemos resumir los resultados anteriores como sigue:

Proposición 1.26. *Sean $\mathcal{F}$ una torre sobre $\mathbb{F}_q$ y $\mathcal{F}'$ la extensión por constantes de*

$\mathcal{F}$ por $\mathbb{F}_{q^n}$. Entonces:

i. El género, la tasa de descomposición y el límite de $\mathcal{F}$ y $\mathcal{F}'$ se relacionan así:

$$\gamma(\mathcal{F}') = \gamma(\mathcal{F}), \qquad \nu(\mathcal{F}') \geq \nu(\mathcal{F}) \qquad y \qquad \lambda(\mathcal{F}') \geq \lambda(\mathcal{F}).$$

ii. Se cumple que $\mathcal{R}(\mathcal{F}') = \{P' \in \mathbb{P}(F_0') : P' \cap F_0 \in \mathcal{R}(\mathcal{F})\}$ donde $\mathcal{R}(\mathcal{F})$ y $\mathcal{R}(\mathcal{F}')$ son los espacios de ramificación de $\mathcal{F}$ y $\mathcal{F}'$ respectivamente.

iii. Los espacios de descomposición $\mathcal{S}_j(\mathcal{F})$ y $\mathcal{S}_j(\mathcal{F}')$ satisfacen que

$$\mathcal{S}_j(\mathcal{F}') \supseteq \{Q \in \mathbb{P}(F_j') : Q \cap F_j \in \mathcal{S}_j(\mathcal{F})\} \qquad y \qquad |\mathcal{S}_j(\mathcal{F}')| \geq |\mathcal{S}_j(\mathcal{F})|.$$

La proposición anterior implica que si una torre $\mathcal{F}$ tiene espacio de descomposición no vacío sobre $\mathbb{F}_q$ entonces tiene tasa de descomposición positiva sobre $\mathbb{F}_{q^n}$ para todo n entero positivo.

En las siguientes secciones denotaremos por $\mathcal{F}$ sobre $\mathbb{F}_{q^n}$ en vez de $\mathcal{F}'$ sobre $\mathbb{F}_{q^n}$ a la extensión por constantes obtenida de la torre $\mathcal{F}$ sobre $\mathbb{F}_q$ y la extensión $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$.

CAPÍTULO 2
UN PROBLEMA DE BEELEN, GARCIA Y STICHTENOTH EN UNA TORRE DE TIPO ARTIN-SCHREIER SOBRE $\mathbb{F}_{2^s}$.

En este capítulo estudiaremos el comportamiento asintótico de la torre de cuerpos de funciones $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ definida de forma recursiva por la ecuación de tipo Artin-Schreier

$$y^2 + y = \frac{x}{x^2 + x + 1} \tag{2.1}$$

sobre $\mathbb{F}_{2^s}$ donde s es un entero positivo cualquiera. Para ello dividimos el capítulo en cinco secciones. En la primera sección probamos que en cada paso de la sucesión $\mathcal{H}$ existe un lugar totalmente ramificado lo que garantiza que $\mathcal{H}$ es una torre. También demostramos que $\mathcal{H}$ es una torre salvaje con género finito; para ello vemos que la torre tiene espacio de ramificación finito y que es débilmente ramificada; esta última condición es necesaria para concluir que la torre tiene género finito, pues la finitud del espacio de ramificación en torres salvajes no asegura la finitud del género. En la segunda sección estudiamos la tasa de descomposición de la torre sobre $\mathbb{F}_4$. Se definen los conceptos de elementos de tipo 1 y 2 y de condición de ramificación para una cierta sucesión de lugares. También se prueban tres lemas que implican que el espacio de descomposición de la torre es no vacío. En particular se deduce que la torre es asintóticamente buena sobre $\mathbb{F}_{2^s}$ para todo s entero positivo par. De esta manera, se responde a la pregunta planteada por Beelen, García y Stichtenoth en relación con el comportamiento asintótico de esta torre. En la cuarta sección calculamos de forma precisa el número de lugares racionales y el género de cada paso de la torre sobre $\mathbb{F}_4$ y concluimos que es una torre óptima. En la quinta y

última sección mostramos que la tasa de descomposición de la torre sobre $\mathbb{F}_{2^s}$ para s entero positivo impar es cero. Este resultado se obtiene como consecuencia de que el número de lugares racionales de cada cuerpo de funciones permanece constante después del primer paso de la torre.

Iniciamos este capítulo con dos resultados claves y la siguiente notación. Sea $\mathbb{F}_{2^s}$ un cuerpo finito con 2^s elementos. Si s es par, existe $\alpha \in \mathbb{F}_{2^s}$ que satisface $\alpha^2+\alpha+1 = 0$. El conjunto $\{0, 1, \alpha, \alpha + 1\} \subseteq \mathbb{F}_{2^s}$ es el cuerpo finito con cuatro elementos y lo denotaremos por $K := \mathbb{F}_4$.

Lema 2.1. *Consideremos la ecuación*

$$y^2 + y = f(x) := \frac{x}{x^2 + x + 1}.$$

Entonces

$$f(y) + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1} = y + \frac{1}{x^2 + x + 1} + \frac{1}{x+1}.$$

Demostración.

$$f(y) + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1} = \frac{y}{y^2 + y + 1} + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1}$$

$$= \frac{y}{f(x)+1} + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1}$$

$$= y\frac{x^2 + x + 1}{(x+1)^2} + \left(\frac{y+1}{x+1}\right)^2 + \frac{y}{x+1} + \frac{1}{x+1}$$

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

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

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

□

Proposición 2.2. *Sean F/K un cuerpo de funciones, x un elemento de $F \setminus K$ y K el cuerpo total de constantes de F. Supongamos que F'/F es una extensión de*

Artin-Schreier de grado dos tal que $F' = F(y)$ *y*

$$y^2 + y = f(x) := \frac{x}{x^2 + x + 1}.$$

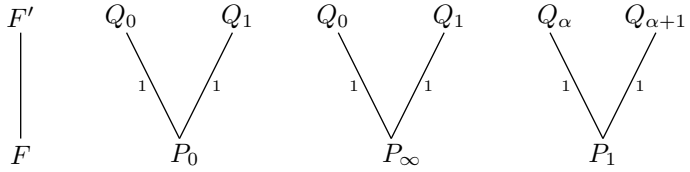
Entonces cualquier cero P_0 *y cualquier polo* P_∞ *de* x *en* F*, se descomponen completamente en* F'/F *en un cero* Q_0 *de* y *y un cero* Q_1 *de* $y + 1$*. Cualquier cero* P_1 *de* $x + 1$ *en* F *se descompone completamente en* F'/F *en un cero* Q_α *de* $y + \alpha$ *y un cero* $Q_{\alpha+1}$ *de* $y + \alpha + 1$*. Además,*

$$\nu_{Q_i}(y + i) = \nu_{P_0}(x) = -\nu_{P_\infty}(x),$$

con $i = 0, 1$ *y*

$$\nu_{Q_\beta}(y + \beta) = 2\nu_{P_1}(x + 1),$$

con $\beta \in \{\alpha, \alpha + 1\}$.



Gráfica 2.1: Decomposición de algunos ceros y polos de $K(x)$

Demostración. Observemos que el polinomio $\varphi(T) := T^2 + T + f(x)$ define la extensión F'/F. Si el lugar $P \in \mathbb{P}(F)$ es un cero o polo de x entonces P es un cero de $f(x)$, luego $\varphi(T)$ es entero sobre $\mathcal{O}_P$ y la reducción módulo P de $\varphi(T)$ es el polinomio

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

Luego el Teorema de Kummer (Teorema 1.16) garantiza que en F' existen un cero Q_0 de y y un cero Q_1 de $y + 1$ arriba de P. Por otra parte, como y satisface la ecuación (2.1) tenemos que

$$\nu_{Q_i}(y + i) = \nu_{P_0}(x) \qquad \text{y} \qquad \nu_{Q_i}(y + i) = -\nu_{P_\infty}(x).$$

Sea P_1 un cero de $x + 1$ en F. Entonces $\nu_{P_1}(x + 1) > 0$ y $\nu_{P_1}(x) = 0$ así que $\nu_{P_1}(f(x)) = 0$ y la clase residual $x(P_1)$ es 1. Luego

$$\varphi_{P_1}(T) = T^2 + T + 1 = (T + \alpha)(T + \alpha + 1),$$

y de nuevo el Teorema de Kummer asegura la existencia en F' de un cero Q_α de $y+\alpha$ y un cero $Q_{\alpha+1}$ de $y+\alpha+1$ arriba de P_1. Ahora, reescribiendo la ecuación (2.1) como

$$y^2+y+1=\frac{(x+1)^2}{x^2+x+1}, \tag{2.2}$$

vemos para Q_β arriba de P_1 que $\nu_{Q_\beta}(y+\beta)=2\nu_{P_1}(x+1)$ como se quería probar. □

2.1. El género de la torre

El objetivo de esta sección es probar que la sucesión de cuerpos de funciones $\mathcal{H}$ es una torre de género finito sobre K.
En el siguiente lema y en la gráfica 2.2 describiremos el comportamiento de la ramificación del cuerpo de funciones básico $F=K(x,y)$ asociado a la torre $\mathcal{H}$.

Lema 2.3. *Sean $F=K(x,y)$ el cuerpo de funciones básico asociado a la torre $\mathcal{H}$ y $\beta\in\{\alpha,\alpha+1\}$. Entonces $F/K(x)$ es una extensión de Artin-Schreier de grado 2 y K es el cuerpo total de constantes de F. Además, se cumplen las siguientes propiedades:*

i. El lugar P_β de $K(x)$ es totalmente ramificado en F y tiene exponente diferente 2. Además, si $Q\in\mathbb{P}(F)$ cae sobre P_β, entonces $Q\cap K(y)=R_\infty$.

ii. El lugar P_0 de $K(x)$ se descompone completamente en F. Además, si $Q\in\mathbb{P}(F)$ cae sobre P_0, entonces $Q\cap K(y)$ es igual a R_0 o R_1.

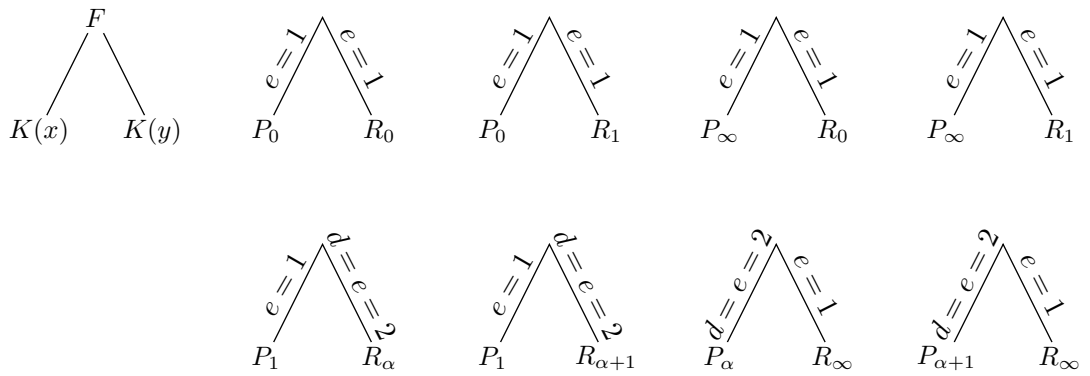
iii. El lugar P_∞ de $K(x)$ se descompone completamente en F. Además, si $Q\in\mathbb{P}(F)$ cae sobre P_∞ entonces $Q\cap K(y)$ es igual a R_0 o R_1.

iv. El lugar P_1 de $K(x)$ se descompone completamente en F. Además, si $Q\in\mathbb{P}(F)$ cae sobre P_1 entonces $Q\cap K(y)$ es igual a R_α o $R_{\alpha+1}$.

v. El lugar R_β de $K(y)$ es totalmente ramificado en F y tiene exponente diferente 2.

vi. Si P es un lugar de $K(x)$ (resp. $K(y)$) diferente de P_β (resp. R_β) entonces P no ramifica en F. Por lo tanto las extensiones $F/K(x)$ y $F/K(y)$ son débilmente ramificadas.

Demostración. Consideremos el lugar $P_\beta\in\mathbb{P}(K(x))$. Dado que P_β es un cero simple de x^2+x+1 entonces $\nu_{P_\beta}(f(x))=-1$, luego por el criterio de Eisenstein 1.15 tenemos que el polinomio $\varphi(T):=T^2+T+f(x)$ es irreducible sobre $K(x)$ y P_β es totalmente



Gráfica 2.2: Ramificación en $F/K(x)$ y $F/K(y)$

ramificado en $F/K(x)$, por lo tanto, $F/K(x)$ es una extensión de Artin-Schreier de grado dos y K es el cuerpo total de constantes de F. Si Q es el único lugar de F arriba de P_β entonces Q es un polo simple de y ya que

$$2\nu_Q(y) = \nu_Q(y^2 + y) = e(Q|P_\beta)\nu_{P_\beta}(f(x)) = -2.$$

Para finalizar la prueba de i calculamos el exponente diferente de $Q|P_\beta$. Si denotamos por $m_\beta := -\nu_{P_\beta}(f(x)) = 1$ tenemos, por el Teorema 1.18, que

$$d(Q|P_\beta) = (2-1)(m_{P_\beta} + 1) = 2.$$

Los incisos ii, iii y iv son una consecuencia directa de la Proposición 2.2.

Ahora probaremos la afirmación v. Sean Q un lugar de F arriba de R_β y S la restricción de Q a $K(x)$, es decir, $S := Q \cap K(x)$. De la igualdad (2.2) obtenemos

$$\nu_Q(y^2 + y + 1) = \nu_Q\left(\frac{(x+1)^2}{x^2 + x + 1}\right).$$

Dado que R_β es un cero simple de $y^2 + y + 1$ tenemos que $\nu_Q(y^2 + y + 1) = e(Q|R_\beta)$. Por otra parte, si consideramos $h(x) := x^2 + x + 1$ se sigue que

$$\nu_Q((x+1)^2/h(x)) = 2e(Q|S)\nu_S((x+1)/h(x)).$$

De todo lo anterior tenemos que

$$2e(Q|S)\nu_S((x+1)/h(x)) = e(Q|R_\beta),$$

por lo tanto, los índices de ramificación son $e(Q|R_\beta) = 2$, $e(Q|S) = 1$ y la valuación

satisface

$$1 = \nu_S((x+1)/h(x)) = \nu_S(x+1) - \nu_S(h(x)).$$

De la última igualdad se deduce que $S = P_\infty$ o $S = P_1$, pero el caso $S = P_\infty$ contradice el inciso iii, por lo tanto, $S = P_1$. En particular R_β es totalmente ramificado en $F/K(x)$ y $x+1$ es un elemento primo para Q. Notemos que $F = K(x+1, y)$ y que la ecuación (2.1) se puede escribir como

$$(x+1)^2 + (x+1)\left(\frac{y^2+y+1}{y^2+y}\right) + \frac{y^2+y+1}{y^2+y} = 0.$$

Luego

$$\phi(T) = T^2 + \left(\frac{y^2+y+1}{y^2+y}\right)T + \frac{y^2+y+1}{y^2+y} \tag{2.3}$$

es el polinomio minimal de $x+1$ sobre $K(y)$ tomando $P = R_\beta$ y aplicando el criterio de Eisenstein (Proposición 1.15). Por lo tanto, la Proposición 1.10 afirma que

$$d(Q|R_\beta) = \nu_Q(\phi'(x+1)) = \nu_Q\left(\frac{y^2+y+1}{y^2+y}\right) = 2.$$

Finalmente, probaremos vi. Por i (resp. v) sabemos que el lugar P_β de $K(x)$ (resp. R_β de $K(y)$) es totalmente ramificado en $F/K(x)$. Sea P un lugar de $K(x)$ diferente de P_β, entonces $\nu_P(f(x)) \geq 0$, luego por el Teorema 1.18 tenemos que P no ramifica en F. Ahora consideremos un lugar R de $K(y)$ diferente de R_δ con $\delta \in \{0, 1, \alpha, \alpha+1\}$ y Q un lugar de F arriba de R. Como la extensión $F/K(y)$ está definida por el polinomio $\phi(T)$, el cual es entero sobre $\mathcal{O}_R$, entonces por la Proposición 1.9 tenemos que

$$d(Q|R) \leq \nu_Q(\varphi'(x+1)) = \nu_Q\left(\frac{y^2+y+1}{y^2+y}\right) = e(Q|R)\nu_R\left(\frac{y^2+y+1}{y^2+y}\right) = 0,$$

por lo tanto, R no ramifica en $F/K(x)$. Nos resta mostrar que $R = R_i$, con $i = 0, 1$, no ramifica en F. Sean Q un lugar de F que cae sobre R y $P = Q \cap K(x)$, entonces de ii y iii tenemos que $P = P_0$ o $P = P_\infty$; además, deben existir exactamente dos lugares Q distintos arriba de R, pues en caso contrario tendríamos $P_0 = Q \cap K(x) = P_\infty$ lo cual es una contradicción. Concluimos que R no ramifica en $F/K(y)$ puesto que se descompone completamente en $F/K(y)$. □

Proposición 2.4. *La sucesión de cuerpos de funciones $\mathcal{H}$ es una torre sobre K.*

Demostración. Denotaremos por Q_0^i (resp. Q_1^i) a un cero de $x_i \in F_i$ (resp. $x_i+1 \in F_i$) y por Q_β^i a un cero de $x_i + \beta \in F_i$ con $\beta \in \{\alpha, \alpha+1\}$. Probaremos para cada $i \geq 0$

que la extensión F_{i+1}/F_i es una extensión de Artin-Schreier de grado dos, que existe un lugar Q_β^i totalmente ramificado de F_{i+1}/F_i y que el cuerpo total de constantes de F_{i+1} es K. El resultado es válido para $i = 0$ ya que del Lema 2.3 se sigue que F_1/F_0 es una extensión de grado 2, Q_β^0 es totalmente ramificado y K es el cuerpo total de constantes de F_1. Además, por la Proposición 2.2 arriba de Q_0^0 (resp. Q_∞^0) hay dos ceros simples Q_j^1 con $j = 0, 1$ y arriba de Q_1^0 hay dos ceros dobles, a saber Q_β^1 con $\beta \in \{\alpha, \alpha+1\}$. Recordemos que cada extensión F_{i+1}/F_i está definida por la ecuación

$$x_{i+1}^2 + x_{i+1} = f(x_i) := \frac{x_i^2}{x_i^2 + x_i + 1}.$$

Consideremos el elemento $u_i := (x_i + 1)/(x_{i-1} + 1) \in F_i$ y el polinomio

$$\phi_{i+1}(T) = (T + u_i)^2 + (T + u_i) + f(x_i) = T^2 + T + f(x_i) + u_i^2 + u_i \in F_i[T].$$

Para cada $i \geq 1$ tenemos que $F_{i+1} = F_i(x_{i+1}) = F_i(x_{i+1} + u_i)$, además $\phi_{i+1}(T)$ es separable y sus dos raíces $x_{i+1}+u_i, x_{i+1}+u_i+1$ pertenecen a F_{i+1}, luego para probar que F_{i+1}/F_i es una extensión de Artin-Schreier de grado 2 es suficiente mostrar que el polinomio $\phi_{i+1}(T)$ es irreducible sobre F_i. Procedamos por inducción. En efecto, para $i = 1$ el Lema 2.1 implica que

$$f(x_1) + u_1^2 + u_1 = x_1 + \frac{1}{x_0^2 + x_0 + 1} + \frac{1}{x_0 + 1},$$

luego $\nu_{Q_\beta^1}(f(x_1) + u_1^2 + u_1) = \nu_{Q_1^0}(1/(x_0 + 1)) = -1$ y por el criterio de Eisenstein (Proposición 1.15) tenemos que el polinomio $\phi_2(T)$ es irreducible sobre F_1, que Q_β^1 es un lugar totalmente ramificado en F_2/F_1 y que el cuerpo total de constantes de F_2 es K. Además de la Proposición 2.2 se sigue que en F_2 arriba del cero simple Q_0^1 existen dos ceros simples Q_j^2 con $j = 0, 1$ y arriba de Q_1^1 hay dos ceros dobles denotados por Q_β^1 con $\beta \in \{\alpha, \alpha + 1\}$. Ahora supongamos que F_i/F_{i-1} es una extensión de grado 2, que el cuerpo de constantes de F_{i+1} es K y que Q_1^{i-1} (resp. Q_0^{i-1}) es un cero simple de $x_{i-1} + 1$ (resp. x_{i-1}). La Proposición 2.2 garantiza que cada uno de dichos lugares se descompone completamente en F_i/F_{i-1} en dos ceros dobles Q_β^i con $\beta \in \{\alpha, \alpha+1\}$. (resp. dos ceros simples Q_0^i y Q_1^i). Nuevamente, el Lema 2.1 implica que

$$f(x_i) + u_i^2 + u_i = x_i + \frac{1}{x_{i-1}^2 + x_{i-1} + 1} + \frac{1}{x_{i-1} + 1},$$

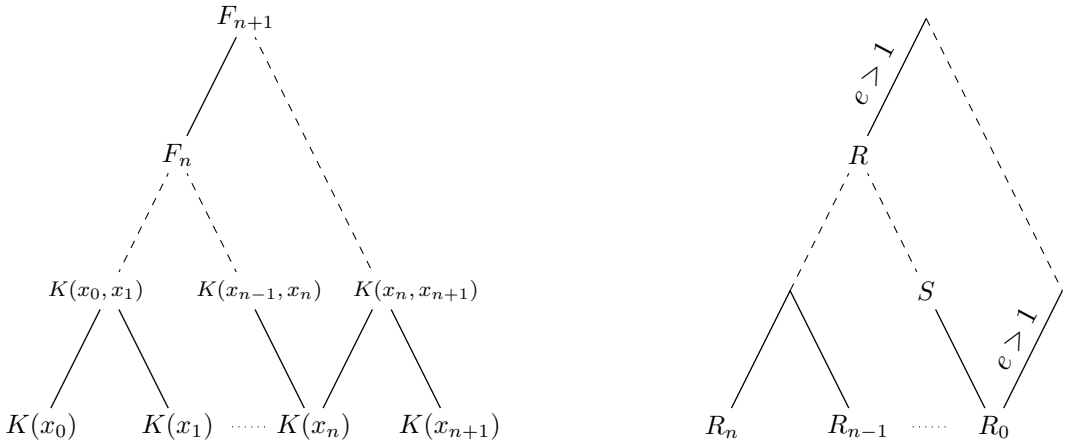
luego $\nu_{Q_\beta^i}(f(x_i) + u_i^2 + u_i) = \nu_{Q_1^{i-1}}(1/(x_{i-1} + 1)) = -1$ y por el criterio de Eisenstein tenemos que el polinomio $\phi_{i+1}(T)$ es irreducible sobre F_i, que Q_β^i es un lugar totalmente ramificado en F_{i+1}/F_i y que el cuerpo total de constantes de F_{i+1} es

K. Finalmente de la Proposición 2.2 se sigue que en F_{i+1} existen dos ceros simples Q_j^{i+1}, con $j = 0, 1$, arriba del cero simple Q_0^i y que existen dos ceros dobles Q_β^{i+1}, con $\beta \in \{\alpha, \alpha+1\}$, arriba de Q_1^i. Para demostrar que la sucesión de géneros $g(F_i)$ tiende a infinito cuando i tiende a infinito es suficiente ver existe un cuerpo de funciones de $\mathcal{H}$ con género mayor a uno. Usando la fómula del género de Hurtwitz 1.8 y que todo lugares de tipo Q_β^i es totalmente ramificados en F_{i+1}/F_i para $i = 0, 1$ se prueba que $g(F_1) = 1$ y $g(F_2) = 3$. Por la tanto $\mathcal{H}$ es una torre sobre K. □

Proposición 2.5. *El espacio de ramificación $\mathcal{R}(\mathcal{H})$ de la torre $\mathcal{H}$ sobre K es finito. Más precisamente,*

$$\mathcal{R}(\mathcal{H}) \subseteq \{P_0,\, P_1,\, P_\alpha,\, P_{\alpha+1},\, P_\infty\}.$$

Demostración. Sea $P \in \mathcal{R}(\mathcal{H})$ entonces existe un entero positivo n y un lugar R de F_n arriba de P que ramifica en la extensión F_{n+1}/F_n. Para $i = 0, \ldots, n$ denotamos por R_i a la restricción de R a $K(x_{n-i})$ y por S a la restricción de R a $K(x_{n-1}, x_n)$, es decir, $R_i := R \cap K(x_{n-i})$ y $S := R \cap K(x_{n-1}, x_n)$, respectivamente. Dado que F_{n+1} es la composición de los cuerpos F_n y $K(x_{n+1}, x_n)$ y $R \in \mathbb{P}(F_n)$ ramifica en F_{n+1}/F_n entonces el Corolario 1.4 garantiza que R_0 ramifica en $K(x_{n+1}, x_n)$ (ver gráfica 2.3); además, el Lema 2.3 implica que R_0 es un cero de $x_n + \alpha$ o $x_n + \alpha + 1$, $e(S|R_0) = 2$ y que R cae sobre un cero de $x_{n-1} + 1$, esto es, $R_1 = S \cap K(x_{n-1})$ es un cero de $x_{n-1} + 1$. Ahora, supongamos que para todo $i = 2, .., n-1$ el lugar R_i es un polo de x_{n-i} o un cero de $x_{n-i} + \delta$ para algún $\delta \in \{0, 1, \alpha, \alpha+1\}$. Entonces el Lema 2.3 asegura en cualquier caso que el lugar $P = R_n \in \{P_0,\, P_1,\, P_\alpha,\, P_{\alpha+1},\, P_\infty\}$ como se quería probar. □



Gráfica 2.3: Cálculo del espacio de ramificación en la torre $\mathcal{H}$

En este momento estamos en condiciones de probar el resultado principal de esta sección.

Teorema 2.6. *La torre $\mathcal{H}$ sobre K es débilmente ramificada y tiene género finito. En particular, para todo entero positivo s la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ tiene género finito y $\gamma(\mathcal{H})$ satisface la desigualdad*

$$\gamma(\mathcal{H}) \leq 4.$$

Demostración. Sea $F = K(x, y)$ el cuerpo de funciones básico asociado a $\mathcal{H}$. Del Lema 2.3 inciso vi se sigue que $F/K(x)$ y $F/K(y)$ son extensiones débilmente ramificadas. Dado que cada extensión F_{i+1}/F_i es una extensión de Galois de grado 2 entonces el Corolario 1.23 asegura que la torre $\mathcal{H}$ sobre K es débilmente ramificada, además es de género finito ya que por la Proposición 2.5 el espacio de ramificación de $\mathcal{H}$ es finito. Finalmente, del Teorema 1.22 se concluye que

$$\gamma(\mathcal{H}) \leq 4,$$

como se quería probar. □

Observación 2.7. *En el Teorema 2.16 se calcula el valor exacto del género de cada cuerpo de funciones de la torre $\mathcal{H}$, como consecuencia se obtiene una mejora de la cota anterior.*

2.2. La tasa de descomposición de la torre: caso par

El objetivo de esta sección es probar que la torre $\mathcal{H}$ tiene tasa de descomposición positiva sobre $\mathbb{F}_4$. En este sentido, calcularemos el género y el número de lugares racionales de cada cuerpo de funciones de la torre $\mathcal{H}$ sobre $\mathbb{F}_4$. Como consecuencia de esos resultados concluiremos que $\mathcal{H}$ es una torre óptima sobre $\mathbb{F}_4$ y que $\mathcal{H}$ es una torre asintóticamente buena sobre $\mathbb{F}_{2^s}$ para todo s entero positivo par. En ésta y en la siguiente sección el símbolo Tr denotará la función traza de $\mathbb{F}_4$ a $\mathbb{F}_2$.

Proposición 2.8. *Sean F/K un cuerpo de funciones, x un elemento de $F \setminus K$ y K el cuerpo total de constantes de F. Supongamos que F'/F es una extensión de Artin-Schreier de grado dos tal que $F' = F(y)$ y*

$$y^2 + y = f(x) := \frac{x}{x^2 + x + 1}.$$

i. Supongamos que existe un elemento $u \in F$ tal que

$$\nu_{P_\beta}(f(x) + u^2 + u) = -1,$$

entonces P_β es un lugar totalmente ramificado en F'/F. El único lugar de F' arriba de P_β es un polo Q_∞ de $y \in F'$ tal que

$$\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta) \quad y \quad d(Q_\infty|P_\beta) = 2.$$

Además, si P es un lugar que no es un cero de $x+\beta$, P no ramifica en F'/F.

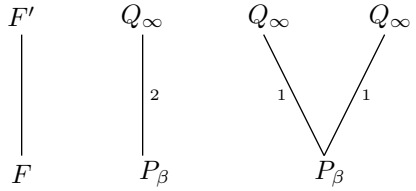
ii. Supongamos que existe un elemento $u \in F$ tal que

$$\nu_{P_\beta}(f(x)+u^2+u) \geq 0 \quad y \quad \mathrm{Tr}((f(x)+u^2+u)(P_\beta)) = 0.$$

Entonces P_β se descompone completamente en F'/F en dos polos de $y \in F'$, además se cumple que

$$2\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta)$$

donde Q_∞ denota cualquiera de esos dos polos.



Gráfica 2.4: Posible descomposición de P_β

Demostración. Probemos i. El Teorema 1.18 garantiza que P_β es totalmente ramificado en F'/F con exponente diferente $d(Q_\infty|P_\beta) = 2$; además, también afirma que si P no es un cero de $x+\beta$ entonces P no ramifica en F'/F ya que $\nu_P(f(x)) \geq 0$. Finalmente, P_β es un polo de $f(x)$ ya que es un cero de $x+\beta$, luego de la ecuación (2.1) se sigue que

$$\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta).$$

Probemos ii. Del Teorema 1.18 se sigue que P_β no ramifica en F'. Por otra parte, como $y^2+y = f(x)$ y $F' = F(y) = F(y+u)$ entonces el polinomio minimal de $y+u$ sobre F es

$$\phi(T) = T^2 + T + f(x) + u^2 + u.$$

Dado que $\mathrm{Tr}((f(x)+u^2+u)(P_\beta)) = 0$ entonces el polinomio

$$\phi_{P_\beta}(T) = T^2 + T + (f(x)+u^2+u)(P_\beta)$$

tiene sus dos raíces en K y por el Teorema de Kummer concluimos que P_β se

descompone completamente en F'/F. De la igualdad $y^2 + y = f(x)$ se obtiene fácilmente que

$$2\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x + \beta). \qquad \square$$

La construcción de elementos que satisfagan las condiciones i o ii de la Proposición anterior será crucial para probar que existe un lugar racional que se descompone completamente en la torre $\mathcal{H}$. En este momento es conveniente introducir la siguiente definición.

Sean F'/F una extensión de Artin-Schreier de grado dos definida por la ecuación (2.1) como en la Proposición 2.8 y P un lugar de F. Un elemento $u \in F$ es llamado un **elemento de tipo** 1 para P si

$$\nu_P(f(x) + u^2 + u) = -1.$$

Un elemento $u \in F$ es llamado un **elemento de tipo** 2 para un lugar racional P si se cumple que

$$\nu_P(f(x) + u^2 + u) \geq 0 \quad \text{y} \quad \mathrm{Tr}((f(x) + u^2 + u)(P)) = 0,$$

donde $(f(x) + u^2 + u)(P)$ denota la reducción módulo P del elemento $f(x) + u^2 + u$.

Observación 2.9. *Los argumentos dados en la Proposición 2.8 garantizan que un lugar P de F es totalmente ramificado en F'/F si existe un elemento de tipo 1 para P y que un lugar racional P se descompone completamente en F'/F si existe un elemento de tipo 2 para P.*

A partir de ahora y hasta la siguiente sección usaremos la notación utilizada en la prueba de la Proposición 2.4, es decir, un cero de x_i (resp. $x_i + 1$) en F_i será denotado por Q_0^i (resp. Q_1^i) y un polo de x_i en F_i será denotado por Q_∞^i. Un cero de $x_i + \beta$ en F_i, con $\beta \in \{\alpha, \alpha + 1\}$, será denotado por Q_β^i y, en general, ese será el significado de un símbolo de la forma Q_δ^i cuando una letra griega como δ sea usada como subíndice.

Ahora probaremos tres resultados técnicos (Lemas 2.10, 2.11 y 2.12). En los dos primeros supondremos que se cumple la siguiente condición:

Condición de ramificación. *Sean $k \geq 0$ y $F_k \subset F_{k+1} \subset F_{k+2}$ una subsucesión de la torre $\mathcal{H}$. Para los lugares $Q_1^k \subset Q_\beta^{k+1}$ una y sólo una de las siguientes condiciones se cumple:*

R1. $\nu_{Q_1^k}(x_k+1)=1$ *y* Q_β^{k+1}*es totalmente ramificado en* F_{k+2}/F_{k+1} *(luego existe un único polo* Q_∞^{k+2} *de* x_{k+2} *en* F_{k+2} *arriba de* Q_β^{k+1}*).*

R2. $\nu_{Q_1^k}(x_k+1)=2$ *y* Q_β^{k+1} *se descompone completamente en* F_{k+2}/F_{k+1} *(luego existen dos polos* Q_∞^{k+2} *de* x_{k+2} *en* F_{k+2} *arriba de* Q_β^{k+1}*).*

Si R1 (resp. R2) se cumple diremos que la sucesión $Q_1^k\subset Q_\beta^{k+1}\subset Q_\infty^{k+2}$ *satisface la condición de ramificación R1 (resp. R2).*

Lema 2.10. *Sean* $k\geq 0$ *e* $i\geq k+4$*. Consideremos la subsucesión* $\{F_j\}_{j=k}^{i-1}$ *de la torre* $\mathcal{H}$ *y la siguiente sucesión de lugares:*

$$Q_1^k\subset Q_\beta^{k+1}\subset Q_\infty^{k+2}\subset Q_0^{k+3}\subset\cdots\subset Q_0^{i-1}$$

donde únicamente tenemos los lugares Q_0^j *para* $k+3\leq j\leq i-1$*. Entonces* $Q_0^{i-1}|Q_\infty^{k+2}$ *no ramifica en* F_{i-1}/F_{k+2}*. Además se cumplen las siguientes propiedades:*

i. Si $\delta:=x_{k+2}+\dfrac{x_{k+1}+1}{x_k+1}$ *entonces* $(x_{k+2}+(x_{k+1}\delta)^2+x_{k+1}\delta)(Q_\infty^{k+2})=\beta$*.*

ii. Para $j=k+3,\cdots,i-1$ *se tiene que* $\left(\dfrac{1}{x_j}+x_{k+2}\right)(Q_0^j)=0$*.*

Demostración. De la Proposición 2.2 se sigue fácilmente que $Q_0^{i-1}|Q_\infty^{k+2}$ no ramifica en la extensión F_{i-1}/F_{k+2}. Demostremos que

$$(x_{k+2}+(x_{k+1}\delta)^2+x_{k+1}\delta)(Q_\infty^{k+2})=\beta.$$

La condición de ramificación implica que

$$\nu_{Q_\infty^{k+2}}(x_k+1)=e(Q_\infty^{k+2}|Q_1^k)\nu_{Q_1^k}(x_k+1)=2. \tag{2.4}$$

Por otra parte, puesto que $\nu_{Q_1^k}(x_k^2+x_k+1)=0$ y $\nu_{Q_\beta^{k+1}}(x_{k+1})=0$ tenemos que

$$\nu_{Q_\infty^{k+2}}(x_{k+1})=\nu_{Q_\infty^{k+2}}\left(\frac{1}{x_k^2+x_k+1}\right)=0. \tag{2.5}$$

En lo sucesivo probaremos una identidad fundamental en el desarrollo de la prueba. Para una mejor comprensión de dicha identidad escribimos $x=x_k$, $y=x_{k+1}$ y $z=x_{k+2}$. En este caso tenemos que $\delta=z+\dfrac{y+1}{x+1}$, además x,y,z satisfacen las siguientes identidades:

$$z^2=z+f(y), \tag{2.6}$$

$$y^2 f(y) = 1 + y + \frac{1}{y^2+y+1}, \tag{2.7}$$

$$\frac{1}{y^2+y+1} + \frac{1}{(x+1)^2} + \frac{1}{x+1} = \frac{x^2+x+1}{(x+1)^2} + \frac{x}{(x+1)^2} = 1. \tag{2.8}$$

Entonces

$$\begin{aligned} z + (y\delta)^2 + y\delta &= z + z^2y^2 + zy + \frac{y^2(y+1)^2}{(x+1)^2} + \frac{y(y+1)}{x+1} \\ &= z + (z + f(y))y^2 + zy + \frac{y^2(y+1)^2}{(x+1)^2} + \frac{y(y+1)}{x+1} \\ &= z + zy^2 + f(y)y^2 + zy + \frac{(y^2+y)^2}{(x+1)^2} + \frac{y^2+y}{x+1} \\ &= z(y^2+y+1) + y + \frac{1}{y^2+y+1} + 1 + \frac{(y^2+y)^2}{(x+1)^2} + \frac{y^2+y}{x+1} \\ &= z(y^2+y+1) + y + \frac{(y^2+y+1)^2}{(x+1)^2} + \frac{y^2+y+1}{x+1} \\ &= z\frac{(x+1)^2}{x^2+x+1} + y + \frac{(x+1)^2}{(x^2+x+1)^2} + \frac{x+1}{x^2+x+1}, \end{aligned}$$

donde la segunda, cuarta y quinta igualdad se obtienen de las ecuaciones (2.6), (2.7) y (2.8) respectivamente. Por lo tanto,

$$x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta = x_{k+2}\frac{(x_k+1)^2}{x_k^2+x_k+1} + x_{k+1} + \frac{(x_k+1)^2}{(x_k^2+x_k+1)^2} + \frac{x_k+1}{x_k^2+x_k+1}.$$

Veremos que todos los términos de la derecha en la igualdad anterior, excepto x_{k+1}, tienen valuación positiva. De (2.4) y (2.5) tenemos que

$$\nu_{Q_\infty^{k+2}}(x_{k+1}) = \nu_{Q_\infty^{k+2}}\left(\frac{1}{x_k^2+x_k+1}\right) = 0 \quad \text{y} \quad \nu_{Q_\infty^{k+2}}(x_k+1) = 2,$$

lo cual implica junto con la ecuación

$$x_{k+2}^2 + x_{k+2} = f(x_{k+1}) = x_{k+1}\frac{x_k^2 + x_k + 1}{(x_k+1)^2}$$

que $\nu_{Q_\infty^{k+2}}(x_{k+2}) = -2$. De todo lo anterior se deduce que

$$\nu_{Q_\infty^{k+2}}(x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta) = 0$$

y

$$(x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta)(Q_\infty^{k+2}) = x_{k+1}(Q_\infty^{k+2}) = x_{k+1}(Q_\beta^{k+1}) = \beta.$$

Para probar el segundo inciso también usaremos varias ecuaciones que se obtienen de la ecuación (2.1) que define la torre. Para todo j entero positivo se cumple que

$$x_j^2 + x_j = f(x_{j-1}) \qquad \text{y} \qquad \frac{1}{f(x_{j-1})} = \frac{1}{x_{j-1}} + 1 + x_{j-1}.$$

De aquí se deduce que

$$\begin{aligned}\frac{1}{x_j} + x_{k+2} &= \frac{x_j+1}{x_j^2+x_j} + x_{k+2} = \frac{x_j+1}{f(x_{j-1})} + x_{k+2} \\ &= \frac{x_j}{x_{j-1}} + x_j + x_j x_{j-1} + 1 + x_{j-1} + \frac{1}{x_{j-1}} + x_{k+2}. \end{aligned} \tag{2.9}$$

También se ve que

$$(x_{k+3}^2 + x_{k+3})x_{k+2} = \frac{x_{k+2}^2}{x_{k+2}^2 + x_{k+2} + 1} \qquad \text{y} \qquad \frac{x_j^2 + x_j}{x_{j-1}} = \frac{1}{x_{j-1}^2 + x_{j-1} + 1}. \tag{2.10}$$

Por otra parte, en la prueba del item anterior mostramos que Q_∞^{k+2} es un polo de orden dos de x_{k+2} y que $e(Q_0^j | Q_\infty^{k+2}) = 1$, luego por la Proposición 2.2 se tiene que

$$\nu_{Q_0^{i-1}}(x_{i-1}) = \cdots = \nu_{Q_0^{k+3}}(x_{k+3}) = -\nu_{Q_\infty^{k+2}}(x_{k+2}) = 2,$$

lo que implica que

$$(x_{i-1}x_{i-2})(Q_0^{i-1}) = \cdots = \left(\frac{x_{k+3}}{x_{k+2}}\right)(Q_0^{k+3}) = 0.$$

Ahora procedamos por inducción sobre j. La ecuación (2.9) para $j = k+3$ es

$$\frac{1}{x_{k+3}} + x_{k+2} = \frac{x_{k+3}}{x_{k+2}} + x_{k+3} + (x_{k+3}x_{k+2} + 1) + \frac{1}{x_{k+2}}.$$

Como Q_0^{k+3} es un cero de los elementos $x_{k+3}, \frac{1}{x_{k+2}}, \frac{x_{k+3}}{x_{k+2}}$ se cumple que la reducción

módulo Q_0^{k+3} del primer, segundo y cuarto sumando en la ecuación anterior es cero. Dado que $(x_{k+3}+1)(Q_0^{k+3}) = 1$ la ecuación (2.10) implica que

$$(x_{k+3}x_{k+2})(Q_0^{k+3}) = ((x_{k+3}+1)(x_{k+3}x_{k+2}))(Q_0^{k+3})$$

$$= \left(\frac{x_{k+2}^2}{x_{k+2}^2 + x_{k+2} + 1}\right)(Q_\infty^{k+2}) = 1,$$

por lo tanto, $(x_{k+2}x_{k+3}+1)(Q_0^{k+3}) = 0$ y concluimos que

$$\left(\frac{1}{x_{k+3}} + x_{k+2}\right)(Q_0^{k+3}) = 0.$$

Ahora, para $j - 1 \geq k+3$ supongamos que se satisface

$$\left(\frac{1}{x_{j-1}} + x_{k+2}\right)(Q_0^{j-1}) = 0.$$

De la ecuación (2.9) tenemos

$$\frac{1}{x_j} + x_{k+2} = \left(\frac{x_j}{x_{j-1}} + 1\right) + x_j + x_j x_{j-1} + x_{j-1} + \frac{1}{x_{j-1}} + x_{k+2}.$$

Como $(x_j+1)(Q_0^j) = 1$ tomando la reducción Q_0^j en la ecuación (2.10) se obtiene

$$\left(\frac{x_j}{x_{j-1}}\right)(Q_0^j) = \left(\frac{(x_j+1)x_j}{x_{j-1}}\right)(Q_0^j) = \left(\frac{1}{x_{j-1}^2 + x_{j-1} + 1}\right)(Q_0^j) = 1.$$

Finalmente, como Q_0^j es un cero de los elementos $x_{j-1}, x_j, x_j x_{j-1}$ y $\frac{1}{x_{j-1}} + x_{k+2}$ concluimos que

$$\left(\frac{1}{x_j} + x_{k+2}\right)(Q_0^j) = 0$$

como se quería probar. □

Lema 2.11. *Sean $k \geq 0$, $i \geq k+3$ y $\{F_j\}_{j=k}^{i+2}$ la subsucesión de la torre $\mathcal{H}$. Si $i = k+3$ consideramos la sucesión de lugares*

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2} \subset Q_1^{k+3} \subset Q_\theta^{k+4} \subset Q_\infty^{k+5},$$

y si $i > k+3$ consideramos la sucesión de lugares

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2} \subset Q_0^{k+3} \subset \cdots \subset Q_0^{i-1} \subset Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2},$$

donde únicamente tenemos los lugares Q_0^j *para* $k+3 \le j \le i-1$. *Entonces* Q_θ^{i+1} *se descompone completamente en* F_{i+2}/F_{i+1} *y se cumple la condición de ramificación R2 para*

$$Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2}.$$

Demostración. Probaremos que el lugar Q_θ^{i+1} se descompone completamente en la extensión F_{i+2}/F_{i+1} mostrando que

$$u := \frac{x_{i+1}+1}{x_i+1} + x_{k+1}\delta$$

es un elemento de tipo 2 para Q_θ^{i+1} con δ definido en el Lema 2.10. Del Lema 2.1 se sigue que

$$\begin{aligned} f(x_{i+1}) + u^2 + u &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + \frac{1}{x_i+1} + (\delta x_{k+1})^2 + \delta x_{k+1} \\ &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i\left(x_{i-1}+1+\frac{1}{x_{i-1}}\right) + (\delta x_{k+1})^2 + \delta x_{k+1} \\ &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i(x_{i-1}+1) + \frac{x_i}{x_{i-1}} + (\delta x_{k+1})^2 + \delta x_{k+1} \\ &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i(x_{i-1}+1) + \frac{x_i+1}{x_{i-1}} + \left(\frac{1}{x_{i-1}} + x_{k+2}\right) \\ &\quad + (x_{k+2} + (\delta x_{k+1})^2 + \delta x_{k+1}). \end{aligned} \tag{2.11}$$

Ahora calcularemos la reducción módulo Q_θ^{i+1} del elemento $f(x_{i+1}) + u^2 + u$. Si $i > k+3$ tenemos que $x_i(Q_\theta^{i+1}) = x_i(Q_1^i) = 1$ y $x_{i-1}(Q_\theta^{i+1}) = x_{i-1}(Q_0^{i-1}) = 0$, además

$$\left(x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i(x_{i-1}+1)\right)(Q_\theta^{i+1}) = \theta + 1 + 1 = \theta.$$

Por otra parte, la ecuación (2.10) con $j = i$, implica que

$$\left(\frac{x_i+1}{x_{i-1}}\right)(Q_\theta^{i+1}) = \left(\frac{x_i^2+x_i}{x_{i-1}}\right)(Q_1^i) = \left(\frac{1}{x_{i-1}^2+x_{i-1}+1}\right)(Q_0^{i-1}) = 1.$$

Finalmente, el Lema 2.10 implica que

$$\left(\frac{1}{x_{i-1}} + x_{k+2}\right)(Q_\theta^{i+1}) + (x_{k+2} + (\delta x_{k+1})^2 + \delta x_{k+1})(Q_\theta^{i+1}) = 0 + \beta = \beta.$$

De todo lo anterior concluimos que

$$(f(x_{i+1}) + u^2 + u)(Q_\theta^{i+1}) = \theta + 1 + \beta.$$

Para $i = k+3$ vale el mismo resultado. Al reescribir la ecuación (2.11) obtenemos

$$f(x_{k+4}) + u^2 + u = x_{k+4} + \frac{1}{x_{k+3}^2 + x_{k+3} + 1} + x_{k+3}\left(1 + \frac{1}{x_{k+2}}\right) +$$

$$+ (x_{k+3} + 1)x_{k+2} + x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta.$$

Como $x_{k+3}(Q_\theta^{k+4}) = x_{k+3}(Q_1^{k+3}) = 1$ y $\frac{1}{x_{k+2}}(Q_\theta^{k+4}) = \frac{1}{x_{k+2}}(Q_\infty^{k+2}) = 0$ entonces

$$\left(x_{k+4} + \frac{1}{x_{k+3}^2 + x_{k+3} + 1} + x_{k+3}\left(1 + \frac{1}{x_{k+2}}\right)\right)(Q_\theta^{k+4}) = \theta + 1 + 1 = \theta$$

y de la ecuación (2.10) se sigue que

$$\begin{aligned}((x_{k+3} + 1)x_{k+2})(Q_\theta^{k+4}) &= ((x_{k+3}^2 + x_{k+3})x_{k+2})(Q_1^{k+3}) \\ &= \left(\frac{x_{k+2}^2}{x_{k+2}^2 + x_{k+2} + 1}\right)(Q_\infty^{k+2}) = 1.\end{aligned}$$

Finalmente, para cualquier $i \geq k+3$ tenemos que

$$\mathrm{Tr}((f(x_{i+1}) + u^2 + u)(Q_\theta^{i+1})) = \mathrm{Tr}(\theta + 1 + \beta) = 0$$

ya que $\theta + 1 + \beta \in \mathbb{F}_2$. Entonces por la Proposición 2.8 concluimos que Q_θ^{i+1} se descompone completamente en F_{i+2}/F_{i+1}. Para garantizar que la sucesión

$$Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2}$$

cumple la condición de ramificación R2 resta probar que $\nu_{Q_1^i}(x_i + 1) = 2$ para $i \geq k+3$. Esto es fácil de ver pues la Proposición 2.2 afirma que

$$\nu_{Q_1^i}(x_i + 1) = \nu_{Q_0^{i-1}}(x_{i-1}) \qquad \text{o} \qquad \nu_{Q_1^{k+3}}(x_{k+3} + 1) = -\nu_{Q_\infty^{k+2}}(x_{k+2})$$

y en la demostración del Lema 2.10 vimos que $\nu_{Q_0^{i-1}}(x_{i-1}) = -\nu_{Q_\infty^{k+2}}(x_{k+2}) = 2$. □

Lema 2.12. *Sea $\{F_j\}_{j=k}^{k+2}$ una subsucesión de la torre $\mathcal{H}$. Si Q_1^k es un cero simple de $x_k+1 \in F_k$ entonces la sucesión de lugares*

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2}$$

cumple la condición de ramificación R1, es decir, el lugar Q_β^{k+1} es totalmente ramificado en F_{k+2}/F_{k+1}.

Demostración. Sean $u = \frac{x_{k+1}+1}{x_k+1}$ y $\delta = x_{k+2} + u$. Por el Lema 2.1 tenemos que

$$\delta^2 + \delta = f(x_{k+1}) + u^2 + u = x_{k+1} + \frac{1}{x_k^2 + x_k + 1} + \frac{1}{x_k + 1}.$$

Dado que Q_1^k es un cero simple de $x_k + 1$ por hipótesis y $e(Q_\beta^{k+1}|Q_1^k) = 1$ por la Proposición 2.2, entonces

$$\begin{aligned} \nu_{Q_\infty^{k+2}}(\delta^2+\delta) &= e(Q_\infty^{k+2}|Q_\beta^{k+1})\nu_{Q_\beta^{k+1}}\left(x_{k+1} + \frac{1}{x_k^2+x_k+1} + \frac{1}{x_k+1}\right) \\ &= -e(Q_\infty^{k+2}|Q_\beta^{k+1}). \end{aligned}$$

Luego, $2\nu_{Q_\infty^{k+2}}(\delta) = -e(Q_\infty^{k+2}|Q_\beta^{k+1})$ y concluimos que $e(Q_\infty^{k+2}|Q_\beta^{k+1}) = 2$. □

Ahora estamos preparados para enunciar y demostrar el resultado principal de esta sección.

Teorema 2.13. *Sea $\{F_j\}_{j=k}^{k+2}$ una subsucesión de la torre $\mathcal{H}$ y consideremos la sucesión*

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2}.$$

Supongamos que Q_1^k es un lugar racional y un cero simple de x_k+1. Entonces Q_∞^{k+2} se descompone completamente en $\mathcal{H}$.

Demostración. De las Proposiciones 2.2 y 2.8 toda sucesión de lugares en la torre $\mathcal{H}$ arriba de Q_∞^{k+2} es una combinación de subsucesiones de tipo 1 y/o tipo 2 respectivamente:

$$Q_1^j \subset Q_\theta^{j+1} \subset Q_\infty^{j+2},$$

y

$$Q_0^j \subset \cdots \subset Q_0^{j+l-1},$$

donde $j \geq k+3$ y $l \geq 1$. Cualquier lugar en una subsucesión de tipo 2 se descompone completamente en cada paso de la torre, así que es suficiente considerar sucesiones que tienen subsucesiones intermedias de tipo 1 o de tipo 1 y 2. Iniciemos con el caso

$j = k+3$. Dado que Q_1^k es un cero simple de $x_k + 1$ entonces el Lemma 2.12 asegura que la condición de ramificación R1 es válida en la subsucesión

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2},$$

además dichos lugares son racionales por la Proposición 2.2 y por ser Q_1^k un lugar racional. Ahora, el Lema 2.11 implica que las subsucesiones

$$Q_1^{k+3} \subset Q_\theta^{k+4} \subset Q_\infty^{k+5} \qquad \text{y} \qquad Q_1^{k+l+3} \subset Q_\gamma^{k+l+4} \subset Q_\infty^{k+l+5}$$

satisfacen la condición de ramificación R2, donde se tienen las subsucesiones, que son combinación de subsucesiones de tipo 1 y de tipo 1 y 2 respectivamente, que se muestran a continuación:

$$Q_1^k \subset Q_\theta^{k+1} \subset Q_\infty^{k+2} \subset Q_1^{k+3} \subset Q_\theta^{k+4} \subset Q_\infty^{k+5},$$

y

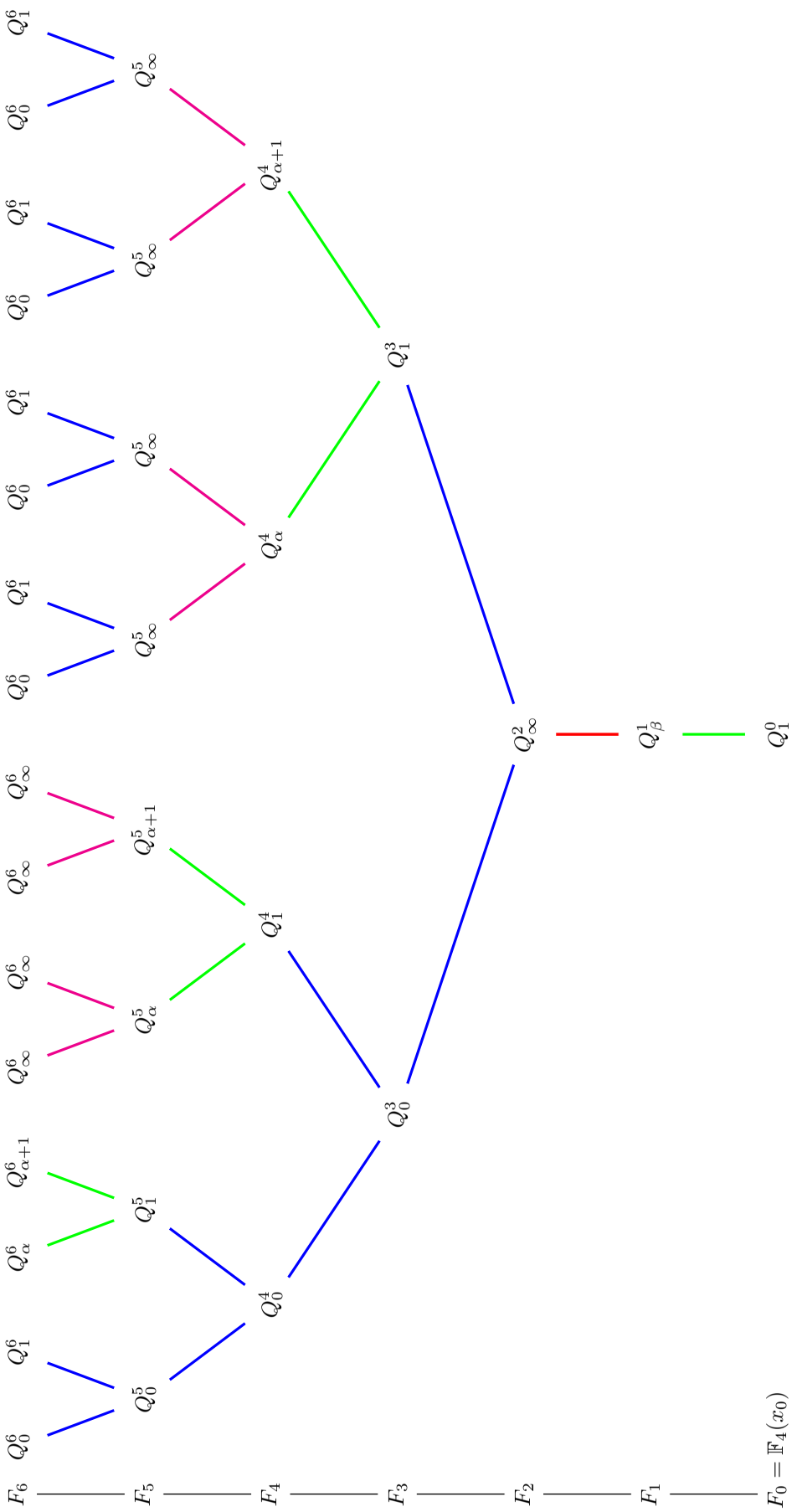
$$Q_1^k \subset Q_\theta^{k+1} \subset Q_\infty^{k+2} \subset Q_0^{k+3} \subset \cdots \subset Q_0^{k+l+2} \subset Q_1^{k+l+3} \subset Q_\gamma^{k+l+4} \subset Q_\infty^{k+l+5},$$

con $l \geq 1$; todos los lugares en estas subsucesiones son racionales ya que Q_∞^{k+2} es racional y todo lugar que cae sobre él se descompone completamente en su respectiva extensión. Los argumentos anteriores garantizan que cualquier sucesión de lugares en la torre $\mathcal{H}$ arriba de Q_∞^{k+2} es precisamente una combinación de subsucesiones intermedias de lugares racionales de tipo 1 y/o tipo 2 en la que toda subsucesión de tipo 1 satisface la condición de ramificación R2, por lo tanto Q_∞^{k+2} se descompone completamente en la torre $\mathcal{H}$. □

Finalizamos esta sección con un corolario de gran importancia en este trabajo.

Corolario 2.14. *La torre $\mathcal{H}$ es asintóticamente buena sobre $\mathbb{F}_{2^s}$ para s entero positivo par.*

Demostración. Dado que Q_1^0 es un cero simple de $x_0 + 1$ entonces por el Teorema 2.13 tenemos que Q_∞^2 se descompone completamente en la torre $\mathcal{H}$ sobre $\mathbb{F}_4$. Por otra parte, del Teorema 2.6 sabemos que $\mathcal{H}$ tiene género finito sobre $\mathbb{F}_4$, luego por el Corolario 1.25 concluimos que $\mathcal{H}$ es asintóticamente buena sobre $\mathbb{F}_4$. Por último, $\mathcal{H}$ es asintóticamente buena sobre $\mathbb{F}_{2^s}$ con s par ya que es una extensión por constantes de la torre $\mathcal{H}$ sobre $\mathbb{F}_4$ y la extensión algebraica $\mathbb{F}_{2^s}$ con s par. □



Gráfica 2.5: Descomposición de Q_2^∞

2.3. El límite de la torre sobre $\mathbb{F}_4$

El propósito de esta sección es dar una fórmula explícita para el número de lugares racionales y el género de cada cuerpo de funciones F_l de la torre $\mathcal{H}$ sobre $\mathbb{F}_4$. Como consecuencia de ese resultado veremos que la torre $\mathcal{H}$ sobre $\mathbb{F}_4$ es óptima, esto es, $\lambda(\mathcal{H}) = A(4) = 1$. Más aún veremos que para todo $s > 2$ entero positivo par el límite de la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ es al menos uno.

Teorema 2.15. *Sea $l \geq 3$. El número de lugares racionales $N(F_l)$ del cuerpo de funciones $F_l \in \mathcal{H}$ es*

$$N(F_l) = 2^{l+1} + 8.$$

El número de lugares totalmente ramificados en F_{i+1}/F_i es: dos para $i = 0, 1$, cuatro para $i = 2$ y ocho para $3 \leq i \leq l-1$.

Demostración. Para calcular el número de lugares racionales de F_l debemos contar el número de lugares racionales arriba de cada lugar racional Q_β^0 con $\beta \in \mathbb{F}_4 \cup \{\infty\}$. Iniciamos con el lugar Q_1^0 que es un cero simple de $x_0 + 1 \in F_0$. Entonces por la Proposición 2.2 y el Lema 2.12 tenemos dos sucesiones:

$$Q_1^0 \subset Q_\alpha^1 \subset Q_\infty^2 \qquad \text{y} \qquad Q_1^0 \subset Q_{\alpha+1}^1 \subset Q_\infty^2. \tag{2.12}$$

Por el Teorema 2.13 cada Q_∞^2 se descompone completamente en F_l/F_2, luego existen $2 \cdot 2^{l-2}$ lugares racionales en F_l arriba de Q_0^1. Además, los lugares Q_α^1 y $Q_{\alpha+1}^1$ son totalmente ramificados en la extensión F_2/F_1 y ningún otro lugar Q de F_j, con $0 \leq j \leq l-1$, arriba de Q_1^0 es totalmente ramificado en F_{j+1}/F_j por la Proposiciones 2.2, 2.8 y el Lema 2.11.

Ahora consideremos el lugar racional Q_0^0 que es un cero simple de $x_0 \in F_0$. Por la Proposición 2.2, Q_0^0 se descompone completamente en los lugares Q_1^1, un cero simple de $x_1 + 1$, y Q_0^1, un cero simple de x_1. Por lo que tenemos dos sucesiones $Q_0^0 \subset Q_1^1$ y $Q_0^0 \subset Q_0^1$. En el primer caso del Lema 2.12 obtenemos las sucesiones:

$$Q_1^1 \subset Q_\alpha^2 \subset Q_\infty^3 \qquad \text{y} \qquad Q_1^1 \subset Q_{\alpha+1}^2 \subset Q_\infty^3. \tag{2.13}$$

Notemos que la situación descrita en (2.13) se corresponde con la analizada en (2.12) porque Q_1^1 es un lugar racional y es un cero simple de $x_1 + 1 \in F_1$. Por lo tanto, los mismos argumentos usados anteriormente para deducir el número de lugares racionales en F_l arriba de Q_1^0 nos permiten concluir que existen 2^{l-2} lugares racionales de F_l arriba de Q_1^1, donde los lugares Q_α^2 y $Q_{\alpha+1}^2$ son totalmente ramificados en la extensión F_3/F_2; además, ningún otro lugar Q de F_j arriba de Q_1^1 es totalmente

ramificado en F_{j+1}/F_j, con $2 \leq j \leq l-1$. Ahora para $1 \leq i \leq l-2$ tenemos las siguientes sucesiones de lugares sobre Q_0^0

$$Q_0^0 \subset Q_0^1 \subset \cdots \subset Q_0^{i-1} \subset Q_1^i, \quad \text{y} \quad Q_0^0 \subset Q_0^1 \subset \cdots \subset Q_0^{l-3} \subset Q_0^{l-2}.$$

Cada una de las primeras $l-2$ sucesiones aporta 2^{l-i-1} lugares racionales a F_l, de los cuales Q_α^{i+1} y $Q_{\alpha+1}^{i+1}$ son los únicos lugares arriba de Q_0^0 que son totalmente ramificados en la extensión F_{i+2}/F_{i+1}. La última sucesión aporta otros cuatro lugares racionales, pues la Proposición 2.2 afirma que Q_α^l, $Q_{\alpha+1}^l$, Q_∞^l y Q_∞^l son racionales y están arriba de Q_0^{l-2}. Por lo tanto, el número de lugares racionales de F_l arriba de Q_0^0 es:

$$2^{l-2} + 2^{l-3} + \cdots + 2 + 4 = 2^{l-1} + 2,$$

además, para $2 \leq j \leq l-1$ en la extensión F_{j+1}/F_j tenemos exactamente dos lugares que son totalmente ramificados y están arriba de Q_0^0. Concretamente son los lugares Q_β^j con $\beta \in \{\alpha, \alpha+1\}$ tales que la sucesión de lugares en $\{F_k\}_{k=0}^j$ es del tipo:

$$Q_0^0 \subset Q_0^1 \subset \cdots \subset Q_0^{j-2} \subset Q_1^{j-1} \subset Q_\beta^j. \tag{2.14}$$

Ahora consideremos el lugar racional Q_∞^0, el cual es un polo simple de x_0. De la Proposición 2.2 vemos que el lugar racional tiene el mismo comportamiento en la extensión F_1/F_0 que el lugar Q_0^0, por lo tanto, tiene el mismo comportamiento que Q_0^0 en la torre $\mathcal{H}$, lo que implica que el número de lugares racionales en F_l arriba de Q_∞^0 también es $2^{l-1}+2$; además, en la extensión F_{j+1}/F_j, con $2 \leq j \leq l-1$, tenemos exactamente dos lugares Q_β^j que son totalmente ramificados y caen sobre Q_∞^0. Por lo tanto, en $\{F_k\}_{k=0}^j$ tenemos la sucesión de lugares del tipo:

$$Q_\infty^0 \subset Q_0^1 \subset \cdots \subset Q_0^{j-2} \subset Q_1^{j-1} \subset Q_\beta^j. \tag{2.15}$$

Finalmente, calcularemos el número de lugares racionales en F_l y el número de lugares totalmente ramificados arriba de Q_β^0, con $\beta \in \{\alpha, \alpha+1\}$, en cada extensión intermedia. Dado que Q_β^0 es un cero simple de $x_0 + \beta$ de la Proposición 2.8 inciso i (con $u = 0$) tenemos que Q_β^0 es totalmente ramificado en F_1/F_0 y que el lugar Q_∞^1 de F_1 que cae sobre Q_β^0 es un polo simple de x_1. Observemos que el lugar Q_∞^1 cumple las mismas propiedades que el lugar Q_∞^0 analizado previamente, por lo tanto, $2^{l-2}+2$ es el número de lugares racionales en F_l arriba de Q_∞^1 y, en particular, arriba de Q_β^0. Además, para $3 \leq j \leq l-1$ y $l > 3$, en la extensión F_{j+1}/F_j hay exactamente cuatro lugares totalmente ramificados, dos arriba de Q_α^0 y dos arriba de $Q_{\alpha+1}^0$. En este caso

los tipos de sucesiones de lugares en $\{F_k\}_{k=0}^{j}$ que obtenemos son las siguientes:

$$Q_\alpha^0 \subset Q_\infty^1 \subset Q_1^2 \subset Q_\beta^3 \quad \text{y} \quad Q_\alpha^0 \subset Q_\infty^1 \subset Q_0^2 \subset \cdots \subset Q_0^{j-2} \subset Q_1^{j-1} \subset Q_\beta^j, \tag{2.16}$$

la primera para $j = 3$ y la segunda con $j > 3$. Arriba de $Q_{\alpha+1}^0$ obtenemos

$$Q_{\alpha+1}^0 \subset Q_\infty^1 \subset Q_1^2 \subset Q_\beta^3 \quad \text{y} \quad Q_{\alpha+1}^0 \subset Q_\infty^1 \subset Q_0^2 \subset \cdots \subset Q_0^{j-2} \subset Q_1^{j-1} \subset Q_\beta^j, \tag{2.17}$$

la primera para $j = 3$ y la segunda con $j > 3$. Notemos que todos los lugares que aparecen en los distintos tipos de sucesiones son diferentes, a pesar de estar denotados de la misma forma. De todo lo anterior tenemos que el número $N(F_l)$ de lugares racionales en F_l es exactamente

$$N(F_l) = 2^{l-1} + 2 \cdot (2^{l-1} + 2) + 2 \cdot (2^{l-2} + 2) = 2^{l+1} + 8,$$

además, damos la descripción precisa de los lugares totalmente ramificados para cada extensión F_{i+1}/F_i con $0 \leq i \leq l-1$. En principio para $0 \leq i \leq 2$ tenemos que

$$\begin{cases} Q_\beta^0 & \text{en} \quad F_1/F_0, \\ Q_\beta^1 & \text{en} \quad F_2/F_1 \text{ con } Q_\beta^1 | Q_1^0, \\ Q_\beta^2 & \text{en} \quad F_3/F_2 \text{ con } Q_\beta^2 | Q_0^0 \text{ y } Q_\beta^2 | Q_\infty^0 \end{cases}$$

y para $i \geq 3$ tenemos los lugares Q_β^i en F_{i+1}/F_i y están completamente determinados por las sucesiones (2.14), (2.15), (2.16) y (2.17) respectivamente. Finalmente hay que resaltar que el exponente diferente de cada lugar es 2 lo cual es una consecuencia de la Proposición 2.8 item i. □

Teorema 2.16. *Sea $l \geq 3$. El género $g(F_l)$ del cuerpo de funciones $F_l \in \mathcal{H}$ es*

$$g(F_l) = 2^{l+1} - 7.$$

Demostración. Del Teorema 2.15 tenemos que en las extensiones F_1/F_0 y F_2/F_1 existen dos lugares totalmente ramificados, en F_3/F_4 existen cuatro lugares totalmente ramificados y en F_{i+1}/F_i existen ocho lugares totalmente ramificados donde $3 \leq i \leq l-1$; además, todos ellos son lugares racionales y tienen exponente diferente dos, por lo tanto,

$$\deg(\mathrm{Diff}(F_{i+1}/F_i)) = \begin{cases} 4 & \text{si } i = 0, 1, \\ 8 & \text{si } i = 2, \\ 16 & \text{si } i \geq 3. \end{cases}$$

Ahora por la fórmula del género de Hurwitz (Teorema 1.8) tenemos que

$$g(F_{i+1}) - 1 = (g(F_i) - 1) \cdot 2 + \frac{1}{2} \deg(\mathrm{Diff}(F_{i+1}/F_i)).$$

Fácilmente vemos que $g(F_1) = 1$, $g(F_2) = 3$, $g(F_3) - 1 = 2^3$ y que

$$g(F_4) - 1 = (g(F_3) - 1) \cdot 2 + \frac{1}{2} 2^4 = (2^3) \cdot 2 + 2^3 = 2^4 + 2^3.$$

Sea $i \geq 4$. Supongamos que

$$g(F_i) - 1 = 2^i + 2^{i-1} + \cdots + 2^4 + 2^3 = \sum_{j=3}^{i} 2^j$$

entonces

$$g(F_{i+1}) - 1 = (g(F_i) - 1) \cdot 2 + \frac{1}{2} 2^4 = \left(\sum_{j=3}^{i} 2^j \right) \cdot 2 + 2^3 = \sum_{j=3}^{i+1} 2^j.$$

Por lo tanto, para cualquier $l \geq 3$ tenemos que

$$g(F_l) - 1 = \sum_{j=3}^{l} 2^j = 2^{l+1} - 2^3. \qquad \square$$

Corolario 2.17. *La torre $\mathcal{H}$ sobre $\mathbb{F}_4$ es óptima y tanto su tasa de descomposición como su género son iguales a dos.*

Demostración. De los Teoremas 2.15 y 2.16 tenemos que

$$\lambda(\mathcal{H}) = \lim_{l \to \infty} \frac{N(F_l)}{g(F_l)} = \lim_{l \to \infty} \frac{2^{l+1} + 8}{2^{l+1} - 7} = 1,$$

además $\mathcal{H}$ tiene tasa de descomposición

$$\nu(\mathcal{H}) = \lim_{l \to \infty} \frac{N(F_l)}{[F_l : F_0]} = \lim_{l \to \infty} \frac{2^{l+1} + 8}{2^l} = 2$$

y género

$$\gamma(\mathcal{H}) = \lim_{l \to \infty} \frac{g(F_l)}{[F_l : F_0]} = \lim_{l \to \infty} \frac{2^{l+1} - 7}{2^l} = 2. \qquad \square$$

Corolario 2.18. *El límite de la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ con s entero positivo par satisface*

$$\lambda(\mathcal{H}) \geq 1\cdot$$

Demostración. Es una consecuencia inmediata del corolario anterior y la Proposición 1.26. □

Finalizamos esta sección con algunas observaciones e interrogantes.

Observación 2.19. Otra prueba[1] de que el género la torre $\mathcal{H}$ es dos es la siguiente: para cualquier conjunto de lugares S de F_0 denotaremos por $\mathbb{P}_i(S)$ al conjunto de lugares de F_i que caen sobre los lugares de S. Por el Lema 2.3 y el Corolario 1.23 tenemos que $\mathcal{H}$ es una torre débilmente ramificada sobre $\mathbb{F}_4$. Luego por la fórmula del género de Hurwitz (Teorema 1.8), la Proposición 2.5 y la igualdad fundamental (Proposición 1.1) tenemos que el género de F_i satisface que

$$2g(F_i) - 2 = -2[F_i : F_0] + 2 \sum_{P\in\mathcal{R}(\mathcal{H})} \sum_{Q|P} (e(Q|P) - 1),$$

luego

$$\begin{aligned} g(F_i) - 1 &= -2^i + \sum_{P\in\mathcal{R}(\mathcal{H})} \sum_{Q|P} e(Q|P) - \sum_{P\in\mathcal{R}(\mathcal{H})} \sum_{Q|P} 1 \\ &= -2^i + \sum_{P\in\mathcal{R}(\mathcal{H})} 2^i - 2|\mathbb{P}_i(\mathcal{R}(\mathcal{H}))| \\ &= -2^i + 2^i|\mathcal{R}(\mathcal{H})| - |\mathbb{P}_i(\mathcal{R}(\mathcal{H}))| \\ &= 2^i(|\mathcal{R}(\mathcal{H})| - 1) - |\mathbb{P}_i(\mathcal{R}(\mathcal{H}))|. \end{aligned}$$

Del Teorema 2.15 tenemos que

$$|\mathbb{P}_i(\mathcal{R}(\mathcal{H}))| = N(F_i) = 2^{i+1} + 8,$$

por lo tanto,

$$g(F_i) - 1 = 2^{i+2} - 2^{i+1} - 8 = 2^{i+1} - 8$$

y

$$\gamma(\mathcal{H}) = \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]} = 2.$$

Antes de enunciar nuestra siguiente observación introducimos el concepto de clausura de Galois de una torre. Sean $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre sobre $\mathbb{F}_q$ y E_i la clausura de

[1] Esta observación fue planteada por P. Beelen en la revisión del artículo [7].

Galois de la extensión F_i/F_0 para cada $i \geq 1$. La sucesión de cuerpos de funciones $\mathcal{G} = \{E_i\}_{i=0}^{\infty}$, con $E_0 = F_0$, se denomina la **clausura de Galois** de $\mathcal{F}$.

En el artículo [12] se demostró que es suficiente que una torre $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ tenga espacio de descomposición no vacío para asegurar que su clausura de Galois $\mathcal{G}$ sea una torre sobre $\mathbb{F}_q$. Si, adicionalmente, $\mathcal{F}$ tiene espacio de ramificación finito y es una torre 2-acotada tal que cada F_{i+1}/F_i es una p-extensión de Galois, donde p es la característica de $\mathbb{F}_q$, entonces $\mathcal{G}$ es una torre asintóticamente buena. Estas condiciones las cumple la torre $\mathcal{H}$, ver Teorema 2.13, Proposición 2.5 y Lema 2.3. En consecuencia:

Observación 2.20. La clausura de Galois de la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ es una torre asintóticamente buena.

Pregunta 2.21. ¿Es asintóticamente óptima la clausura de Galois de $\mathcal{H}$ sobre $\mathbb{F}_4$?

Pregunta 2.22. ¿Cuál es valor exacto del límite $\lambda(\mathcal{H})$ si consideramos la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ con $s > 2$ entero positivo par?

Pregunta 2.23. ¿Existe una torre $\mathcal{F}$ sobre $\mathbb{F}_{q^2}$ definida de forma recusiva que generalice la torre $\mathcal{H}$ sobre $\mathbb{F}_4$?

Pregunta 2.24. ¿Es modular la torre $\mathcal{H}$ sobre $\mathbb{F}_4$?

Esta última pregunta surge de la famosa conjetura de la modularidad de Elkies [10].

Conjetura de Elkies. Cualquier torre asintóticamente óptima definida de forma recursiva sobre un cuerpo finito de cardinalidad cuadrada es modular, esto es, los cuerpos en la torre son cuerpos de funciones de curvas modulares o de curvas modulares de Shimura o reducción de curvas modulares de Drinfeld.

2.4. La tasa de descomposición de la torre: caso impar

En esta sección calcularemos el número de lugares racionales de cada cuerpo de funciones de la torre $\mathcal{H}$ sobre $k := \mathbb{F}_{2^s}$ para cualquier entero positivo impar s. Como consecuencia de esto concluiremos que la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ tiene tasa de descomposición cero y, por lo tanto, es asintóticamente mala. Con este importante resultado finalizaremos el capítulo 2.

Denotamos la función traza de $\mathbb{F}_{2^s}$ a $\mathbb{F}_2$ por Tr. Iniciamos con el siguiente lema clave:

Lema 2.25. *Sean $\theta, \beta \in k$ tales que $\theta^2 + \theta = \frac{\beta}{\beta^2+\beta+1}$. Entonces*

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) \neq \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right).$$

Demostración. Supongamos que

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right)$$

entonces la linealidad de la traza implica que

$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0. \tag{2.18}$$

Por otra parte, por hipótesis

$$\theta^2 + \theta = \frac{\beta}{\beta^2+\beta+1}$$

luego

$$\frac{1}{\theta^2+\theta+1} = \frac{\beta^2+\beta+1}{\beta^2+1} = 1 + \frac{\beta}{\beta+1} + \left(\frac{\beta}{\beta+1}\right)^2.$$

Finalmente, dado que $\mathrm{Tr}(1) = 1$ y $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2)$ para todo $\alpha \in k$, tenemos que

$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = \mathrm{Tr}(1) + \mathrm{Tr}\left(\frac{\beta}{\beta+1}\right) + \mathrm{Tr}\left(\left(\frac{\beta}{\beta+1}\right)^2\right) = 1,$$

lo cual contradice (2.18). □

Llegados a este punto, estamos en posición de probar el resultado principal de esta sección.

Teorema 2.26. *Consideremos la torre $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ sobre k. Para todo $i \geq 1$, el número de lugares racionales de F_i es constante, más precisamente, para todo $i \geq 1$ se tiene que*

$$N(F_i) = 2(|S| + 1),$$

donde

$$S = \left\{\beta \in k : \mathrm{Tr}\left(\frac{\beta}{\beta^2+\beta+1}\right) = 0\right\}.$$

Demostración. Sea P un lugar racional de F_i. Dado que s es impar, entonces para cualquier $\beta \in k$ se tiene que $\beta^2 + \beta + 1 \neq 0$. Luego la reducción módulo P del

polinomio

$$\phi = T^2 + T + \frac{x_i}{x_i^2 + x_i + 1} \in F_i[T],$$

es el polinomio

$$\phi_\beta = T^2 + T + \frac{\beta}{\beta^2 + \beta + 1} \in k[T].$$

para algún $\beta \in k$. Por otra parte, el Teorema 90 de Hilbert afirma que

$$\mathrm{Tr}\left(\frac{\beta}{\beta^2 + \beta + 1}\right) = 0 \quad \text{si y sólo si} \quad \frac{\beta}{\beta^2 + \beta + 1} = \theta^2 + \theta,$$

para algún $\theta \in k$, por lo tanto, ϕ_β es irreducible sobre k si y sólo si

$$\mathrm{Tr}\left(\frac{\beta}{\beta^2 + \beta + 1}\right) = 1.$$

Sean P_∞ el polo de x_0 en $F_0 = k(x_0)$ y P_β el cero de $x_0 + \beta$ en F_0, donde $\beta \in k$. Entonces $\phi \mod P_\infty = \phi_0$ y $\phi \mod P_\beta = \phi_\beta$ para $\beta \in k$. Si $\beta \notin S \cup \{\infty\}$ tenemos que ϕ_β es irreducible sobre k y del Teorema de Kummer (Teorema 1.16) se sigue que P_β es inerte, que existe un sólo lugar en F_1 arriba de P_β y que tiene grado dos. Ahora si $\beta \in S \cup \{\infty\}$ el polinomio ϕ_β se descompone completamente sobre k, es decir, ϕ_β se factoriza como producto de dos polinomios lineales distintos sobre k. Claramente si $\theta \in k$ es una raíz de ϕ_β entonces $\phi_\beta(T) = (T + \theta)(T + (\theta + 1))$. Nuevamente por el Teorema de Kummer, existen exactamente dos lugares racionales Q_θ, $Q_{\theta+1}$ de $F_1 = F_0(x_1)$ arriba de P_β. Entonces

$$N(F_1) = 2(|S| + 1).$$

El Teorema de Kummer también afirma que $x_1 + \theta \in Q_\theta$ y $x_1 + (\theta + 1) \in Q_{\theta+1}$ así que las clases residuales $x_1(Q_\theta)$ y $x_1(Q_{\theta+1})$ son θ y $\theta + 1$ respectivamente. Consideremos ahora los lugares racionales de F_2. Cada uno de estos lugares está arriba de un lugar racional de la forma Q_θ, $Q_{\theta+1}$ para algún $\theta \in k$, así que los polinomios ϕ_θ y $\phi_{\theta+1}$ son la reducción de ϕ módulo Q_θ y $Q_{\theta+1}$ respectivamente. El Lema 2.25 garantiza que

$$\phi_\theta = T^2 + T + \frac{\theta}{\theta^2 + \theta + 1},$$

se descompone completamente sobre k (resp. es irreducible sobre k) si y sólo si

$$\phi_{\theta+1} = T^2 + T + \frac{\theta + 1}{\theta^2 + \theta + 1}$$

es irreducible sobre k (resp. se descompone completamente sobre k), luego Q_θ se

descompone completamente (resp. es inerte) si y sólo si $Q_{\theta+1}$ es inerte (resp. se descompone completamente). Por lo tanto, para cada par de lugares Q_θ, $Q_{\theta+1}$ tenemos que, nuevamente por el Teorema de Kummer, uno de ellos es inerte y que existen dos lugares racionales de F_2 que caen sobre el otro. Así el número de lugares racionales de F_2 es

$$N(F_2) = N(F_1) = 2(|S| + 1).$$

En particular, hemos probado que cada lugar racional de F_2 cae sobre un lugar racional de F_1 de la forma Q_θ para algún $\theta \in k$, el cuál se descompone completamente en F_2 en dos lugares racionales de F_2 de la forma Q_γ y $Q_{\gamma+1}$ con clases residuales $x_2(Q_\gamma) = \gamma$ y $x_2(Q_{\gamma+1}) = \gamma + 1$ por el Teorema de Kummer. Por hipótesis inductiva, $N(F_i) = 2(|S| + 1)$ y cada lugar racional de F_i cae arriba de un lugar racional F_{i-1} de la forma Q_θ para algún $\theta \in k$, el cuál se descompone completamente en F_i en dos lugares racionales de F_i de la forma Q_δ y $Q_{\delta+1}$ con clases residuales $x_i(Q_\delta) = \delta$ y $x_i(Q_{\delta+1}) = \delta + 1$. De nuevo vemos que la reducción de ϕ módulo esos dos lugares son los polinomios ϕ_δ y $\phi_{\delta+1}$ así que por el Lema 2.25

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

se descompone completamente sobre k (resp. es irreducible sobre k) si y sólo si

$$\phi_{\delta+1}(T) = T^2 + T + \frac{\delta + 1}{\delta^2 + \delta + 1}$$

es irreducible sobre k (resp. se descompone completamente sobre k). Por lo tanto, Q_δ o $Q_{\delta+1}$ se descompone completamente en F_{i+1} mientras que el otro es inerte en F_{i+1}, lo que permite concluir que

$$N(F_{i+1}) = N(F_i) = 2(|S| + 1). \qquad \square$$

Corolario 2.27. *Para todo entero impar s la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ es asintóticamente mala.*

Demostración. Del Teorema 2.26 tenemos que

$$\nu(\mathcal{H}) = \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]} = \lim_{i\to\infty} \frac{2(|S| + 1)}{2^i} = 0. \qquad \square$$

CAPÍTULO 3
SUBSUCESIONES Y SUPERSUCESIONES DE CUERPOS DE FUNCIONES

En la teoría de torres de cuerpos de funciones las subtorres y supertorres juegan un papel relevante, pues en muchos casos, nos brindan información asintótica de una torre dada. En este sentido, un resultado bien conocido en la teoría es que una subtorre de una torre asintóticamente buena también es asintóticamente buena. Un ejemplo del uso de esta técnica fue presentado por Bassa, Garcia y Stichtenoth [1], quienes construyeron una torre $\mathcal{F}$ sobre $\mathbb{F}_{q^3}$ asintóticamente buena, que además, resultó ser una supertorre de la torre $\mathcal{E}$ estudiada anteriormente por Bezerra, Garcia y Stichtenoth en el artículo [4]. Vale la pena destacar que el estudio del comportamiento asintótico de $\mathcal{E}$ requirió cálculos más extensos y técnicos que aquellos empleados en el estudio asintótico de la torre $\mathcal{F}$. Teniendo esta idea como motivación dedicamos gran parte de este capítulo a la construcción de subsucesiones y supersucesiones recursivas de torres de cuerpos de funciones.
Iniciamos este capítulo con algunas definiciones y resultados básicos de torres y subtorres de cuerpos de funciones.

Sean $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ y $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ sucesiones no triviales de cuerpos de funciones sobre $\mathbb{F}_q$. Diremos que $\mathcal{E}$ es una **subsucesión** de $\mathcal{F}$ o que $\mathcal{F}$ es una **supersucesión** de $\mathcal{E}$ si para cada $i \geq 0$ existe un índice $j := j(i)$ y una inmersión $\iota_i : E_i \to F_j$ sobre $\mathbb{F}_q$. Lo anterior equivale a que $E_i \subseteq F_j$. Sin perdida de generalidad podemos suponer que $E_i \subseteq F_i$ omitiendo algunos de los F_i y reenumerando si es necesario. Si la contenencia anterior es propia para infinitos índices, es decir, $E_i \subsetneq F_i$ para infinitos índices, diremos que $\mathcal{E}$ es una **subsucesión propia** de $\mathcal{F}$. En caso de que $\mathcal{E}$ y $\mathcal{F}$ sean torres decimos que $\mathcal{E}$ es una **subtorre** de $\mathcal{F}$ y lo denotamos por $\mathcal{E} \prec \mathcal{F}$.

Proposición 3.1. *[20, Proposición 7.28]. Si $\mathcal{E}$ es una subtorre de $\mathcal{F}$ entonces*

$$\lambda(\mathcal{E}) \geq \lambda(\mathcal{F}).$$

En particular, se tiene que:

i. Si $\mathcal{F}$ es asintóticamente buena entonces $\mathcal{E}$ también es asintóticamente buena.

ii. Si $\mathcal{E}$ es asintóticamente mala entonces $\mathcal{F}$ también es asintóticamente mala.

Observación 3.2. Si suponemos que la extensión F_0/E_0 es finita y separable, se puede mostrar la relación siguiente relación las tasas de descomposición y los géneros de $\mathcal{E}$ y $\mathcal{F}$:

$$\nu(\mathcal{E}) \geq \frac{\nu(\mathcal{F})}{[F_0 : E_0]} \qquad \text{y} \qquad \gamma(\mathcal{E}) \leq \frac{\gamma(\mathcal{F})}{[F_0 : E_0]}.$$

En particular, obtenemos los resultados de la proposición anterior. En efecto, observemos que

$$[E_i : F_i] < \infty \qquad \text{y} \qquad N(F_i) \leq N(E_i)[F_i : E_i],$$

luego,

$$\frac{N(E_i)}{[E_i : E_0]} = \frac{N(E_i)[F_i : E_i]}{[F_i : E_0]} \geq \frac{N(F_i)}{[F_i : E_0]} = \frac{1}{[F_0 : E_0]} \frac{N(F_i)}{[F_i : F_0]},$$

por lo tanto,

$$\nu(\mathcal{E}) \geq \frac{\nu(\mathcal{F})}{[F_0 : E_0]}.$$

Por otra parte, dado que F_i/E_0 es una extensión separable entonces la extensión F_i/E_i también lo es y como el divisor diferente es efectivo, es decir $\mathrm{Diff}(F_i/E_i) \geq 0$, entonces

$$\deg(\mathrm{Diff}(F_i/E_i)) \geq 0.$$

Este hecho y la fórmula del género de Hurwitz (Teorema 1.8) implican que

$$g(F_i) - 1 \geq [F_i : E_i](g(E_i) - 1),$$

luego,

$$\frac{g(F_i) - 1}{[F_i : F_0][F_0 : E_0]} \geq \frac{(g(E_i) - 1)[F_i : E_i]}{[F_i : E_0]} = \frac{g(E_i)}{[E_i : E_0]},$$

de lo que concluimos que,

$$\gamma(\mathcal{E}) \leq \frac{\gamma(\mathcal{F})}{[F_0 : E_0]}.$$

3.1. Un método para construir subsucesiones de cuerpos de funciones

En esta sección proponemos un método para construir subsucesiones recursivas de (a, b)-sucesiones de cuerpos de funciones y mostramos que varias de las subtorres conocidas en la literatura en realidad se pueden obtener de esta manera. También vemos que este método generaliza el método dado en [6]. Iniciamos esta sección con un resultado clave.

Proposición 3.3. *Sean $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ y $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sucesiones recursivas no triviales de cuerpos de funciones sobre $\mathbb{F}_q$ definidas respectivamente por las relaciones*

$$h(y_i, y_{i+1}) = 0 \qquad y \qquad f(x_i, x_{i+1}) = 0$$

donde $h(X, Y)$ y $f(X, Y)$ son polinomios con coeficientes en $\mathbb{F}_q$ y $\{x_i\}_{i=0}^{\infty}$ y $\{y_i\}_{i=0}^{\infty}$ son sucesiones de elementos trascendentes sobre $\mathbb{F}_q$. Para cada $i \geq 0$ supongamos que

$$\deg_Y h \leq [F_{i+1} : F_i]$$

y $y_i = g(x_i)$ con $g(T) = g_1(T)/g_2(T)$ una función racional con coeficientes en $\mathbb{F}_q$ de grado mayor que uno. Entonces $E_i \subsetneq F_i$ para cada $i \geq 0$, esto es, $\mathcal{E}$ es una subsucesión propia de $\mathcal{F}$.

Demostración. Dado que $y_i = g(x_i)$, $E_i = \mathbb{F}_q(y_0, \cdots, y_i)$ y $F_i = \mathbb{F}_q(x_0, \cdots, x_i)$ entonces $E_i \subseteq F_i$ para cada $i \geq 0$. Por otra parte, sin perdida de generalidad podemos suponer que el grado de la función racional $g(T)$ es $\deg g(T) = \deg g_1(T)$. Para cada $i \geq 0$ consideremos el polinomio

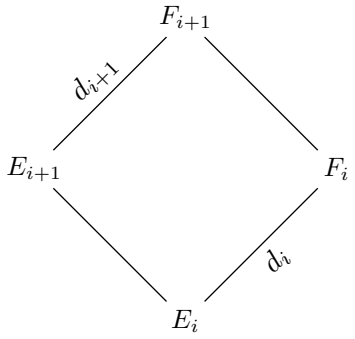
$$\varphi_i(T) = g_1(T) - g_2(T)y_i \in E_i[T].$$

Es claro que el elemento x_i es una raíz del polinomio $\varphi_i(T)$ para cada $i \geq 0$. Dado que $E_0 = \mathbb{F}_q(y_0)$ y $F_0 = \mathbb{F}_q(x_0)$ entonces $[F_0 : E_0] = \deg g > 1$. Ahora sea $d_i = [F_i : E_i]$. Puesto que el grado de una torre de cuerpos es multiplicativo (ver gráfica 3.1) tenemos que

$$d_{i+1}[E_{i+1} : E_i] = d_i[F_{i+1} : F_i].$$

Probemos por inducción que $d_i > 1$ para $i \geq 1$. Supongamos que $d_1 = 1$ entonces

$$\deg g[F_1 : F_0] = d_0[F_1 : F_0] = [E_1 : E_0].$$



Gráfica 3.1: Subcuerpos en las torres $\mathcal{E}$ y $\mathcal{F}$

Por hipótesis $[E_1 : E_0] \leq \deg_Y h \leq [F_1 : F_0]$, por lo tanto, $\deg g \leq 1$ lo cual es una contradicción. Supongamos ahora que $d_i > 1$ y $d_{i+1} = 1$ entonces

$$d_i[F_{i+1} : F_i] = [E_{i+1} : E_i] \leq \deg_Y h \leq [F_{i+1} : F_i],$$

y esto implica que $d_i \leq 1$, lo cual es una contradicción. Concluimos que $E_i \subsetneq F_i$ para cada $i \geq 0$, es decir, $\mathcal{E}$ es una subsucesión propia de $\mathcal{F}$. □

Observación 3.4. De la demostración de la proposición anterior se deduce que

$$\deg g = [F_0 : E_0] \qquad \text{y} \qquad [F_i : E_i] \geq \deg g$$

para cada $i \geq 1$. Aún más, si para cada $i \geq 0$ se cumple la condición

$$[E_{i+1} : E_i] = \deg_Y h = [F_{i+1} : F_i]$$

entonces para $i \geq 0$ se tiene que

$$[F_i : E_i] = \deg g.$$

A continuación recordamos las definiciones de (a, b)-sucesión recursiva y del grado de una función racional ya que serán usadas en el resto del capítulo. Una sucesión recursiva $\mathcal{F}$ sobre $\mathbb{F}_q$ es una (a, b)-**sucesión recursiva** o una **sucesión recursiva** de tipo (a, b) si $a(T), b(T)$ son funciones racionales con coeficientes en $\mathbb{F}_q$ tales que

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

donde $(a_1(T), a_2(T)) = 1$ y $(b_1(T), b_2(T)) = 1$ y $\mathcal{F}$ está definida por un polinomio

de la forma

$$H(X,Y) = a_1(Y)b_2(X) - a_2(Y)b_1(X).$$

En este caso se suele decir que la (a,b)-sucesión recursiva $\mathcal{F}$ está definida por la ecuación con variables separadas

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

Sean $g_1(T)$, $g_2(T) \in \mathbb{F}_q[T]$ polinomios primos relativos. Se define el **grado de la función racional** $g(T) = g_1(T)/g_2(T)$ como

$$\deg g(T) = \text{máx}\{\deg g_1(T), \deg g_2(T)\}.$$

En adelante, consideramos (a,b)-sucesiones recursivas con $\deg a = \deg b$ ya que las torres recursivas que no poseen esta propiedad resultan ser asintóticamente malas. (Ver [13]).

Teorema 3.5. ***(El método)*** *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ una (a,b)-sucesión no trivial de cuerpos de funciones y $\{x_i\}_{i=0}^{\infty}$ una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ tales que*

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

para cada $i \geq 0$. Supongamos que $A(T), B(T), g(T), s(T) \in \mathbb{F}_q(T)$ son funciones racionales que cumplen las condiciones:

$$A \circ g = s \circ a \qquad y \qquad B \circ g = s \circ b. \tag{3.1}$$

Entonces $\{g(x_i)\}_{i=0}^{\infty}$ es una sucesión de elementos trascendentes sobre $\mathbb{F}_q$,

$$A(g(x_{i+1})) = B(g(x_i))$$

y la sucesión $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ definida por $E_0 = \mathbb{F}_q(g(x_0))$ y $E_{i+1} = E_i(g(x_{i+1}))$ es una (A,B)-subsucesión recursiva de $\mathcal{F}$. Si, además, suponemos que la sucesión $\mathcal{E}$ es no trivial y que para cada $i \geq 0$ se cumple la condición:

$$\deg A \leq [F_{i+1} : F_i] \tag{3.2}$$

Entonces $\mathcal{E}$ es una subsucesión propia de $\mathcal{F}$.

Demostración. Puesto que $\{x_i\}_{i=0}^{\infty}$ es una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ y $g(T)$ es una función racional con coeficientes en $\mathbb{F}_q$ entonces $\{g(x_i)\}_{i=0}^{\infty}$ es

una sucesión de elementos trascendentes sobre $\mathbb{F}_q$. Para cada $i \geq 0$ se tiene que $a(x_{i+1}) = b(x_i)$, entonces por las condiciones (3.1) tenemos que

$$A(g(x_{i+1})) = s(a(x_{i+1})) = s(b(x_i)) = B(g(x_i)).$$

Ahora, dado que $F_i = \mathbb{F}_q(x_0, \ldots, x_i)$ y $y_j = g(x_j) \in F_i$, para cada $0 \leq j \leq i$, se deduce que $E_i = \mathbb{F}_q(g(x_0), \ldots, g(x_i)) \subseteq F_i$ para todo $i \geq 0$, es decir, $\mathcal{E}$ es una subsucesión de $\mathcal{F}$. Ahora, supongamos que la sucesión $\mathcal{E}$ es no trivial, que se cumple la condición (3.2) y consideremos el polinomio

$$h(X, Y) = A_1(Y) - A_2(Y)B(X)$$

donde $A(Y) = A_1(Y)/A_2(Y)$. Es fácil ver que $\mathcal{E}$ está recursivamente definida por la ecuación $h(X, Y) = 0$ y que

$$\deg_Y h = \deg A \leq [F_{i+1} : F_i].$$

Entonces por la Proposición 3.3 tenemos que $\mathcal{E}$ es una subsucesión propia de $\mathcal{F}$, como se quería probar. □

Una ventaja notable del método anterior es que, en general, la condición (3.2) es fácil de comprobar. ¿Bajo que condiciones se puede concluir que $\mathcal{E}$ es una subtorre propia de $\mathcal{F}$ en caso de no se cumpla dicha condición?

Observación 3.6. Supongamos que $\mathcal{E}$ y $\mathcal{F}$ son sucesiones recursivas no triviales que satisfacen las condiciones (3.1). Si para cada $i \geq 0$ se cumplen las condiciones:

$$\deg A > [F_{i+1} : F_i] \qquad \text{y} \qquad [E_{i+1} : E_i] \leq [F_{i+1} : F_i].$$

Entonces $\mathcal{E}$ es una subtorre propia de $\mathcal{F}$.

Ahora describiremos brevemente el método propuesto en [6] para construir subsucesiones de una sucesión de cuerpos de funciones dada:

Proposición 3.7. *[6, Proposición 3.2.6] Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una (a, b)-sucesión no trivial de cuerpos de funciones. Sean f, $\tilde{a}$ y $\tilde{b}$ funciones racionales irreducibles con coeficientes en $\mathbb{F}_q$ tales que*

$$\tilde{a} \circ f \circ b = \tilde{b} \circ f \circ a\,. \tag{3.3}$$

Consideremos la sucesión recursiva no trivial $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ *definida por*

$$\tilde{a}(y_{i+1}) = \tilde{b}(y_i)$$

con $y_i = f(a(x_i))$ *para cada* $i \geq 0$. *Supongamos que se cumplen las siguientes condiciones:*

i. $\deg a = [F_{i+1} : F_i]$ *y* $\deg \tilde{a} = [E_{i+1} : E_i]$ *para cada* $i \geq 0$.

ii. $\deg a \geq \deg \tilde{a}$ *o* $(\deg \tilde{a}, \deg a) = 1$.

Entonces $\mathcal{E}$ *es una subsucesión propia de* $\mathcal{F}$.

A continuación hacemos algunas observaciones relacionadas con este método.

Observación 3.8. Para ver que el método anterior es un caso particular del planteado en el Teorema 3.5 basta tomar $A = \tilde{a}$, $B = \tilde{b}$, $g = f \circ a$ y $s = \tilde{a} \circ f$ y ver que las condiciones (3.1) se satisfacen. En efecto,

$$A \circ g = \tilde{a} \circ f \circ a = s \circ a \qquad \text{y} \qquad B \circ g = \tilde{b} \circ f \circ a = \tilde{a} \circ f \circ b = s \circ b.$$

También podemos tomar $g = f \circ b$ y $s = \tilde{b} \circ f$, luego

$$A \circ g = \tilde{a} \circ f \circ b = \tilde{b} \circ f \circ a = s \circ a \qquad \text{y} \qquad B \circ g = \tilde{b} \circ f \circ b = s \circ b.$$

Observación 3.9. Si tomamos $g = f \circ a$, como en la observación anterior, entonces

$$[F_0 : E_0] = \deg g = \deg f \cdot \deg a.$$

A continuación mostraremos tres ejemplos en los que se construyen subtorres propias de una torre dada usando el método propuesto en el Teorema 3.5, además, mostraremos que dichas subtorres no se pueden obtener por el método anterior.

Ejemplo 3.10. Sea $\mathcal{F}_1$ sobre $\mathbb{F}_{q^2}$ la (a, b)-torre recursiva definida por la ecuación

$$y^q + y = \frac{x^q}{x^{q-1} + 1}. \tag{3.4}$$

Esta torre es óptima y fue estudiada en [11]. Por otra parte, Bezerra y Garcia mostraron en [3] que la (A, B)-torre $\mathcal{F}_0 = \{E_i\}_{i=0}^{\infty}$ definida sobre $\mathbb{F}_{q^2}$ por la ecuación

$$\frac{y-1}{y^q} = \frac{x^q - 1}{x} \tag{3.5}$$

es una subtorre de $\mathcal{F}_1$. Veamos que $\mathcal{F}_0$ es una subtorre propia de $\mathcal{F}_1$ que se puede obtener usando el método dado en el Teorema 3.5. En este caso tenemos que

$$a(T) = T^q + T, \quad b(T) = \frac{T^q}{T^{q-1}+1}, \quad A(T) = \frac{T-1}{T^q} \quad \text{y} \quad B(T) = \frac{T^q - 1}{T}.$$

Consideremos las funciones racionales

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

Entonces se cumplen las condiciones (3.1). En efecto,

$$A(g(T)) = \frac{\frac{1}{T^{q-1}+1} - 1}{\left(\frac{1}{T^{q-1}+1}\right)^q} = -T^{q-1}(T^{q-1}+1)^{q-1}$$

$$= -(T^q + T)^{q-1} = s(a(T))$$

y

$$B(g(T)) = \frac{\left(\frac{1}{T^{q-1}+1}\right)^q - 1}{\frac{1}{T^{q-1}+1}} = \frac{(1-(T^{q-1}+1)^q)(T^{q-1}+1)}{(T^{q-1}+1)^q}$$

$$= -\frac{(T^{q-1})^q}{(T^{q-1}+1)^{q-1}} = s(b(T)).$$

Por otro lado, si la subtorre $\mathcal{E}$ pudiese obtenerse por el método dado en la Proposición 3.7 entonces, por la Observación 3.9, tendríamos que

$$q - 1 = [F_0 : E_0] = \deg f \cdot \deg a = \deg f \cdot q,$$

lo cual es una contradicción.

Ejemplo 3.11. Consideremos la (a,b)-torre $\mathcal{F}_2 = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_{q^3}$ estudiada por Bassa et al. en [1] y que está definida por la ecuación

$$(y^q - y)^{q-1} + 1 = -\frac{x^{q(q-1)}}{(x^{q-1}-1)^{q-1}}. \tag{3.6}$$

Una característica notable de esta torre es que

$$[F_1 : F_0] = q(q-1) \qquad \text{y} \qquad [F_{i+1} : F_i] = q \quad \text{para todo } i \geq 1.$$

Esto implica que no podemos usar el método de la Proposición 3.7 para obtener subtorres propias de $\mathcal{F}_2$ pues esta torre no cumple la condición i. Usemos el método planteado en el Teorema 3.5 para mostrar que la (A, B)-torre $\mathcal{F}_3 = \{E_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_{q^3}$ estudiada en el artículo [4] y definida por la ecuación

$$\frac{1-y}{y^q} = \frac{x^q + x - 1}{x} \tag{3.7}$$

es una subtorre propia de $\mathcal{F}_2$. A diferencia de $\mathcal{F}_2$, cada extensión E_{i+1}/E_i de $\mathcal{F}_3$ es de grado q. En este caso tenemos

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

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

Consideremos las funciones racionales

$$g(T) = -\frac{1}{T^{q-1}-1} \qquad \text{y} \qquad s(T) = -T + 1$$

y comprobemos que se cumplen las condiciones (3.1). En efecto,

$$\begin{aligned} A(g(T)) &= \frac{1 + \frac{1}{T^{q-1}-1}}{\left(-\frac{1}{T^{q-1}-1}\right)^q} = -T^{q-1}(T^{q-1}-1)^{q-1} \\ &= -T^{q-1}(T^{q-1}-1)^{q-1} = -(T^q - T)^{q-1} = s(a(T)) \end{aligned}$$

y

$$B(g(T)) = \left(\frac{1}{T^{q-1}-1}\right)^{q-1} + 1 - (T^{q-1}-1)$$

$$= \left(\frac{1}{T^{q-1}-1}\right)^{q-1} + 1 - \frac{(T^{q-1}-1)^q}{(T^{q-1}-1)^{q-1}}$$

$$= \frac{(T^{q-1})^q}{(T^{q-1}-1)^{q-1}} + 1 = s(b(T)).$$

Finalmente, podemos destacar una propiedad adicional que tienen estas dos torres: dado que $H_i \subsetneq F_i$ para cada $i \geq 0$ tenemos que

$$[F_0 : H_0] = q - 1 \qquad \text{y} \qquad [F_i : H_i] = (q-1)^2 \quad \text{para cada} \quad i \geq 1,$$

por lo tanto, para cada $i \geq 1$ tenemos que el cuerpo F_{i+1} es la composición de los cuerpos F_i y H_{i+1}.

Ejemplo 3.12. Sea $\mathcal{F}_4 = \{H_i\}_{i=0}^{\infty}$ la (A, B)-torre recursiva sobre $\mathbb{F}_{q^3}$ definida por la ecuación

$$y^{q+1} + y = \frac{x+1}{x^{q+1}}. \tag{3.8}$$

Veamos que $\mathcal{F}_4$ es una subtorre propia de la (a, b)-torre $\mathcal{F}_3$ considerada en el ejemplo anterior. Hay que resaltar que el grado de cada extensión H_{i+1}/H_i es q a pesar de que la ecuación (3.8) es de grado $q+1$, por lo que la hipótesis i no se cumple y no podemos usar el método planteado en la Proposición 3.7. Por otra parte, notemos que las hipótesis de la Observación 3.6 sí se satisfacen; de modo que, para concluir que $\mathcal{F}_4$ es una subtorre propia de $\mathcal{F}_3$ resta mostrar que se satisfacen las condiciones (3.1). En efecto, si consideramos

$$A(T) = T^{q+1} + T, \quad B(T) = \frac{T+1}{T^{q+1}}, \quad a(T) = \frac{1-T}{T^q},$$

$$b(T) = \frac{T^q + T - 1}{T}, \quad g(T) = -\frac{T^q + T - 1}{T-1} \quad \text{y} \quad s(T) = -\frac{T-1}{T^{q+1}},$$

entonces

$$A(g(T)) = \frac{(1 - T - T^q)T^{q^2}}{(T-1)^{q+1}} = s(a(T))$$

y

$$B(g(T)) = -\frac{T^q(T-1)^q}{(T^q + T - 1)^{q+1}} = s(b(T)).$$

3.2. Sobre la composición de torres de cuerpos de funciones

A continuación describiremos una manera de construir supertorres asintóticamente buenas a partir de una torre asintóticamente buena. Este método fue propuesto en el artículo [14].

Introducimos las siguientes definiciones. Sean $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ una sucesión de cuerpos de funciones y F/E_0 una extensión finita y separable. La sucesión de

cuerpos de funciones $\{F_i\}_{i=0}^{\infty}$, donde $F_i = E_iF$ para cada $i \geq 0$, es llamada la **composición** de $\mathcal{E}$ y F y se denota por $\mathcal{E}F$. Diremos que la sucesión $\mathcal{E}$ y el cuerpo F son **linealmente disjuntos** sobre E_0 si para cada $i \geq 1$ los cuerpos E_i y F son linealmente disjuntos sobre E_0.

Teorema 3.13. *[14, Teorema 3.2] Sea $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ una torre de cuerpos de funciones sobre $\mathbb{F}_q$ que cumple las siguientes condiciones:*

i. E_{i+1}/E_i es una extensión de Galois para cada $i \geq 0$.

ii. el espacio de descomposición $\mathcal{S}(\mathcal{E})$ de la torre $\mathcal{E}$ es no vacío.

iii. $\mathcal{E}$ es asintóticamente buena.

Supongamos que F/E_0 una extensión finita y separable, que $\mathbb{F}_q$ es el cuerpo total de constantes de F, que la torre $\mathcal{E}$ y el cuerpo F son linealmente disjuntos sobre E_0 y que el conjunto

$$S := \{Q \in \mathbb{P}(F) : \deg Q = 1 \quad y \quad Q \cap E_0 \in \mathcal{S}(\mathcal{E})\}$$

es no vacío. Entonces $\mathcal{E}F$ es una torre asintóticamente buena sobre $\mathbb{F}_q$ y su límite $\lambda(\mathcal{E}F)$ satisface la desigualdad

$$\lambda(\mathcal{E}F) \geq \frac{|S|}{g(F) - 1 + [F : E_0](1 + N(E_0)/\lambda(\mathcal{E}))}.$$

Observación 3.14. En la demostración del resultado anterior se obtiene la siguiente cota superior para el género de $\mathcal{E}F$

$$\gamma(\mathcal{E}F) \leq g(F) - 1 + [F : E_0]\left(1 + \frac{N(E_0)}{\nu(\mathcal{E})}\gamma(\mathcal{E})\right). \tag{3.9}$$

Los resultados del teorema anterior pueden generalizarse de la siguiente manera:

Proposición 3.15. *Sean $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ una torre de cuerpos de funciones sobre $\mathbb{F}_q$ y F/E_0 una extensión finita y separable tal que la torre $\mathcal{E}$ y el cuerpo F son linealmente disjuntos sobre E_0. Supongamos que el espacio de descomposición de $\mathcal{E}$, $\mathcal{S}(\mathcal{E})$, y que el conjunto*

$$S := \{Q \in \mathbb{P}(F) : \deg Q = 1 \quad y \quad Q \cap E_0 \in \mathcal{S}(\mathcal{E})\}$$

son no vacíos, entonces la sucesión $\mathcal{E}F$ es una torre sobre $\mathbb{F}_q$, su género, $\gamma(\mathcal{E}F)$, cumple

$$\gamma(\mathcal{E}F) \leq g(F) - 1 + [F : E_0](1 + \gamma(\mathcal{E})) \tag{3.10}$$

y su límite $\lambda(\mathcal{E}F)$ satisface la desigualdad

$$\lambda(\mathcal{E}F) \geq \frac{|S|}{g(F) - 1 + [F : E_0](1 + \gamma(\mathcal{E}))}.$$

Si, además, $\mathcal{E}$ tiene género finito entonces $\mathcal{E}F$ es asintóticamente buena.

Demostración. Es claro que la sucesión $\mathcal{E}F = \{F_i\}_{i=0}^{\infty}$ con $F_i = E_iF$ es una sucesión no trivial de cuerpos de funciones, que cada F_{i+1}/F_i es una extensión finita y separable y que $g(F_i) \to \infty$ cuando $i \to \infty$. Para concluir que $\mathcal{E}F$ es una torre resta ver que $\mathbb{F}_q$ es el cuerpo total de constantes de cada F_i. Esta condición será probada después. Ahora mostraremos que se cumple (3.10). Por la Proposición 1.7 (desigualdad de Castelnuovo) tenemos, para $i \geq 1$, que

$$g(F_i) \leq g(F)[F_i : F] + g(E_i)[F_i : E_i] + ([F_i : F] - 1)([F_i : E_i] - 1),$$

esto es,

$$\frac{g(F_i)}{[F_i : F]} \leq g(F) + g(E_i)\frac{[F_i : E_i]}{[F_i : F]} + \frac{[F_i : F] - 1}{[F_i : F]}([F_i : E_i] - 1).$$

Por otra parte, como en la extensiones de cuerpos los grados son multiplicativos, se tiene que

$$[F_i : E_i][E_i : E_0] = [F_i : E_0] = [F_i : F][F : E_0],$$

es decir,

$$\frac{[F_i : E_i]}{[F_i : F]} = \frac{[F : E_0]}{[E_i : E_0]}.$$

Dado que $F_i = E_iF$ para cada $i \geq 1$, también se satisface que

$$[F_i : E_i] \leq [F : E_0],$$

para cada $i \geq 1$. De todo lo anterior se sigue que

$$\begin{aligned}
\frac{g(F_i)}{[F_i : F]} &\leq g(F) + g(E_i)\frac{[F_i : E_i]}{[F_i : F]} + \frac{[F_i : F] - 1}{[F_i : F]}([F_i : E_i] - 1) \\
&= g(F) + g(E_i)\frac{[F : E_0]}{[F_i : E_i]} + \frac{[F_i : F] - 1}{[F_i : F]}([F_i : E_i] - 1) \\
&\leq g(F) + [F : E_0]\frac{g(E_i)}{m_i} + \frac{[F_i : F] - 1}{[F_i : F]}([F : E_0] - 1),
\end{aligned}$$

por lo tanto,

$$\gamma(\mathcal{E}F) \leq g(F) - 1 + [F : E_0](\gamma(\mathcal{E}) + 1).$$

Supongamos que $\mathcal{S}(\mathcal{E})$ y S son conjuntos no vacíos y tomemos un lugar Q en S. Dado que Q es un lugar racional de F tenemos que el cuerpo total de constantes de F es $\mathbb{F}_q$. Ahora, como $P := Q \cap E_0$ pertenece a $\mathcal{S}(\mathcal{E})$ entonces P es un lugar racional de E_0 que se descompone en E_i/E_0 para cada $i \geq 1$. Luego por la Proposición 1.6 el lugar racional Q se descompone completamente en F_i/F_0 para cada $i \geq 1$ y esto implica que $\mathbb{F}_q$ es el cuerpo total de constantes de cada F_i. En particular, $\mathcal{E}F$ es una torre sobre $\mathbb{F}_q$, Q se descompone completamente en la torre $\mathcal{E}$ y se sigue que $S \subseteq \mathcal{S}(\mathcal{E}F)$. Finalmente, concluimos que

$$\lambda(\mathcal{E}F) = \frac{\nu(\mathcal{E}F)}{\gamma(\mathcal{E}F)} \geq \frac{|\mathcal{S}(\mathcal{E}F)|}{\gamma(\mathcal{E}F)} \geq \frac{|S|}{g(F) - 1 + [F : E_0](1 + \gamma(\mathcal{E}))}. \qquad \square$$

Observación 3.16. Si $\mathcal{E}$ es una torre de género finito entonces la cota (3.10) mejora la cota (3.9). En efecto, dado que el número de lugares racionales $N(E_i)$ de E_i satisface que

$$N(E_i) \leq N(E_0)[E_i : E_0]$$

entonces $\nu(\mathcal{E}) \leq N(E_0)$. Por lo tanto,

$$\gamma(\mathcal{E}) \leq \frac{N(E_0)}{\nu(\mathcal{E})}\gamma(\mathcal{E}),$$

y esto implica que

$$g(F) - 1 + [F : E_0](\gamma(\mathcal{E}) + 1) \leq g(F) - 1 + [F : E_0]\left(1 + \frac{N(E_0)}{\nu(\mathcal{E})}\gamma(\mathcal{E})\right).$$

Observemos que el lado izquierdo de la desigualdad anterior es la cota (3.10) para el género de $\mathcal{E}F$, obtenida en la Proposición 3.15, y el lado derecho es la cota (3.9) para el género de $\mathcal{E}F$ obtenida por Garcia et. al. en el Teorema 3.13. A continuación se muestra un ejemplo en el cual la desigualdad anterior es estricta.

Ejemplo 3.17. Consideremos la torre $\mathcal{F}_0 = \{E_i\}_{i=0}^{\infty}$ definida sobre $\mathbb{F}_{q^2}$ por la ecuación

$$\frac{y-1}{y^q} = \frac{x^q - 1}{x}. \tag{3.11}$$

En el artículo [3] Bezerra y Garcia demostraron que $\mathcal{F}_0$ es una torre óptima con género $\gamma(\mathcal{F}_0) = \frac{q}{q-1}$ y tasa de descomposición $\nu(\mathcal{F}_0) = q$. Este último resultado se

obtuvo al mostrar que el espacio de descomposición de $\mathcal{F}_0$ es

$$\mathcal{S}(\mathcal{F}_0) = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ tales que } \alpha^q + \alpha - 1 = 0\}.$$

También demostraron, para $q \neq 2$, que las extensiones E_{i+1}/E_i no son Galois. Sea $q \neq 2$ y consideremos la extensión finita $F = \mathbb{F}_{q^2}(x_0, z_0)$ de $E_0 = \mathbb{F}_{q^2}(x_0)$ definida por la ecuación de tipo Kummer

$$z_0^{q-1} = -\frac{x_0 - 1}{x_0^q}. \tag{3.12}$$

Por la teoría de extensiones de Kummer (Teorema 1.17) el polinomio mínimo de z_0 sobre E_0 es

$$\varphi(T) = T^{q-1} + \frac{x_0 - 1}{x_0^q}$$

y el grado de la extensión F/E_0 es $q-1$; los únicos lugares que ramifican en F/E_0 son P_0, el cero de x_0, y P_1, el cero de $x_0 + 1$, además, son totalmente ramificados. Luego por la fórmula del género de Hurwitz se sigue que el género de F es cero. Ahora para cada $P_\alpha \in \mathcal{S}(\mathcal{F}_0)$ tenemos que

$$\varphi_{P_\alpha}(T) := \varphi(T) \quad \text{mód } P_\alpha = T^{q-1} - 1$$

y como este polinomio tiene $q-1$ raíces distintas en $\mathbb{F}_{q^2}$, por el Teorema de Kummer concluimos que $|S| = q(q-1)$ donde

$$S = \{Q \in \mathbb{P}(F) : Q \text{ es racional y } Q \cap E_0 \in \mathcal{S}(\mathcal{F}_0)\}.$$

Finalmente, por la Proposición 3.15 concluimos que el género de la torre $\mathcal{E} = \mathcal{F}_0 F$ sobre $\mathbb{F}_{q^2}$ está acotado por

$$\gamma(\mathcal{E}) \leq g(F) - 1 + [F : E_0](1 + \gamma(\mathcal{F}_0)) = 2(q-1)$$

que y el límite de $\mathcal{E}$ satisface

$$\lambda(\mathcal{E}) \geq \frac{|S|}{2(q-1)} = \frac{q}{2}.$$

Estos resultados mejoran las cotas para el género y el límite de la torre $\mathcal{E}$ que se obtienenen con el Teorema 3.13 y que se muestran a continuación:

$$\gamma(\mathcal{E}) \leq g(F) - 1 + [F : E_0](1 + N(E_0)/\lambda(\mathcal{F}_0)) = q^2 + q - 1$$

y

$$\lambda(\mathcal{E}F) \geq |S|/(2(q-1)) = q(q-1)/(q^2+q-1).$$

En la Proposición 3.15 vimos que para obtener resultados asintóticos de la composición de $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ y un cuerpo F (que contiene a E_0) es necesario que $\mathcal{E}$ y F sean linealmente disjuntos sobre E_0. Un resultado bien conocido en la teoría de cuerpos afirma que si los grados $[E_i : E_0]$ y $[F : E_0]$ son primos relativos (como en el ejemplo anterior) entonces E_i y F son cuerpos linealmente disjuntos sobre E_0. Si los grados no son primos relativos no hay un criterio simple para garantizar que $\mathcal{E}$ y F sean linealmente disjuntos sobre E_0. En la siguiente proposición tratamos este problema.

Proposición 3.18. *Sea $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones no trivial sobre $\mathbb{F}_q$ tal que cada extensión E_{i+1}/E_i es una extensión de grado primo s. Supongamos que F sobre $\mathbb{F}_q$ es un cuerpo de funciones tal que F/E_0 es una extensión de Galois finita y que $F \not\subseteq E_i$ para cada $i \geq 0$. Supongamos que los géneros de E_1 y F satisfacen que $g(E_1) > g(F)$ y que $\mathbb{F}_q$ es el cuerpo total de constantes de F y de cada E_i. Entonces $\mathcal{E}$ y F son linealmente disjuntos sobre E_0.*

Demostración. Sea i un entero positivo. Dado que F/E_0 es una extensión de Galois finita, la Proposición 1.21 afirma que E_i y F son cuerpos linealmente disjuntos sobre E_0 si y sólo si

$$E_i \cap F = E_0.$$

Como $F \not\subseteq E_i$ para cada $i \geq 0$ entonces $E_i \cap F \neq F$. Ahora, puesto que $[E_i : E_0] = s^i$ con s primo y $E_0 \subseteq E_i \cap F \subseteq E_i$ entonces $E_l = E_i \cap F$ para algún $0 \leq l \leq i$. Por otra parte, como $E_l = E_i \cap F \subsetneq F$ entonces por la fórmula del género de Hurwitz, Teorema 1.8, tenemos que $g(E_l) \leq g(F)$. Además, por hipótesis $g(F) < g(E_1)$, luego,

$$g(E_l) \leq g(F) < g(E_1).$$

Si $0 < l \leq i$ entonces $g(E_l) < g(E_1)$, lo cual es una contradicción. Por lo tanto, $l = 0$, es decir, $E_i \cap F = E_0$. □

Proposición 3.19. *Sean $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ y $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sucesiones recursivas no triviales sobre $\mathbb{F}_q$ tales que $\mathbb{F}_q$ es el cuerpo total de constantes de cada E_i y cada F_i. Supongamos que F_0/E_0 es una extensión de Galois finita, que $F_0 \not\subseteq E_i$ para cada $i \geq 0$, que $\mathcal{E}$ es una subsucesión propia de $\mathcal{F}$ y que*

$$[E_{i+1} : E_i] = [F_{i+1} : F_i] = s,$$

donde s un número primo. Si $g(E_1) > 0$ entonces $\mathcal{F}$ es la composición de $\mathcal{E}$ con F_0.

Demostración. Por hipótesis F_0/E_0 es una extensión de Galois finita, $F_0 \not\subseteq E_i$ para cada $i \geq 1$, cada extensión E_{i+1}/E_i es de grado primo y $g(E_1) > 0 = g(F_0)$. Entonces por la Proposición 3.18 tenemos, para $i \geq 1$, que E_i y F_0 son cuerpos linealmente disjuntos sobre E_0. Por lo tanto, para $i \geq 1$ se tiene que

$$[E_iF_0 : F_0] = [E_i : E_0] = s^i.$$

Finalmente, como $F_0 \subseteq E_iF_0 \subseteq F_i$ y por hipótesis $[F_i : F_0] = s^i$ con s primo, concluimos que $E_iF_0 = F_i$ para $i \geq 1$, es decir, $\mathcal{F}$ es la composición de $\mathcal{E}$ con F_0. □

A continuación definiremos el concepto de composición de dos torres de cuerpos de funciones.

Sean $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ y $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ torres de cuerpos de funciones sobre $\mathbb{F}_q$ tales que $E_0 = F_0$. Se define la **composición** de $\mathcal{E}$ y $\mathcal{F}$ (sobre E_0) como la sucesión de cuerpos de funciones $\mathcal{EF} := \{M_i\}_{i=0}^{\infty}$, con $M_0 = E_0$ y $M_i := E_iF_i$ para cada $i \geq 1$.

Observación 3.20. Como consecuencia inmediata de la definición de la composición $\mathcal{EF} = \{M_i\}_{i=0}^{\infty}$ de dos torres $\mathcal{E}$ y $\mathcal{F}$ sobre $\mathbb{F}_q$ se tienen las siguientes propiedades:

i. $M_i \subseteq M_{i+1}$ *para cada* $i \geq 0$.

ii. M_{i+1}/M_i *es una extensión separable para cada* $i \geq 0$.

iii. $g(M_i) \to \infty$ *si* $i \to \infty$.

iv. $\mathcal{E}$ *y* $\mathcal{F}$ *son subsucesiones de* $\mathcal{M}$.

Sean $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ y $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ torres de cuerpos de funciones sobre $\mathbb{F}_q$. Diremos que las torres $\mathcal{E}$ y $\mathcal{F}$ son **linealmente disjuntas** sobre E_0 si $E_0 = F_0$ y para cada $i \geq 1$ los cuerpos de funciones E_i y F_i son linealmente disjuntos sobre E_0.

Proposición 3.21. *Sean* $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ *y* $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *torres sobre* $\mathbb{F}_q$ *linealmente disjuntas sobre* E_0. *Supongamos que la intersección* $\mathcal{S}(\mathcal{F}) \cap \mathcal{S}(\mathcal{E})$ *de los espacios de ramificación de* $\mathcal{E}$ *y* $\mathcal{F}$ *es un conjunto no vacío, entonces* $\mathcal{EF}$ *es una torre sobre* $\mathbb{F}_q$ *con tasa de descomposición positiva. Además, el género de* $\mathcal{EF}$ *satisface la desigualdad*

$$\gamma(\mathcal{EF}) \leq \gamma(\mathcal{E}) + \gamma(\mathcal{F}) + 1$$

y el límite de la torre $\mathcal{EF}$ *cumple que*

$$\lambda(\mathcal{EF}) \geq \frac{|\mathcal{S}(\mathcal{F}) \cap \mathcal{S}(\mathcal{E})|}{\gamma(\mathcal{E}) + \gamma(\mathcal{F}) + 1}.$$

En particular, si $\mathcal{E}$ y $\mathcal{F}$ tienen género finito entonces $\mathcal{EF}$ es una torre asintóticamente buena.

Demostración. Sea $P \in \mathcal{S}(\mathcal{F}) \cap \mathcal{S}(\mathcal{E})$ entonces P es un lugar racional de E_0 que se descompone completamente en E_i/E_0 y en F_i/E_0 para cada $i \geq 1$, así que la Proposición 1.6 asegura que el lugar P se descompone completamente en M_i/E_0 para cada $i \geq 1$. De este hecho se sigue que $\mathbb{F}_q$ es el cuerpo total de constantes de cada M_i y P se descompone completamente en la torre $\mathcal{EF}$. En particular tenemos que

$$\mathcal{S}(\mathcal{F}) \cap \mathcal{S}(\mathcal{E}) \subseteq \mathcal{S}(\mathcal{EF})$$

y el Teorema 1.24 implica que

$$\nu(\mathcal{EF}) \geq |\mathcal{S}(\mathcal{EF})| \geq |\mathcal{S}(\mathcal{F}) \cap \mathcal{S}(\mathcal{E})|.$$

Veamos la cota para el género de $\mathcal{EF}$. Para cada $i \geq 1$ tenemos que M_i es la composición de los cuerpos de funciones E_i y F_i, entonces por la desigualdad de Castelnuovo, Proposición 1.7, tenemos que

$$g(M_i) \leq g(E_i)[M_i : E_i] + g(F_i)[M_i : F_i] + [M_i : E_i][M_i : F_i].$$

Por otra parte, dado que

$$[M_i : E_0] = [M_i : E_i][E_i : E_0] = [M_i : F_i][F_i : E_0]$$

entonces

$$\frac{g(M_i)}{[M_i : E_0]} \leq \frac{g(E_i)}{[E_i : E_0]} + \frac{g(F_i)}{[F_i : E_0]} + 1,$$

luego,

$$\gamma(\mathcal{EF}) \leq \gamma(\mathcal{E}) + \gamma(\mathcal{F}) + 1.$$

Claramente tenemos la siguiente cota para el límite de $\mathcal{EF}$

$$\lambda(\mathcal{EF}) = \frac{\nu(\mathcal{EF})}{\gamma(\mathcal{EF})} \geq \frac{|\mathcal{S}(\mathcal{F}) \cap \mathcal{S}(\mathcal{E})|}{\gamma(\mathcal{E}) + \gamma(\mathcal{F}) + 1}.$$

□

3.3. Sobre el espacio de descomposición de sucesiones recursivas

El espacio de descomposición de una torre de cuerpos de funciones definida de forma recursiva juega un papel vital en el estudio de su comportamiento asintótico, pues

si dicho espacio es no vacío entonces la torre tiene tasa de descomposición positiva (Teorema 1.24). Hasta el momento no se conocen torres recursivas asintóticamente buenas con espacio de descomposición vacío. De allí la relevancia de dar condiciones que garanticen que una sucesión no trivial de cuerpos de funciones tenga espacio de descomposición no vacío.
A lo largo de esta sección el símbolo Z_f denotará el conjunto de ceros en $\overline{\mathbb{F}}_q$ de una función racional $f \in \mathbb{F}_q(T)$.

Teorema 3.22. *[8, Teorema 2.1] Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ una (a,b)-sucesión de cuerpos de funciones, con $a(T) = a_1(T)/a_2(T)$, tal que $\mathbb{F}_q$ es el cuerpo total de constantes para cada $i \geq 0$. Supongamos que existe una función racional $\phi(T) \in \mathbb{F}_q(T)$ y que se cumplen las siguientes condiciones:*

i. $\mathrm{Z}_{a_1} \cap \mathrm{Z}_{a_2} = \emptyset$.

ii. $\mathrm{Z}_{\phi \circ a} \subseteq \mathbb{F}_q$.

iii. $\mathrm{Z}_{\phi \circ a} \subseteq \mathrm{Z}_{\phi \circ b}$.

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

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

Entonces para todo $\gamma \in \mathrm{Z}_{\phi \circ a}$, *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*

$$|\mathcal{S}(\mathcal{F})| \geq |\,\mathrm{Z}_{\phi \circ a}\,|.$$

En particular,

$$g(F_i) \to \infty \quad \textit{cuando} \quad i \to \infty \qquad y \qquad N(F_i) \geq \deg(a)^i |\,\mathrm{Z}_{\phi \circ a}\,|.$$

A continuación veremos que el teorema anterior se puede generalizar modificando la hipótesis *iv*. Observemos que dicha hipótesis implica que $[F_{i+1} : F_i] = \deg a$ para cada $i \geq 0$. Sin embargo, lo que en general cumple una (a,b)-sucesión no trivial $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ es que $[F_{i+1} : F_i] \leq \deg a$ para cada $i \geq 0$. Si existe un entero no negativo j tal que $[F_{i+1} : F_i] < \deg a$ para cada $i \geq j$ diremos que la (a,b)-sucesión $\mathcal{F}$ es **reducible**.

Sean $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una (a,b)-sucesión reducible no trivial sobre $\mathbb{F}_q$ tal que cada extensión F_{i+i}/F_i está definida por el polinomio separable

$$\rho_{i+1}(T) := a_1(T) - a_2(T)b(x_i),$$

donde $\rho_{i+1}(T)$ es un polinomio reducible para cada $i \geq j$ y j es un entero no negativo, y denotemos por $\varphi_{i+1}(T) \in F_i[T]$ al polinomio minimal de x_{i+1} sobre F_i. Supongamos también que para cada $i \geq j$

$$r = \deg \varphi_{i+1} = [F_{i+1} : F_i] < \deg a \qquad \text{y} \qquad \rho_{i+1}(T) = \varphi_{i+1}(T)\eta_{i+1}(T)$$

para algún $\eta_{i+1}(T) \in F_i[T]$ de grado mayor que uno.

Teorema 3.23. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ es una sucesión (a,b)-recursiva no trivial como la descrita anteriormente. Si existe $\phi(t) \in \mathbb{F}_q(t)$ tal que se cumple que:*

i. $\mathrm{Z}_{\phi\circ a} \subseteq \mathbb{F}_q$.

ii. $\mathrm{Z}_{\phi\circ a} \subseteq \mathrm{Z}_{\phi\circ b}$.

iii. Para cada $\alpha \in \mathrm{Z}_{\phi\circ a}$ existe un lugar racional $P_\alpha \in \mathbb{P}(F_j)$ tal que el polinomio $\rho_\alpha(T) := \rho_{i+1}(T) \mod P_\alpha \in \mathbb{F}_q[T]$ es separable de grado $\deg a$.

Entonces $\mathcal{F}$ es una torre sobre $\mathbb{F}_q$ con espacio de descomposición $\mathcal{S}_j(\mathcal{F})$ no vacío y tasa de descomposición positiva, además, $\nu(\mathcal{F})$ satisface la siguiente estimación

$$\nu(\mathcal{F}) \geq |\mathcal{S}_j(\mathcal{F})| \geq \frac{|\,\mathrm{Z}_{\phi\circ a}\,|}{[F_j : F_0]}.$$

Demostración. Probaremos que $\{P_\alpha \in \mathbb{P}(F_j) : \alpha \in \mathrm{Z}_{\phi\circ a}\} \subseteq \mathcal{S}_j(\mathcal{F})$. Consideremos el lugar racional $P_\alpha \in \mathbb{P}(F_j)$ donde $\alpha \in \mathrm{Z}_{\phi\circ a}$. Dado que el polinomio minimal de x_{j+1} sobre F_j es $\varphi_{j+1}(T)$ y $\rho_{j+1}(T) = \varphi_{j+1}(T)\eta_{j+1}(T)$ para algún $\eta_{j+1}(T) \in F_{j+1}[T]$ entonces la condición iii implica que $\varphi_\alpha(T) := \varphi_{j+1}(T) \mod P_\alpha \in \mathbb{F}_q[T]$ es un polinomio separable, así que $\varphi_\alpha(T)$ tiene $r = \deg \varphi_\alpha = \deg \varphi_{j+1}$ raíces distintas en $\overline{\mathbb{F}}_q$, llamémoslas $\beta_1, \ldots, \beta_r$. Dado que $\rho_\alpha(\beta_i) = \varphi_\alpha(\beta_i)\eta_\alpha(\beta_i) = 0$ entonces $a(\beta_i) = b(\alpha)$. Por otra parte, la condición ii implica que $\alpha \in \mathrm{Z}_{\phi\circ b}$, por lo tanto,

$$\phi(a(\beta_i)) = \phi(b(\alpha)) = 0,$$

es decir, $\beta_i \in \mathrm{Z}_{\phi\circ a}$. Finalmente, de la condición i, se sigue que $\beta_i \in \mathbb{F}_q$. Hemos probado que el polinomio $\varphi_\alpha(T)$ tiene todas sus raíces en $\mathbb{F}_q$, luego por el Teorema de Kummer (Teorema 1.16) existen $Q_1, \ldots, Q_r$ lugares racionales arriba de P_α tales

que $x_{j+1}(Q_i) = \beta_i$ para $i = 1, \ldots, r$, es decir, que P_α se descompone completamente en F_{j+1}/F_j. Ahora procedamos por inducción. Supongamos que el lugar P_α de F_j se descompone completamente en la extensión F_n/F_j para $n > j$, es decir, que existen $k := [F_n : F_j]$ lugares racionales arriba de P_α denotados por $Q_{\alpha,1}, \ldots, Q_{\alpha,k}$ que satisfacen $x_n(Q_{\alpha,i}) = \gamma_i$ para algún $\gamma_i \in \mathrm{Z}_{\phi\circ a}$. Veamos que los lugares $Q_{\alpha,i}$ se descomponen completamente en F_{n+1}/F_n. Sean $Q = Q_{\alpha,i}$ y $\gamma = \gamma_i$ para algún $1 \leq i \leq k$. Por la condición iii tenemos que el polinomio

$$\rho_\gamma(T) = \varphi_\gamma(T)\eta_\gamma(T)$$

es separable, por lo tanto, $\varphi_\gamma(T)$ tiene r raíces distintas en $\overline{\mathbb{F}}_q$ y las denotaremos por $\theta_1, \ldots, \theta_r$. Dado que $\rho_\gamma(\theta_l) = \varphi_\gamma(\theta_l)\eta_\gamma(\theta_l) = 0$ entonces $a(\theta_l) = b(\gamma)$, luego por la condición ii

$$\phi(a(\theta_l)) = \phi(b(\gamma)) = 0,$$

por lo tanto, $\theta_l \in \mathrm{Z}_{\phi\circ a}$ y del inciso i concluimos que $\theta_l \in \mathbb{F}_q$. Hemos probado que cada polinomio $\varphi_{\gamma_i}(T)$ tiene todas sus raíces en $\mathbb{F}_q$, luego por el Teorema de Kummer cada lugar $Q_{\alpha,i}$ se descompone completamente en la extensión F_{n+1}/F_n, esto es, existen

$$R_{\alpha,i,1}, \ldots, R_{\alpha,i,r}$$

lugares racionales arriba de $Q_{\alpha,i}$ tales que $x_{n+1}(R_{\alpha,i,l}) = \theta_l$ para $l = 1, \ldots, r$. Finalmente, concluimos que el lugar P_α se descompone completamente en la torre, luego

$$\mathcal{S}_j(\mathcal{F}) \supseteq \{P_\alpha \in \mathbb{P}(F_j) : \alpha \in \mathrm{Z}_{\phi\circ a}\},$$

y por el Teorema 1.24 tenemos que

$$\nu(\mathcal{F}) \geq \frac{|\mathcal{S}_j(\mathcal{F})|}{[F_j : F_0]} \geq \frac{|\,\mathrm{Z}_{\phi\circ a}\,|}{[F_j : F_0]}.$$

En particular, $N(F_i) \to \infty$ cuando $i \to \infty$ luego por la cota de Hasse-Weil se tiene que $g(F_i) \to \infty$ cuando $i \to \infty$, además, la existencia de al menos un lugar racional en cada F_i garantiza que $\mathbb{F}_q$ es el cuerpo total de constantes de F_i para cada $i \geq 0$. □

A continuación presentaremos algunos ejemplos.

Ejemplo 3.24. Consideremos la sucesión de cuerpos de funciones $\mathcal{S} = \{G_i\}_{i=0}^{\infty}$

sobre $\mathbb{F}_9$ definida de forma recursiva por la ecuación

$$\frac{y^4-y}{y+1} = -\frac{x+2}{x^4+x}. \tag{3.13}$$

En este caso el polinomio que define la sucesión $\mathcal{S}$ es

$$\rho(T) = T^4 - T + (T+1)\frac{x+2}{x^4+x} = T^4 - \frac{x^4+1}{x^4+x}T + \frac{x+2}{x^4+x}.$$

Puesto que $\rho(\frac{x-1}{x+1}) = 0$ entonces $\rho(T) = \varphi(T)\eta(T)$ con $\eta(T) = T - \frac{x-1}{x+1}$ y

$$\varphi(y) = y^3 + \frac{x+2}{x+1}y^2 + \left(\frac{x+2}{x+1}\right)^2 y + \frac{2}{x(x+1)^2} = 0. \tag{3.14}$$

Podemos reescribir la ecuación anterior como

$$(y+2)^3 + \frac{x+2}{x+1}(y+2)^2 + \frac{x+2}{(x+1)^2}(y+2) + \frac{x+2}{x(x+1)^2} = 0,$$

luego, un polinomio que se anula en $y+2$ y define la sucesión $\mathcal{S}$ es

$$\hat{\varphi}(T) = T^3 + \frac{x+2}{x+1}T^2 + \frac{x+2}{(x+1)^2}T + \frac{x+2}{x(x+1)^2}.$$

Para probar que $\mathcal{S}$ es una sucesión no trivial de cuerpos de funciones es suficiente mostrar que existe un lugar totalmente ramificado en cada extensión F_{i+1}/F_i. En efecto, si denotamos por P_1 el cero simple de x_0+2 en F_0 entonces, por el criterio de Eisenstein (Proposición 1.15),

$$\hat{\varphi}_1(T) := T^3 + \frac{x_0+2}{x_0+1}T^2 + \frac{x_0+2}{(x_0+1)^2}T + \frac{x_0+2}{x_0(x_0+1)^2}$$

es un polinomio irreducible sobre F_0, P_1 es totalmente ramificado y existe un único lugar que es un polo simple de x_1+2. Usando inductivamente este argumento se prueba que el lugar P_1 es totalmente ramificado en $\mathcal{S}$, lo que implica que $\mathcal{S}$ es una sucesión no trivial de cuerpos de funciones. En particular, este resultado muestra que el polinomio

$$\varphi_{i+1}(T) := T^3 + \frac{x_i+2}{x_i+1}T^2 + \left(\frac{x_i+2}{x_i+1}\right)^2 T + \frac{2}{x_i(x_i+1)^2} \in F_i[T],$$

que define cada extensión F_{i+1}/F_i, es irreducible para $i \geq 0$. Ahora, veamos que la sucesión $\mathcal{S}$ satisface las demás hipótesis requeridas en el Teorema 3.23. Consideremos

las funciones racionales

$$a(T) = \frac{T^4 - T}{T+1}, \quad b(T) = -\frac{T+2}{T^4+T}, \quad \text{y} \quad \phi(T) = T+1.$$

Entonces

$$\phi(a(T)) = \frac{T^4+1}{T+1} \qquad \text{y} \qquad \phi(b(T)) = \frac{T^4+1}{T^4+T},$$

lo que implica que $\mathrm{Z}_{\phi\circ a} = \mathrm{Z}_{\phi\circ b}$. Es fácil ver que $\mathrm{Z}_{\phi\circ a} \subseteq \mathbb{F}_9$. En efecto, dado $\alpha \in \overline{\mathbb{F}}_9$ tal que $\alpha^4 + 1 = 0$ se tiene que $\alpha^8 = (\alpha^4)^2 = (-1)^2 = 1$, luego $\alpha^9 = \alpha$. Finalmente, para cada $\alpha \in \mathrm{Z}_{\phi\circ a}$ tenemos un lugar racional P_α en $\mathbb{F}_9(x_0)$ y el polinomio

$$\rho_\alpha(T) = \rho(T) \mod P_\alpha = T^4 - \frac{\alpha^4+1}{\alpha^4+\alpha}T + \frac{\alpha+2}{\alpha^4+\alpha} = T^4 + 1$$

es separable y de grado cuatro, por lo tanto, $\mathcal{S}$ es una torre sobre $\mathbb{F}_9$ y su tasa de descomposición satisface $\nu(\mathcal{S}) \geq |\,\mathrm{Z}_{\phi\circ a}\,| = 4$.

Ejemplo 3.25. Consideremos nuevamente la torre $\mathcal{F}_4 = \{H_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_{q^3}$ definida de forma recursiva por la ecuación

$$y^{q+1} + y = \frac{x+1}{x^{q+1}}. \tag{3.15}$$

En este caso el polinomio que define la sucesión $\mathcal{F}_4$ es el polinomio separable

$$\rho(T) = T^{q+1} + T - \frac{x+1}{x^{q+1}}.$$

Dado que $-(x+1)/x$ es una raíz del polinomio $\rho(T)$ entonces

$$\rho(T) = \left(\sum_{j=1}^{q} \left(-\frac{x+1}{x}\right)^{q-j} T^j - \frac{1}{x^q}\right)\left(T + \frac{x+1}{x}\right) := \varphi(T)\eta(T),$$

y dado que $\rho(y) = 0$ se tiene que

$$\varphi(y) = \sum_{j=1}^{q} \left(-\frac{x+1}{x}\right)^{q-j} y^j - \frac{1}{x^q} = 0.$$

Ahora probaremos, para cada $i \geq 0$, que el polinomio

$$\varphi_{i+1}(T) := \sum_{j=1}^{q} \left(-\frac{x_i+1}{x_i}\right)^{q-j} T^j - \frac{1}{x_i^q} \in F_i[T]$$

que define cada extensión F_{i+1}/F_i es irreducible. Puesto que $\varphi_{i+1}(x_{i+1}) = 0$ entonces

$$(x_{i+1}+1)^q + \sum_{j=1}^{q-1} \frac{x_i+1}{(-x_i)^{q-j}}(x_{i+1}+1)^j - \frac{x_i+1}{x_i^q} = 0,$$

es decir, $x_{i+1}+1$ es una raíz del polinomio

$$\hat{\varphi}_{i+1}(T) := T^q + \sum_{j=1}^{q-1} \frac{x_i+1}{(-x_i)^{q-j}}T^j - \frac{x_i+1}{x_i^q} \in F_i[T].$$

Consideremos el cero simple Q_{-1}^0 de x_0+1 en F_0. Puesto que

$$\nu_{Q_{-1}^0}(1) = 0 \qquad \text{y} \qquad \nu_{Q_{-1}^0}\left(\frac{x_0+1}{(-x_0)^{q-j}}\right) = \nu_{Q_{-1}^0}\left(\frac{x_0+1}{x_0^q}\right) = 1$$

entonces por el criterio de Eisenstein existe un único lugar Q_{-1}^1 en F_1 que es un cero simple de x_1+1, además, $e(Q_{-1}^1|Q_{-1}^0) = q$. Usando el argumento anterior se prueba por inducción que el lugar Q_{-1}^0 es totalmente ramificado en la sucesión $\mathcal{F}_4$. En particular, $\mathcal{F}_4$ es una sucesión no trivial y el polinomio φ_{i+1} es irreducible sobre F_i para cada $i \geq 0$, como se quería probar. Ahora, veamos que se satisfacen el resto de condiciones pedidas en el Teorema 3.23. Consideremos las funciones racionales

$$a(T) = T^{q+1} + T, \quad b(T) = \frac{T+1}{T^{q+1}} \quad \text{y} \quad \phi(T) = T+1$$

luego

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

La condición ii se cumple trivialmente. Mostremos que se satisface i. Sea $\alpha \in \mathrm{Z}_{\phi\circ a}$ entonces $\alpha^{q+1} + \alpha + 1 = 0$, luego

$$\alpha^{q^3-1} = (\alpha^{q^2+q+1})^{q-1} = (\alpha^{q^2+q}\cdot\alpha)^{q-1} = ((-\alpha-1)^q\cdot\alpha)^{q-1} = 1^{q-1} = 1.$$

Por último, mostremos que se cumple la condición iii. En este caso $j=0$. Para cada $\alpha \in \mathrm{Z}_{\phi\circ a}$ consideremos el lugar racional P_α de $\mathbb{P}(x_0)$. Claramente el polinomio

$$\rho_\alpha(T) = T^{q+1} + T - \frac{\alpha+1}{\alpha^{q+1}} = T^{q+1} + T + 1$$

se separable y de grado $\deg \rho(T) = q+1$. De todo lo anterior concluimos que $\mathcal{F}_4$ es una torre con espacio de descomposición no vacío sobre F_0 y que su tasa de descomposición satisface

$$\nu(\mathcal{F}) \geq |\,\mathrm{Z}_{\phi\circ a}\,| = q+1.$$

En general, no es fácil determinar si una ecuación define una sucesión no recursiva de cuerpos de funciones, como vimos en los ejemplos anteriores. Para finalizar esta sección daremos algunos criterios para probar que ciertas ecuaciones definen sucesiones recursivas no triviales.

Proposición 3.26. *Sean $a(T), b_1(T), b_2(T)$ polinomios con coeficientes sobre $\mathbb{F}_q$ tales que:*

i. $a'(T) \neq 0$,

ii. $b_1(T)$ *y* $b_2(T)$ *son polinomios coprimos y*

iii. $k := \deg(b_1(T)) - \deg(b_2(T)) > 0$.

Consideremos la sucesión de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ definida recursivamente por la ecuación

$$a(y) = b(x) := \frac{b_1(x)}{b_2(x)}.$$

Supongamos, además, que existe un lugar $P \in \mathbb{P}(F_0)$ que cumple la condición

$$\nu_P(b(x_0)) < 0 \qquad y \qquad (k \cdot \nu_P(b(x_0)), \deg a) = 1. \tag{3.16}$$

Entonces P es un lugar totalmente ramificado en la torre; en particular, $\mathcal{F}$ es una sucesión no trivial sobre $\mathbb{F}_q$ tal que para cada $i \geq 0$ la extensión F_{i+1}/F_i es separable y $\mathbb{F}_q$ es el cuerpo total de constantes de F_i.

Demostración. Es suficiente mostrar que P es totalmente ramificado en la extensión F_i/F_0 para cada $i \geq 0$. Sean $n := \deg a$ y $Q_1 \in \mathbb{P}(F_1)$ un lugar arriba de P. Dado que P es un polo de $b(x_0)$ y $\nu_{Q_1}(a(x_1)) = e(Q_1|P)\nu_P(b(x_0))$ entonces Q_1 es un polo de $a(x_1)$, luego por la desigualdad triangular estricta tenemos que

$$n\nu_{Q_1}(x_1) = \nu_{Q_1}(a(x_1)) = e(Q_1|P)\nu_P(b(x_0)). \tag{3.17}$$

Ahora, la hipótesis $(k \cdot \nu_P(b(x_0)), n) = 1$ y la igualdad (3.17) implican que n divide a $e(Q_1|P)$. Por otra parte, es bien sabido que $e(Q_1|P) \leq [F_1 : F_0] \leq \deg a = n$, por lo tanto, P es totalmente ramificado en F_1/F_0, $\mathbb{F}_q$ es el cuerpo total de constantes de F_1 y el polinomio $\varphi_1(T) := a(T) - b(x_0)$ es irreducible sobre F_0; además, la hipótesis $a'(T) \neq 0$ garantiza que $\varphi_1(T)$ es separable. De la igualdad (3.17) también se deduce que Q_1 es un polo de x_1, por lo tanto,

$$\nu_{Q_1}(b(x_1)) = \deg b_1 \cdot \nu_{Q_1}(x_1) - \deg b_2 \cdot \nu_{Q_1}(x_1) = k \cdot \nu_P(b(x_0)). \tag{3.18}$$

Ahora, para $i > 0$, supongamos que existe un lugar $Q_i \in \mathbb{P}(F_i)$ arriba de P tal que

$$e(Q_i|P) = [F_i : F_0] = n^i \qquad \text{y} \qquad \nu_{Q_i}(x_i) = k^{i-1} \cdot \nu_P(b(x_0)).$$

Sea Q_{i+1} un lugar de F_{i+1} que cae sobre Q_i. Dado que $k^{i-1} \cdot \nu_P(b(x_0)) < 0$ se sigue que Q_i es un polo de x_i, además, por un argumento similar al dado en (3.18) tenemos que

$$\nu_{Q_i}(b(x_i)) = k \cdot \nu_{Q_i}(x_i) = k^i \cdot \nu_P(b(x_0))$$

y

$$\nu_{Q_{i+1}}(a(x_{i+1})) = e(Q_{i+1}|Q_i)\nu_{Q_i}(b(x_i)) = e(Q_{i+1}|Q_i)k^i\nu_P(b(x_0)).$$

Por lo tanto, Q_{i+1} es un polo de x_1 y se cumple que

$$n\nu_{Q_{i+1}}(x_{i+1}) = \nu_{Q_{i+1}}(a(x_{i+1})) = e(Q_{i+1}|Q_i)\nu_P(b(x_0))k^i.$$

Finalmente, la hipótesis $(k\nu_P(b(x_0)), n) = 1$ implica que

$$e(Q_{i+1}|Q_i) = [F_{i+1} : F_i] = n \qquad \text{y} \qquad \nu_{Q_{i+1}}(x_{i+1}) = k^i \cdot \nu_P(b(x_0)),$$

por consiguiente, P es totalmente ramificado en la extensión F_{i+1}/F_0, $\mathbb{F}_q$ es el cuerpo total de constantes de $\mathcal{F}_{i+1}$ y $\varphi_{i+1}(T) = a(T) - b(x_i)$ es irreducible sobre F_i y como $\varphi'_{i+1}(T) = a'(T) \neq 0$ concluimos que la extensión F_{i+1}/F_i es separable. □

Corolario 3.27. *Sean $b_1, b_2 \in \mathbb{F}_q[T]$ polinomios coprimos tales que $k := \deg b_1 - \deg b_2 > 0$. Sea $a(T)$ un polinomio aditivo y separable tal que $\mathbb{F}_q$ es el cuerpo de descomposición de $a(T)$ y consideremos la sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ definida por la ecuación $a(y) = b(x) := \frac{b_1(x)}{b_2(x)}$. Si existen al menos dos lugares en F_0 que cumplen la condición (3.16) entonces $\mathcal{F}$ es una torre de tipo Artin-Schreier.*

Demostración. Para ver que $\mathcal{F}$ es una torre sobre $\mathbb{F}_q$ resta probar que existe F_j tal que $g(F_j) > 2$. Sean P_1, P_2 los lugares de F_0 que satisfacen la condición (3.16). Por la Proposición 3.26 tenemos que P_1 y P_2 son totalmente ramificados en la extensión F_1/F_0, luego el Teorema 1.18 implica que

$$d(Q_i|P_i) = (m_{P_i} + 1)(\deg a - 1),$$

donde m_{P_i} son enteros no negativos y Q_i denota el único lugar en F_2 arriba de P_i.

Ahora, por la fórmula del género de Hurtwiz se sigue que

$$g(F_1) \geq 1 + (g(F_0) - 1) \deg a + \frac{1}{2} \sum_{i=1}^{2} d(Q_i|P_i) \geq 1 - \deg a + 2(\deg a - 1) \geq \deg a - 1.$$

Si $\deg a > 2$ concluimos que $g(F_1) > 1$. En caso de que $\deg a = 2$ y $g(F_1) = 1$, con un argumento similar al anterior, se prueba que $g(F_2) \geq 2$ puesto que Q_1 y Q_2 son lugares totalmente ramificados en F_2/F_1. De todo lo anterior concluimos que $\mathcal{F}$ es una torre. □

A continuación mostramos algunos ejemplos de sucesiones de tipo Artin-Schreier, estudiados previamente de manera independiente, que satisfacen el corolario anterior y el Teorema 3.22, por lo que resultan ser torres con tasa de descomposición positiva.

Ejemplo 3.28. *Consideremos nuevamente la sucesión $\mathcal{F}_1$ sobre $\mathbb{F}_{q^2}$ definida por la ecuación*

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

En este caso $k = 1$ y los lugares que satisfacen la condición (3.16) son P_α con $\alpha^{q-1} = -1$ y P_∞. La función racional requerida en el Teorema 3.22 es $\phi(T) = \frac{1-T^{q-1}}{T}$.

Ejemplo 3.29. *Consideremos nuevamente la sucesión $\mathcal{F}_5$ sobre $\mathbb{F}_8$ definida por la ecuación*

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

En este caso $k = 1$ y los lugares que satisfacen la condición (3.16) son P_∞ y P_0. La función racional requerida en el Teorema 3.22 es $\phi(T) = T^3 + T + 1$.

Ejemplo 3.30. *Sea $\mathcal{F}_6$ sobre $\mathbb{F}_{q^p}$ la sucesión definida por la ecuación*

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

En este caso $k = q - 1$ y los lugares que satisfacen la condición (3.16) son P_∞, P_1. La función racional requerida en el Teorema 3.22 es $\phi(T) = T + 1$.

Proposición 3.31. *Consideremos la sucesión recursiva de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ definida por la ecuación*

$$y^{m+1} + (h(x) - g(x)^m)\, y = h(x)g(x), \tag{3.19}$$

donde m una potencia de $\operatorname{Car}\mathbb{F}_q$ *y*

$$g(T) = \frac{T-\gamma}{\alpha T-\beta}, \qquad h(T) = \frac{(T-\gamma)^j}{h_2(T)} - \gamma,$$

funciones racionales en $\mathbb{F}_q(T)$ tales que $\alpha, \beta, \gamma \in \mathbb{F}_q$ y $\gamma \neq 0$, j es un entero positivo fijo tal que $1 < j \leq m$ y $T-\gamma$ es coprimo a $\alpha T-\beta$ y a $h_2(T)$. Entonces el cero simple P_γ de $x_0-\gamma$ de $\mathbb{P}(F_0)$ es totalmente ramificado en $\mathcal{F}$, F_{i+1}/F_i es de grado m y $\mathbb{F}_q$ es el cuerpo total de constantes de F_i para cada $i \geq 0$. En particular, $\mathcal{F}$ es una sucesión no trivial de cuerpos de funciones.

Demostración. El polinomio que define la sucesión $\mathcal{F}$ es

$$\phi(T) = T^{m+1} + \left(h(x) - g(x)^m\right) T - h(x)g(x).$$

Puesto que $\phi(g(x)) = 0$ entonces $\phi(T) = \varphi(T)(T-g(x))$ donde

$$\varphi(T) = T^m + g(x)T^{m-1} + g(x)^2T^{m-2} + \cdots + g(x)^{m-1}T + h(x) \tag{3.20}$$

además, $\varphi(y) = 0$, por lo que tenemos una forma alternativa de definir la sucesión $\mathcal{F}$ y será de gran utilidad en la prueba. Ahora, sea Q un lugar de F_1 arriba de P_γ y probemos que P_γ es totalmente ramificado en F_1/F_0. Puesto que la extensión F_1/F_0 está definida por la ecuación

$$x_1^{m+1} + \left(h(x_0) - g(x_0)^m\right) x_1 = h(x_0)g(x_0) \tag{3.21}$$

y

$$\nu_{P_\gamma}(h(x_0)g(x_0)) = 1, \quad \nu_{P_\gamma}(h(x_0)+\gamma) = j, \quad \nu_{P_\gamma}(g(x_0)^m) = m$$

entonces

$$\nu_Q(x_1) + \nu_Q(x_1^m + (h(x_0) - g(x_0)^m)) = e(Q|P_\gamma).$$

Mostremos que $\nu_Q(x_1) = 0$. Si $\nu_Q(x_1) < 0$ la desigualdad triangular estricta implica que $\nu_Q(x_1^m + (h(x_0) - g(x_0)^m)) = m\nu_Q(x_1)$, luego

$$(m+1)\nu_Q(x_1) = \nu_Q(x_1) + \nu_Q(x_1^m + h(x_0) - g(x_0)^m) = e(Q|P_\gamma), \tag{3.22}$$

lo cual es una contradicción. Si $\nu_Q(x_1) > 0$ entonces, para cada $0 \leq i \leq m-1$, tenemos que

$$\nu_Q(g(x_0)^i x_1^{m-i}) = i\nu_Q(g(x_0)) + (m-i)\nu_Q(x_1) > 0.$$

Por (3.20) tenemos que

$$x_1^m + g(x_0)x_1^{m-1} + g(x_0)^2x_1^{m-2} + \cdots + g(x_0)^{m-1}x_1 + h(x_0) = 0;$$

dado que $\nu_Q(h(x_0)) = 0$ entonces la desigualdad triangular estricta implica que

$$m\nu_Q(x_1) = \nu_Q(-g(x_0)x_1^{m-1} - g(x_0)^2y^{m-2} - \cdots - g(x_0)^{m-1}x_1 - h(x_0)) = 0$$

lo cual es una contradicción. Luego, $\nu_Q(x_1) = 0$ y $\nu_Q(g(x_0)^i x_1^{m-i}) = ie(Q|P_\gamma)$ con $1 \leq i \leq m$. Ahora, sumando $-\gamma$ a ambos lados de la ecuación (3.22) obtenemos

$$(x_1 - \gamma)^m = -g(x_0)x_1^{m-1} - g(x_0)^2x_1^{m-2} - \cdots + g(x_0)^{m-1}x_1 - (h(x_0) + \gamma). \quad (3.23)$$

Nuevamente por la desigualdad triangular estricta tenemos que la valuación en el lugar Q del lado derecho de la igualdad (3.23) es $\nu_Q(g(x_0)) = e(Q|P_\gamma)$ pues $\nu_Q(h(x_0) + \gamma) = je(Q|P_\gamma) > e(Q|P_\gamma) = \nu_Q(g(x_0))$. Por lo tanto,

$$m\nu_Q(x_1 - \gamma) = e(Q|P_\gamma),$$

lo que implica que P_γ es totalmente ramificado en F_1/F_0 y Q es un cero simple de $x_1 - \gamma$. Finalmente, siguiendo un proceso inductivo concluimos que P_γ es totalmente ramificado en $\mathcal{F}$ y que $\mathcal{F}$ es una sucesión no trivial. □

Finalizamos tercer capítulo con un ejemplo que ilustra el resultado anterior.

Ejemplo 3.32. Consideremos la sucesión $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_2$ definida recursivamente por la ecuación

$$y^3 + y = x^3 + x^2.$$

Veamos que $\mathcal{E}$ define una sucesión no trivial. Consideremos los polinomios

$$g(T) = T + 1, \qquad h(T) = T^2 = (T + 1)^2 + 1$$

y el cero simple P_1 de $x_0 + 1$ en $\mathbb{P}(\mathbb{F}_q(x_0))$. Entonces por la Proposición 3.31 tenemos que P_1 es un lugar totalmente ramificado en $\mathcal{E}$, $\mathbb{F}_q$ es el cuerpo total de constantes de cada E_i y cada extensión E_{i+1}/E_i es de grado dos. Veamos que se cumplen el resto de condiciones requeridas para que $\mathcal{E}$ sea una torre sobre $\mathbb{F}_2$. Se ve fácilmente que las extensiones E_{i+1}/E_i son separables, pues la ecuación que las define es separable y se puede probar que $g(E_3) = 3$.

Ahora probemos que $\mathcal{E}$ es una torre asintóticamente buena sobre $\mathbb{F}_4$ construyendo una (a, b)-supertorre con el método planteado en el Teorema 3.5. Consideremos las

funciones racionales

$$A(T) = T^3 + T, \quad B(T) = T^3 + T^2, \quad a(T) = T^2 + T,$$
$$b(T) = \frac{T^2}{T+1}, \quad g = \frac{T^2+T}{T^2+T+1} \quad \text{y} \quad s = \frac{T}{(T+1)^3}.$$

Puesto que

$$A(g(T)) = \frac{T^2+T}{(T^2+T+1)^3} = s(a(T))$$

y

$$B(g(T)) = \frac{(T^2+T)^2}{(T^2+T+1)^3} = s(b(T)),$$

entonces una supersucesión $\mathcal{F}$ sobre $\mathbb{F}_2$ de $\mathcal{E}$ está definida por la ecuación

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

Esta sucesión define una torre óptima sobre $\mathbb{F}_4$, lo que implica que $\mathcal{E}$ también es asintóticamente óptima sobre $\mathbb{F}_4$. Cabe destacar que la torre $\mathcal{F}$ es precisamente la torre $\mathcal{F}_0$, que fue usada en varios ejemplos de este capítulo, con $q = 2$.

CONCLUSIONES Y TRABAJO FUTURO

En esta tesis obtuvimos resultados en el campo de las torres recursivas de cuerpos de funciones sobre cuerpos finitos en dos direcciones: en primer lugar, demostramos que la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$ definida recursivamente por la ecuación de tipo Artin-Schreier

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

es asintóticamente mala si s es impar y asintóticamente buena si s es par; en particular, para $s = 2$ calculamos el número exacto de lugares racionales y el género de cada cuerpo de funciones, de lo que se concluyó que la torre $\mathcal{H}$ es óptima sobre $\mathbb{F}_4$. El resultado anterior constituye nuestro principal aporte a la clasificación de (a, b)-torres recursivas de tipo Artin-Schreier sobre $\mathbb{F}_2$, con $\deg a = \deg b = 2$. En efecto, con este se finaliza el estudio de este tópico iniciado por Beelen, Garcia y Stichtenoth [2] en el año 2006.

En segundo lugar, generalizamos algunos resultados concernientes a subsucesiones y supersucesiones recursivas; específicamente, planteamos un método para construir subsucesiones propias de una (a, b)-sucesión recursiva dada. Mejoramos la cota dada por Garcia, Stichtenoth y Thomas en [14] para el límite de la composición de una torre y un cuerpo; finalmente, dimos condiciones suficientes para que cierto tipo de (a, b)-sucesiones recursivas reducibles sea no trivial y tenga tasa de descomposición positiva; este último resultado es una generalización del resultado dado por Chara y Toledano [8] en el año 2012.

Además de los aportes antes citados, esta tesis nos deja una serie de interrogantes que servirán como punto de partida para futuras investigaciones. Con respecto a la torre $\mathcal{H}$ sobre $\mathbb{F}_{2^s}$, resulta de interés determinar el límite exacto de la torre, para s un entero par mayor que dos, y de su clausura Galoisiana para s un entero par; estudiar la modularidad de la torre $\mathcal{H}$ sobre $\mathbb{F}_4$ y exhibir, si fuese posible, una torre sobre un cuerpo finito de cardinalidad cuadrática con característica distinta de dos

que generalice la torre $\mathcal{H}$. En lo que respecta a la construcción de subsucesiones recursivas no triviales es importante dar criterios que aseguren que las subsucesiones sean torres y, en el mejor de los casos, que garanticen que la sucesión dada es la composición de una subsucesión y de un cuerpo. Con relación a las sucesiones reducibles de tipo (a, b) con tasa de descomposición positiva resulta indispensable estudiar el comportamiento de su espacio de ramificación y su género para determinar su comportamiento asintótico. Finalmente, cabe resaltar que la torre $\mathcal{H}$ y la torre $\mathcal{S}$ sobre $\mathbb{F}_{p^r}$ definida recursivamente por la ecuación

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

tienen una característica en común: existen lugares totalmente ramificados en el primer paso de la torre que en el siguiente paso se descomponen completamente. Ling, Stichtenoth y Yang [17] probaron que $\mathcal{S}$ tiene género finito si se cumple la condición $bc(b-c)^{2p-2} = 1$ y establecieron como problema abierto la determinación de la tasa de descomposición de esta torre. Ahora bien, la característica compartida por las torres mencionadas nos da la posibilidad de tratar el problema planteado por Ling et al. siguiendo las mismas técnicas usadas en el estudio de la torre $\mathcal{H}$. Estos aspectos resultan importantes en la medida que contribuyen a la teoría de torres de cuerpos de funciones en si y a las aplicaciones de ésta, como por ejemplo, la teoría de códigos.

Bibliografía

[1] A. Bassa, A. Garcia y H. Stichtenoth. *A new tower over cubic finite fields*, Moscow Math. J., 8(3), 401-418, 2008.

[2] P. Beelen, A. Garcia, y H. Stichtenoth. *Towards a classification of recursive towers of function fields over finite fields*, Finite Fields Appl., 12(1):56–77, 2006.

[3] J. Bezerra y A. Garcia. *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, J. Number Theory. 106: 142-154, 2004.

[4] J. Bezerra, A. Garcia, y H. Stichtenoth. *An explicit tower of function fields over cubic fields and Zink's lower bound*, J. Reine Angew. Math., 589:159-199, 2005.

[5] N. Caro and A. Garcia. On a tower of Ihara and its limit, Acta Arithmetica, 151:191–200, 2012.

[6] M. Chara. *Estudio del comportamiento asintótico de torres de cuerpos de funciones*, Tesis de doctorado. Universidad Nacional del Litoral. 2012.

[7] M. Chara, H. Navarro y R. Toledano. *A problem of Beelen, Garcia and Stichtenoth on an Artin-Schreier tower in characteristic two*, Acta Arithmetica, aceptado (2017).

[8] M. Chara y 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.

[9] V. G. Drinfel'd y S. G. Vlâdut. *The number of points of an algebraic curve*, Functional Anal. Appl. 17 (1983), no. 1, 53-54.

[10] N. Elkies. *Explicit modular towers*, Proceedings of the Thirty-Fifth Anual Allerton Conference on Communications, Control and Computing, T. Basar and A. Vardy, eds. 23–32, 1997.

[11] A. Garcia y H. Stichtenoth. *On the asymptotic behaviour of some tower of function fields over finite fields*, J. Number Theory, 61: 248-273, 1996.

[12] A. Garcia y H. Stichtenoth. *On the galois closure of towers*, Recent trends in coding theory and its applications, 83-92, AMS/IP Stud. Adv. Math., 41, Amer. Math. Soc., Providence, RI, 2007.

[13] A. Garcia y H. Stichtenoth. *Skew pyramids of function fields are asymptocally bad*, Coding theory, cryptography and related areas (Guanajuato, 1998), 111-113, Springer, Berlin, 2000.

[14] A. Garcia, H. Stichtenoth y M. Thomas *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl., 3: 257-274, 1997.

[15] 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.

[16] Y. Ihara. *Some remarks on the number the rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokio Sect. IA Math. 28, pp. 721-724.1981.

[17] S. Ling, H. Stichtenoth y S. Yang. *A class of Artin-Schreier Towers with finite genus*, Bull. Braz Math. Soc. 36(3):393–401, 2005.

[18] Y. Manin. *What is the maximum number of points on a curve over* $\mathbb{F}_2$*?* J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28(3):715-720 (1982), 1981.

[19] J. P. Serre. *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Ser. I Math., 269:397-402, 1983.

[20] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of Graduate Texts in Mathematics. Springer-Verlag, Berlin, second edition, 2009.

[21] H. Stichtenoth. *Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound*, IEEE Trans. Inform. Theory, Volume 52, 2218-2214 (2006). edition, 2009.

[22] A. Temkine. *Hilbert class field towers of function fields over finite fields and lower bounds for* $A(q)$, J. Number Theory, 87(2):189-210, 2001.

[23] A. Weil. *Sur les Courbes algébriques et les variétés qui s'en déduisent*, Volume 7 of Publications de l'Institut Mathématique de l'Université de Strasbourg. Hermann & Cie, Paris, 1948.

[24] 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