TORRES RECURSIVAS DE CUERPOS DE FUNCIONES SOBRE CUERPOS FINITOS

RICARDO TOLEDANO

RESUMEN. Se estudia el problema de la construcción de torres recursivas de cuerpos de funciones sobre cuerpos finitos con buenas propiedades asintóticas.

ÍNDICE

INTRODUCCIÓN

Un cuerpo de funciones algebraicas F de una variable sobre un cuerpo K es un cuerpo F en el cual existe un elemento x trascendente sobre K tal que la extensión de cuerpos $F/K(x)$ es finita. Una torre de cuerpos de funciones sobre un cuerpo perfecto K es una sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre K que cumple varias condiciones de naturaleza técnica que se detallan en la Sección 1.3. Las torres de cuerpos de funciones han sido estudiadas con bastante profundidad a partir de la década del 80 debido, principalmente, a los trabajos de Goppa [6] y de Tsfasman, Vladut y Zink [12] en los cuales se muestra la utilidad de estas teorías matemáticas en problemas relacionados con la teoría de códigos algebraicos. En este curso veremos ejemplos de construcción de las denominadas torres de cuerpos de funciones sobre cuerpos finitos asintóticamente buenas (ver Secciones 2 y 3). Esta clase de torres es la que tiene importancia en la teoría de códigos pues permitirían la construcción de códigos cuyos parámetros superan ciertas cotas teóricas que, hasta hace un tiempo atrás, se creían que eran muy difíciles de superar. La referencia básica que mencionaremos para ciertos resultados que no demostraremos es el libro de Stichtenoth [11]. También se pueden estudiar varios de los conceptos mencionados en este curso en los libros de Rosen [9] y de Niederreiter y Xing [8] (en particular en el libro de Niederreiter y Xing se estudian también propiedades asintóticas de torres (no recursivas) de cuerpos de funciones con métodos de la teoría de cuerpos de clases). En el capítulo 7 de [11] y en el artículo [4]

de García y Stichtenoth se puede encontrar la mayoría de los resultados básicos de la teoría asintótica de torres recursivas de cuerpos de funciones. Varios resultados de las Secciones 2 y 3 han sido tomados de la tesis doctoral de María Chara (Universidad Nacional del Litoral e IMAL, 2012) a quien agradezco haberme permitido usarlos en estas notas.

1. Definiciones y Resultados Básicos

1.1. Cuerpos de Funciones. Sean $K \subset F$ cuerpos. Decimos que F es un *cuerpo de funciones algebraicas sobre* K si existe un elemento $x \in F$ trascendente sobre K tal que F es una extensión finita de $K(x)$.

El conjunto

$$\tilde{K} := \{z \in F \,:\, z \text{ es algebraico sobre } K\},$$

es un subcuerpo de F que se denomina *cuerpo de constantes de* F *sobre* K. Se tiene que $K \subseteq \tilde{K} \subseteq F$, y se verifica fácilmente que F es un cuerpo de funciones sobre $\tilde{K}$. Decimos que K es *algebraicamente cerrado en* F (o que K *es el cuerpo total de constantes de* F) si $\tilde{K} = K$, es decir, los únicos elementos de F que son algebraicos sobre K son los elementos de K.

Sea F un cuerpo de funciones sobre K. Un *anillo de valuación* de F es un anillo $\mathcal{O} \subseteq F$ que tiene las siguientes propiedades:

I) $K \subsetneq \mathcal{O} \subsetneq F$, y
II) para cualquier $0 \neq z \in F$ se tiene que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Se sabe que $\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal P (ver [11, Proposición 1.1.5]).

Teorema 1.1. [11, Teorema 1.1.6] *Sea $\mathcal{O}$ un anillo de valuación de un cuerpo de funciones F sobre K y sea P su único ideal maximal. Entonces:*

a) P es un ideal principal.
b) Si $P = t\mathcal{O}$ entonces cualquier $0 \neq z \in F$ tiene una representación única en la forma $z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$.
c) $\mathcal{O}$ es un dominio de ideales principales. Más precisamente, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.

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

Cada anillo de valuación $\mathcal{O}$ de F determina un único lugar P de F y recíprocamente. Debido a esto, es usual denotar por $\mathcal{O}_P$ al anillo de valuación unívocamente determinado por el lugar P.

El conjunto de lugares de F se denotará por $\mathbb{P}(F)$. Se omite el cuerpo K en esta notación pues para cada lugar P de F se puede probar que $\tilde{K} \subseteq \mathcal{O}_P$.

Un ejemplo básico e importante de cuerpo de funciones es el denominado *cuerpo de funciones racionales* $K(x)$ donde x es un elemento trascendente sobre K. En este caso los anillos de valuaciones están asociados de manera unívoca a los polinomios mónicos irreducibles con coeficientes en K con una excepción: sea $f \in K[x]$ un polinomio mónico e irreducible sobre K. El conjunto

$$\mathcal{O}_f := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0 \text{ y } f \nmid g\},$$

es un anillo de valuación de $K(x)$ y su ideal maximal es

$$P_f := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0,\ f|h \text{ y } f \nmid g\}\,.$$

También el conjunto

$$\mathcal{O}_\infty := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0 \text{ y } deg\, f \leq deg\, g\}\,,$$

es un anillo de valuación de $K(x)$ y su ideal maximal es

$$P_\infty := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0 \text{ y } deg\, f < deg\, g\}\,,$$

y se lo denomina *lugar (o lugar o primo) infinito*. Se demuestra en [11, Proposition 1.2.1] que los lugares de $K(x)$ son los arriba mencionados y que

$$deg\, P_f = deg\, f\,,\ deg\, P_\infty = 1 \text{ y } K \text{ es el cuerpo total de constantes de } K(x)\,.$$

Una descripción alternativa de un lugar, que resulta de utilidad en muchos casos, está dada en términos de las denominadas valuaciones discretas de F.

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

1) $v(x) = \infty$ si y sólo si $x = 0$.
2) $v(xy) = v(x) + v(y)$ para todo $x, y \in F$.
3) $v(x + y) \geq \text{mín}\{v(x), v(y)\}$ para todo $x, y \in F$.
4) Existe un elemento $z \in F$ con $v(z) = 1$.
5) $v(a) = 0$ para todo $0 \neq a \in K$.

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

Bajo ciertas condiciones se tiene la igualdad en la Desigualdad Triangular.

Lema 1.2. [11, Lema 1.1.11](Desigualdad Triangular Estricta) *Sea v una valuación discreta de F y sean $x, y \in F$ con $v(x) \neq v(y)$. Entonces*

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

Por cada lugar P de F se puede definir una valuación discreta v_P de F de la siguiente manera: sea t un elemento primo para P. Entonces todo $0 \neq z \in F$ tiene una representación única $z = t^n u$ con $u \in \mathcal{O}_P^*$ y $n \in \mathbb{Z}$. Se define

$$v_P(z) := n \quad \text{y} \quad v_P(0) := \infty\,.$$

Teorema 1.3. [11, Teorema 1.1.13] *Sean F un cuerpo de funciones sobre K y P un lugar de F. La función v_P recién definida es una valuación discreta de F. Más aún, tenemos que*

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

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

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

En el caso del cuerpo de funciones racionales $K(x)$ las valuaciones discretas están determinadas por los polinomios mónicos e irreducibles con coeficientes en K y por el lugar infinito P_∞ de la siguiente manera (ver [11, Proposition 1.2.1]): si $f \in K[x]$ es mónico e irreducible y $z(x) = h(x)/g(x) \in K(x)$ entonces

$$\nu_{P_f}(z(x)) = n, \text{ si } z(x) = f(x)^n \frac{r(x)}{t(x)},$$

donde $f \nmid r$ y $f \nmid t$. En el caso del lugar infinito P_∞ se tiene que si $z(x) = h(x)/g(x) \in K(x)$ entonces

$$\nu_{P_\infty}(z(x)) = deg\, g - deg\, h\,.$$

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

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

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

se denomina *función de clases residuales*.

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

Por ejemplo, los lugares racionales de $K(x)$ están en correspondencia unívoca con los elementos de K y el lugar infinito P_∞. El grado de un lugar es siempre finito, más aún, tenemos el siguiente resultado.

Proposición 1.4. [11, Proposición 1.1.15] *Sean F un cuerpo de funciones sobre K y $P \in \mathbb{P}(F)$. Si $0 \neq x \in P$ entonces*

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

Observación 1.5. Para el caso en que $deg\, P = 1$ tenemos que $F_P = K$, y la función de clases residuales, aplica F en $K \cup \{\infty\}$. En particular, si K es algebraicamente cerrado, todos los lugares son de grado uno, y por lo tanto se puede mirar a cada elemento $z \in F$ como una función

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

Es por esto que a F se lo denomina cuerpo de funciones. Los elementos de K, interpretados como funciones, son funciones constantes y por esta razón K recibe el nombre de cuerpo de constantes de F.

Sea $z \in F$ y $P \in \mathbb{P}(F)$. Decimos que P es un *cero* de orden m de z si $v_P(z) = m > 0$. Decimos que P es un *polo* de orden m de z si $v_P(z) = m < 0$. Notar que en el caso de $K(x)$ el lugar P_∞ es el polo de x mientras que P_f es el cero (de orden uno) de $f(x)$.

Observación 1.6. [11, Corolario 1.3.4] En un cuerpo de funciones F sobre K todo elemento $0 \neq z \in F$ tiene una cantidad finita de ceros y de polos.

Para evitar complicaciones técnicas y casos patológicos supondremos, de ahora en adelante, que el cuerpo de constantes K es algebraicamente cerrado en F, es decir, $\tilde{K} = K$.

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

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

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

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

Un divisor de la forma $D = P$ con $P \in \mathbb{P}(F)$ se dice que es un *divisor primo*. El elemento neutro del grupo de divisores $\mathcal{D}_F$ es el divisor

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

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

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

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

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

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

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

El *grado* de un divisor D se define como

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

Por la Observación 1.6, sabemos que todo elemento no nulo $z \in F$ tiene una cantidad finita de ceros y polos en $\mathbb{P}(F)$. Por lo tanto la siguiente definición tiene sentido. Sea $0 \neq z \in F$ y denotemos por Z al conjunto de ceros (resp. N al conjunto de polos) de z en $\mathbb{P}(F)$. Entonces definimos

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

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

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

Teorema 1.7. [11, Teorema 1.4.11] *Sea $z \in F \setminus K$. Entonces*

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

En particular, todos los divisores principales tienen grado cero.

A divisor $D \in \mathcal{D}_F$ le corresponde un K-espacio vectorial $\mathcal{L}(D)$ que se denomina *espacio de Riemann-Roch* asociado a D y se define como

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

[1] Para todos excepto un número finito.

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

El *género* g de un cuerpo de funciones F sobre K se define como

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

El género es uno de los invariantes más importantes de un cuerpo de funciones, se puede probar que existe y que es un entero no negativo, (ver [11, Proposición 1.4.14]). Por ejemplo, el género de $K(x)$ es cero para todo elemento x trascendente sobre K. Más aún, un cuerpo de funciones F sobre K es de la forma $K(x)$ si y sólo si F es de género cero y tiene al menos un divisor de grado uno (ver [11, Proposition 1.6.3]).

1.2. Extensiones algebraicas y ramificación. De aquí en adelante supondremos que el cuerpo total de constantes de todo cuerpo de funciones es perfecto. Sean F un cuerpo de funciones sobre K y F' un cuerpo de funciones sobre K' tales que $K \subset K'$ y $F \subset F'$. Supondremos también que que ambas extensiones F'/F y K'/K son algebraicas.

Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$. Decimos que Q *divide* a P o que Q *está arriba* de P si $P \subset Q$. Denotamos esta situación con el símbolo $Q|P$.

Se puede probar (ver [11, Proposición 3.1.4]) que si $Q|P$ entonces existe un único entero $e \geq 1$ tal que $v_Q(x) = e\, v_P(x)$ para todo $x \in F$, y además que $Q \cap F = P$. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$ tales que $Q|P$.

a) El *índice de ramificación* $e(Q|P)$ de Q sobre P se define como el único entero $e(Q|P) := e$ que satisface
$$v_Q(x) = e\, v_P(x).$$
(ver [11, Definición 3.1.5])

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

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

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

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

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

Teorema 1.8. [11, Teorema 3.1.11](Igualdad Fundamental) *Si F'/F es una extensión finita de cuerpos de funciones y $P \in \mathbb{P}(F)$ entonces*

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

En el caso de que la extensión F'/F sea finita y Galois se tiene que si $Q|P$ y $Q'|P$ entonces $e(Q|P) = e(Q'|P$ y $f(Q|P) = f(Q'|P)$. Por lo tanto si F'/F es una extensión finita y Galois entonces

$$ref = [F' : F]\,,$$

donde r es el número de lugares de F' arriba de P y $e = e(Q|P)$ y $f = f(Q|P)$ para todo $Q \in \mathbb{P}(F')$ arriba de P.

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

a) Decimos que P se *descompone completamente* en F' si existen exactamente n lugares distintos de F' arriba de P. En este caso se tiene que $e(Q|P) = f(Q|P) = 1$ para todo $Q|P$.
b) Si existe un lugar $Q \in \mathbb{P}(F')$ tal que $e(Q|P) = n$ entonces decimos que el lugar P es *totalmente ramificado* en F'. En este caso se tiene que hay un único lugar de F' arriba de P.
c) Si existe un único lugar $Q \in \mathbb{P}(F')$ arriba de P y $e(Q|P) = 1$ entonces decimos que P es *inerte* en F' y en este caso $f(Q|P) = n$.

En el siguiente resultado se da una condición suficiente para la irreducibilidad de ciertos polinomios con coeficientes en un cuerpo de funciones que, en ciertos casos, es muy útil. Es una versión adaptada a cuerpos de funciones del conocido criterio de irreducibilidad de Eisenstein para polinomios con coeficientes enteros.

Proposición 1.9 (Criterio de Irreducibilidad de Eisenstein)**.** [11, Proposición 3.1.15] *Sea F/K un cuerpo de funciones y consideremos el polinomio*

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

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

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

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

En muchos casos se construyen extensiones de cuerpos de funciones F adjuntando a F un elemento integral sobre un anillo de valuaciones de ese cuerpo. Como veremos más adelante será importante tener un criterio de integrabilidad utilizando el polinomio mínimo del elemento a adjuntar.

Proposición 1.10. [11, Proposición 3.3.1] *Sea F/K un cuerpo de funciones y sea $F' \supseteq F$ una extensión finita de cuerpos. Sea $R \subset F$ un anillo integralmente cerrado tal que F es el cuerpo cociente de R (se dice también que R es un anillo de holomorfía de F). Para $z \in F'$ denotemos por $\varphi(T) \in F[T]$ a su polinomio mínimo sobre F. Entonces*

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

Para determinar el comportamiento de la ramificación de un lugar en extensiones simples en las cuales se conoce el polinomio mínimo del elemento que genera a la extensión, el siguiente teorema, debido originalmente a Kummer, que enunciamos a continuación es de mucha utilidad. Utilizaremos la siguiente notación: dado un lugar P de un cuerpo de funciones F y un polinomio $\psi(T) = \sum c_i T^i \in \mathcal{O}_P[T]$, denotaremos por $\overline{\psi}(T)$ al polinomio

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

donde $F_P = \mathcal{O}_{\mathcal{P}}/P$.

Teorema 1.11 (Teorema de Kummer)**.** [11, Teorema 3.3.7] *Sea F/K un cuerpo de funciones. Supongamos que $F' = F(y)$ donde y es un elemento integral sobre $\mathcal{O}_P$, y*

consideremos el polinomio mínimo $\varphi(T) \in \mathcal{O}_P[T]$ *de* y *sobre* F. *Sea*

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

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

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

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

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

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

Con hipótesis adicionales se pueden obtener los índices de ramificación, grados de inercia y números de lugares arriba de un lugar dado. Supongamos que al menos una de las siguientes hipótesis $(*)$ *o* $(**)$ *vale:*

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

o

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

Entonces para $1 \leq i \leq r$ *existe exactamente un lugar* $P_i \in \mathbb{P}(F')$ *tal que* $P_i|P$ *y* $\varphi_i(y) \in P_i$. *Además* $e(P_i|P) = 1$ *y* $f(P_i|P) = deg\,\gamma_i$ *para* $1 \leq i \leq r$. *Por lo tanto* $P_1, \ldots, P_r$ *son los lugares de* $\mathbb{P}(F')$ *que están arriba de* P.

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

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

donde $d(Q|P)$ es un entero no negativo unívocamente definido por P y Q llamado *exponente diferente*, (ver [11, Sección 3.4]). La determinación precisa de este divisor es fundamental para el cálculo del género de extensiones finitas y separables de cuerpos de funciones.

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

Teorema 1.12 (Teorema del divisor diferente de Dedekind)**.** [11, Teorema 3.5.1] *Siguiendo con la notación anterior tenemos que para todo* $Q|P$

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

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

La denominada *fórmula del género de Hurwitz* establece una importante relación entre los géneros de los cuerpos de funciones que forman una extensión finita y separable.

Teorema 1.13 (Fórmula del género de Hurwitz)**.** [11, Teorema 3.4.13] *Sea* F *un cuerpo de funciones sobre* K *y sea* F'/F *una extensión finita y separable. Denotemos por* K' *al cuerpo de constantes de* F'. *Entonces*

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

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

Sea F'/F una extensión finita y separable de cuerpos de funciones sobre $\mathbb{F}_q$ y sean Q y P lugares de F' y F respectivamente tales que $Q|P$. Decimos que la extensión $Q|P$ *es moderada* si $char\,(\mathbb{F}_q)$ no divide a $e(Q|P)$; en caso contrario decimos que la extensión $Q|P$ *es no moderada* o *salvaje*. Notar que en el caso moderado, si $e(Q|P) = 1$ entonces la extensión $Q|P$ es moderada. En el caso moderado, si hay ramificación, se dice que la ramificación es moderada. En el caso no moderado hay, necesariamente, ramificación.

Enunciamos ahora un resultado sobre la ramificación en una clase especial de extensiones de cuerpos de funciones llamadas extensiones de Kummer.

Teorema 1.14 (Extensiones de Kummer)**.** [11, Proposición 3.7.3] *Sea F/K un cuerpo de funciones tal que K contiene una raíz n-ésima primitiva de la unidad (con $n > 1$ y* $\mathrm{mcd}(n, char\,(K)) = 1$*). Supongamos que $u \in F$ es un elemento que satisface*

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

Sea

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

La extensión F'/F se llama extensión de Kummer de F y se tienen las siguientes propiedades:

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

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

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

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

Corolario 1.15. *Sea F un cuerpo de funciones y sea $F' = F(y)$ con $y^n = u$ y $u \in F$, donde $n \not\equiv 0 \mod char\,(K)$ y K contiene una n-ésima raíz primitiva de la unidad. Supongamos que existe un lugar $Q \in \mathbb{P}(F)$ tal que* $\mathrm{mcd}(v_Q(u), n) = 1$*. Entonces K es el cuerpo total de constantes del cuerpo F', la extensión F'/F es cíclica de grado n, y*

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

1.3. Sucesiones y torres de cuerpos de funciones. La construcción de cuerpos de funciones $F/\mathbb{F}_q$ con abundancia de lugares racionales con respecto al género tiene un papel importante en la teoría algebraica de códigos, (ver [11], [8]). Hay una relación entre $N(F) = N(F/\mathbb{F}_q)$, el número de lugares racionales de F, y $g(F) = g(F/\mathbb{F}_q)$, el género de F, la cual establece que, para q fijo, $N(F)$ no puede ser muy grande con respecto a $g(F)$. Este resultado se conoce como la cota de Hasse-Weil y es uno de los resultados más importantes de la teoría de cuerpos de funciones sobre cuerpos finitos.

Teorema 1.16 (Cota de Hasse-Weil)**.** [11, Teorema 5.2.3] *Sea $F/\mathbb{F}_q$ un cuerpo de funciones. Entonces*

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

Una mejora de esta cota es debida a Serre (ver [11, Teorema 5.3.1]) y establece que

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

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

Una manera de medir cuán abundante son los cuerpos de funciones $F/\mathbb{F}_q$ con muchos lugares racionales con respecto al género, es mediante la denominada función de Ihara que se define como

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

donde

$$N_q(g) = \text{máx}\{N(F/\mathbb{F}_q) \,:\, g(F/\mathbb{F}_q) = g\}\,.$$

Ihara demuestra en [7] que si q es un cuadrado (es decir, $q = p^{2k}$) entonces $A(q) \geq \sqrt{q} - 1$. Drinfeld y Vladut [2] mostraron que $A(q) \leq \sqrt{q} - 1$ con lo cual $A(p^{2k}) = p^k - 1$. Luego García y Stichtenoth [3] dieron la primera demostración constructiva de que $A(p^{2k}) = p^k - 1$ usando extensiones de Artin-Schreier. Cuando q no es un cuadrado, el valor exacto de $A(q)$ no se conoce. La no trivialidad de $A(q)$ para todo q (es decir que $A(q) \neq 0$) se debe a Serre [10] quien, con métodos de la teoría de cuerpos de clases, demostró que existe una constante $c > 0$ tal que

$$A(q) \geq c \cdot \log q\,,$$

para todo q. Posteriormente Zink [13] mejora esta cota inferior para el caso $q = p^3$ demostrando que

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

y más tarde, Bezerra, Garcia y Stichtenoth [1] generalizaron este mismo resultado para cualquier potencia cúbica, es decir

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

para todo q potencia de un primo. El aspecto distintivo de los trabajos mencionados de Garcia y Stichtenoth está en la obtención de una cota inferior para $A(q)$ mediante la construcción de torres de cuerpos de funciones asintóticamente buenas sobre $\mathbb{F}_q$ (Ver [11] y [4]) definidas recursivamente por una ecuación polinomial en dos variables. Este tipo de construcciones es el de mayor interés en la teoría de códigos y es el principal objeto de estudio de este curso. Comenzamos definiendo el concepto de sucesión admisible.

Una *sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones F_i sobre un cuerpo perfecto K* se dice que es *admisible* si se cumplen las siguientes condiciones:

i) $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$,
ii) la extensión F_{i+1}/F_i es finita y separable para todo $i \geq 0$,
iii) K es el cuerpo total de constantes de cada F_i; es decir, el cuerpo K debe ser algebraicamente cerrado en F_i para cada $i \geq 0$.

Si además se cumple que

iv) $g(F_i) \to \infty$ para $i \to \infty$,

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

Observación 1.17. La condición IV) se obtiene de las condiciones I), II) y de la siguiente condición que es levemente más débil y es muy útil en la práctica:

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

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

$$g(F_{i+1}) - 1 \geq [F_{i+1} : F_i](g(F_i) - 1) \qquad \forall\, i \geq 0.$$

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

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

y como el género de un cuerpo de funciones es un número entero, tenemos que $g(F_i) \to \infty$ para $i \to \infty$

Decimos que una sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre K es *recursiva* si existe una sucesión $\{x_i\}_{i=0}^{\infty}$ de elementos trascendentes sobre K y un polinomio en dos variables

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

tales que

I) $F_0 = K(x_0)$;
II) $F_{i+1} = F_i(x_{i+1})$ donde x_{i+1} es un cero de $f(x_i, y) \in \mathbb{F}_q[y]$, es decir, $f(x_i, x_{i+1}) = 0$ para $i \geq 0$.

Notar que si el polinomio en una variable $f(x_i, y) \in K[x_i][y]$ es separable entonces la extensión F_{i+1}/F_i es separable.

Asociado a una sucesión recursiva $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones F_i sobre K tenemos el denominado *cuerpo de funciones básico* $K(x, y)$ donde x es trascendente sobre K y $f(x, y) = 0$. Es usual decir que la ecuación $f(x, y) = 0$ *define o genera* a la sucesión $\mathcal{F}$.

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

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

con a_1, a_2, b_1 y b_2 polinomios con coeficientes en $\mathbb{F}_q$ tales que

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

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

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

y por lo tanto

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

Entonces para probar que una sucesión recursiva $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre K es una torre, basta mostrar que:

I) el polinomio $f(x, y) \in K[x][y]$ es separable, como polinomio en la segunda variable, para cualquier elemento trascendente x sobre K,
II) K es el cuerpo de constantes de todos los F_i,
III) $g(F_{i_0}) > 1$ para algún i_0.

La siguiente proposición (ver [11, Proposición 7.2.15]) da una condición suficiente para que ocurra II).

Proposición 1.18. *Consideremos una sucesión recursiva $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones donde F_0 es un cuerpo de funciones con cuerpo de constantes K y $[F_{i+1} : F_i] < \infty$ para todo $i \geq 0$. Supongamos que para todo $i \geq 0$ existen lugares $P_i \in \mathbb{P}(F_i)$ y $Q_i \in \mathbb{P}(F_{i+1})$ con $Q_i|P_i$ e índice de ramificación $e(Q_i|P_i) > 1$. Entonces $F_i \subsetneq F_{i+1}$.*

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

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

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre K.

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

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

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

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

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

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

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

Las siguientes definiciones son relevantes para esta clase de problemas. Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión admisible de cuerpos de funciones sobre $\mathbb{F}_q$. La *tasa de descomposición* $\nu(\mathcal{F}/F_0)$ y el *género* $\gamma(\mathcal{F}/F_0)$ de $\mathcal{F}$ sobre F_0 se definen, respectivamente, como

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

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

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

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

$$0 \leq \lambda(\mathcal{F}) \leq A(q), \tag{1.1}$$

para cualquier sucesión admisible $\mathcal{F}$ con $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$, para algún i_0 (ver [11, Capítulo 7]).

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

Una sucesión $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es *asintóticamente buena* si $\nu(\mathcal{F}/F_0) > 0$ y $\gamma(\mathcal{F}/F_0) < \infty$. En caso contrario se dice que $\mathcal{F}$ es *asintóticamente mala*. Por lo tanto, una sucesión admisible $\mathcal{F}$ es asintóticamente mala si $\nu(\mathcal{F}/F_0) = 0$ o si $\gamma(\mathcal{F}/F_0) = \infty$.

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

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

Ejercicios.

1. Demostrar la Proposición 1.18.

2. Construyendo torres de cuerpos de funciones

Como ya dijimos, un problema con importantes consecuencias en la teoría de códigos algebraicos es el cálculo de $A(q)$. De la desigualdad (1.1) vemos que se pueden conseguir cotas inferiores de $A(q)$ calculando, o al menos estimando, el límite $\lambda(\mathcal{F})$ de torres recursivas de cuerpos de funciones sobre $\mathbb{F}_q$. El primer problema a resolver es que la ecuación que define recursivamente a una sucesión sea una torre. Estudiaremos a continuación condiciones suficientes para que una ecuación de la forma $a(y) = b(x)$ defina una torre recursiva de cuerpos de funciones sobre $\mathbb{F}_q$.

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

Lema 2.1. *Sean F un cuerpo de funciones sobre K, $x \in F$ un elemento trascendente sobre K y $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ un polinomio de grado n. Supongamos además que $i \in \{0, 1, \ldots, n\}$ es el menor índice tal que $a_i \neq 0$. Entonces, si P es un lugar de F, tenemos que*

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

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

Corolario 2.2. *Con las condiciones del lema anterior tenemos que si $v_P(x) \geq 0$ entonces $v_P(f(x)) \geq 0$ y si $v_P(x) < 0$ entonces $v_P(f(x)) < 0$.*

Sea x un elemento trascendente sobre un cuerpo K. Consideremos el cuerpo de funciones racionales $K(x)$ sobre K. Para $\alpha \in K$, denotamos por P_α al único lugar de $K(x)$ asociado al polinomio $x - \alpha$, es decir, P_α es el cero de $x - \alpha$ en $K(x)$. También denotamos por P_∞ al polo de x en $K(x)$.

Teorema 2.3. *Sea K un cuerpo perfecto y sean a, b_1 y b_2 polinomios coprimos dos a dos con coeficientes en K. Supongamos que $deg\,(a) = deg\,(b_1) = m \geq 2$ y que $deg\,(b_2) = m - r$ con $\mathrm{mcd}(m, r) = 1$. Consideremos los siguientes cuerpos de funciones definidos de manera recursiva:*

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

Entonces $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ es una sucesión recursiva de cuerpos de funciones sobre K. Más aún, se cumple que:

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

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

Si además el polinimo $a(x) - \frac{b_1(x_i)}{b_2(x_i)} \in F_i[x]$ es separable para todo $i \geq 0$, entonces F_{i+1}/F_i es separable para todo $i \geq 0$.

Observación 2.4. Si en el Teorema 2.3 tenemos que $a(T) = T^m$, $deg\,(b_1(T)) = m - r$ y $deg\,(b_2(T)) = m \geq 2$ con $\mathrm{mcd}(m, r) = 1$, entonces se prueba al igual que en el teorema, que el polo de x_i en F_i es totalmente ramificado en F_{i+1} y por lo tanto también se obtiene que K es el cuerpo total de constantes de F_i para todo $i \geq 0$.

Ejercicios.

1. Demostrar el Lema 2.1 y su corolario.
2. Demostrar el Teorema 2.3.

3. Torres de tipo Kummer asintóticamente buenas

En esta sección daremos una demostración de la no trivialidad de la función de Ihara $A(q)$ cuando q es una potencia al menos par de un primo p. Utilizaremos las denominadas torres de tipo Kummer que son sucesiones admisibles y recursivas $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre un cuerpo perfecto K, de característica p, que están definidas por ecuaciones de la forma $y^m = f(x)$ con $\mathrm{mcd}(n, p) = 1$ y para ciertas elecciones adecuadas de $f(x) \in K(x)$.

3.1. Comportamiento asintótico de sucesiones y torres moderadas. Sea F un cuerpo de funciones sobre un cuerpo perfecto K y F' una extensión finita y separable de F. La extensión F'/F se dice que es *moderada* si para todo lugar Q de F' se tiene que el índice de ramificación $e(Q|P)$ es coprimo con la característica de K donde $P = Q \cap F$. En caso contrario se dice que la extensión F'/F es *no moderada* o *salvaje*.

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre un cuerpo perfecto K. Se dice que $\mathcal{F}$ es una sucesión *moderada* si la extensión F_{i+1}/F_i es moderada para todo $i \geq 0$. En caso contrario se dice que $\mathcal{F}$ es una sucesión *no moderada* o *salvaje*.

Uno de los resultados generales más útiles en la teoría de las torres moderadas es el siguiente teorema de Garcia, Stichtenoth and Thomas [5, Theorem 2.1].

Teorema 3.1. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre moderada de cuerpos de funciones sobre $\mathbb{F}_q$. Si*

I) *$\mathcal{F}$ es de ramificación finita, es decir, el conjunto $Ram(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : P$ ramifica en $\mathcal{F}\}$ es finito y*

II) *el conjunto $Split(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : P$ se descompone completamente en $\mathcal{F}\}$ es no vacío,*

entonces $\mathcal{F}$ es asintóticamente buena y además

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

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

Este resultado nos dice que en el caso de torres moderadas con ramificación finita (es decir, el conjunto de ramificación $Ram(\mathcal{F}/F_0)$ es finito) la existencia de al menos un lugar de F_0 que se descomponga completamente en la torre alcanza para garantizar el buen comportamiento asintótico de la torre. Esto es falso en el caso de torres no moderadas pues se conocen ejemplos de torres $\mathcal{F}$ no moderadas con ramificación finita y género $\gamma(\mathcal{F})$ infinito, con lo cual $\lambda(\mathcal{F}) = 0$ y, por lo tanto, $\mathcal{F}$ es asintóticamente mala. El siguiente lema es un criterio útil para garantizar ramificación finita en una sucesión.

Lema 3.2. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión recursiva y admisible de cuerpos de funciones sobre $\mathbb{F}_q$ definido por la ecuación $H(x, y) = 0$ donde $H \in \mathbb{F}_q[x, y]$. Supongamos que existe un conjunto $S_0 \subset \overline{\mathbb{F}}_q$ tal que si $\gamma \in S_0$ y $H(\beta, \gamma) = 0$ entonces $\beta \in S_0$. Sea $\{x_i\}_{i \geq 0}$*

una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ *tal que* $F_0 = \mathbb{F}_q(x_0)$ *y* $F_{i+1} = F_i(x_{i+1})$ *donde* $H(x_i, x_{i+1}) = 0$ *para todo* $i \geq 0$. *Si* Q *es un lugar de* F_i *tal que la clase residual* $x_i(Q) \in S_0$ *entonces* $x_0(Q) \in S_0$.

El lema anterior permite demostrar la siguiente proposición que será de particular utilidad en la construcción de torres asintóticamente buenas de tipo Kummer.

Proposición 3.3. *Sea* $m \geq 2$ *un entero y* q *una potencia de un número primo tal que* $q \equiv 1 \mod m$. *Sea* $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *una sucesión de cuerpos de funciones sobre* $\mathbb{F}_q$ *definida recursivamente por la ecuación*

$$y^m = \frac{b_1(x)}{b_2(x)} \tag{3.1}$$

donde $b_1(T), b_2(T) \in \mathbb{F}_q[T]$ *son polinomios comprimos tales que* $deg\,(b_1(T)) = m$ *y* $deg\,(b_2(T)) = m - r$ *con* $\mathrm{mcd}(m, r) = 1$. *Entonces* $\mathcal{F}$ *es una sucesión admisible y moderada. Supongamos además que existe un conjunto* $S_0 \subset F_q$ *con las siguientes propiedades:*

*(*I*)* $Z_{b_1} \subset S_0$.
*(*II*)* $Z_{b_2} \subset S_0$.
*(*III*)* $Z_{\sigma_\gamma} \subset S_0$, *for all* $\gamma \in S_0$, *donde* $\sigma_\gamma(T) = b_2(T)\gamma^m - b_1(T)$.

Entonces $Ram(\mathcal{F}/F_0)$ *es un conjunto finito. Más precisamente si* $P \in \mathbb{P}(\mathbb{F}_0)$ *es un lugar ramificado en la sucesión* $\mathcal{F}$ *entonces* $P = \mathbb{P}_\infty$ *o* P *es el cero de* $x_0 - \gamma$ *para algún* $\gamma \in S_0$.

Estamos ahora en condiciones de enunciar y demostrar el siguiente resultado que es de importancia para nuestro propósito de hallar una cota inferior no trivial de la función de Ihara en ciertos casos.

Teorema 3.4. *Sea* $m \geq 2$ *un entero y* q *una potencia de un número primo tal que* $q \equiv 1 \mod m$. *Sea* $\beta \in \mathbb{F}_q^*$ *y sea* $h(T) \in \mathbb{F}_q[T]$ *un polinomio separable y de grado* $m - r$ *con* $\mathrm{mcd}(m, r) = 1$ *y* $1 \leq r \leq m - 1$ *tal que* $h(0) = h_0 \neq 0$ *y* $Z_{T^m - (\beta/h_0)} \subset \mathbb{F}_q$. *Supongamos que existe un conjunto* $S_0 \subset \mathbb{F}_q$ *tal que*

*(*I*)* $0 \in S_0$;
*(*II*)* $Z_h \subset S_0$;
*(*III*) para cada* $\gamma \in S_0$ *se tiene que* $Z_{H_\gamma} \subset S_0$ *donde* $H_\gamma(T) = h(T)\gamma^m - \beta T^m$.

Entonces la sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *deinida recursivamente por la ecuación*

$$y^m = \frac{\beta x^m}{h(x)}, \tag{3.2}$$

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

(a) F_{i+1}/F_i *es una extensión moderada de grado* m *para todo* $i \geq 0$.
(b) Sea $P \in \mathbb{P}(F_0)$ *ramificado en* F_i/F_0 *para algún* $i \geq 1$ *y sea* x_0 *un elemento trascendente sobre* $\mathbb{F}_q$ *tal que* $F_0 = \mathbb{F}_q(x_0)$. *Entonces* P *es el polo* P_∞ *de* x_0 *en* F_0 *o es un cero de* $x_0 - \gamma$ *para algún* $\gamma \in S_0 \setminus \{0\}$.
(c) El cero P_{x_0} *de* x_0 *en* F_0 *se descompone completamente en* F_i/F_0 *para todo* $i \geq 1$.
(d) $\lambda(\mathcal{F}) \geq 2(|S_0| - 2)^{-1}$.

Demostración. La Proposición 3.3 nos dice que $\mathcal{F}$ es admisible y moderada. Sea $\{x_i\}_{i\geq 0}$ una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ tales que $F_0 = \mathbb{F}_q(x_0)$ y $F_{i+1} =$

$F_i(x_{i+1})$ donde

$$x_{i+1}^m = \frac{\beta x_i^m}{h(x_i)} \qquad \forall\, i \geq 0. \tag{3.3}$$

Veremos ahora que el lugar P_{x_0} (el cero de x_0 en F_0) se descompone completamente en F_i/F_0. Sea Q un lugar de F_i que sea un cero de x_0. Luego $Q \cap F_0 = P_{x_0}$ y además, por (3.2), se tiene que Q es un cero de $x_1, x_2, \ldots, x_i$. Notar que P_{x_0} se descompone completamente en F_i/F_0 si y sólo si Q se descompone completamente en F_{i+1}/F_i.

Sea $\tilde{\mathcal{F}} = \{\tilde{F}_i\}_{i=0}^{\infty}$ la sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ en la cual $\tilde{F}_0 = F_0 = \mathbb{F}_q(x_0)$ y $\tilde{F}_i = \tilde{F}_{i-1}(x_i/x_{i-1})$ for all $i \geq 1$. Luego $\tilde{\mathcal{F}}$ está recursivamente definida por la ecuación

$$y^m = \frac{\beta}{h(x)}$$

porque de (3.3) se verifica que

$$\left(\frac{x_{i+1}}{x_i}\right)^m = \frac{\beta}{h(x_i)}, \qquad \forall\, i \geq 0.$$

En realidad se tiene que $\tilde{\mathcal{F}} = \mathcal{F}$ pues $F_{i+1} = \tilde{F}_{i+1}$. Por lo tanto se puede considerar a $\mathcal{F}$ definida por la ecuación

$$y^m = \frac{\beta}{h(x)}.$$

Sea $z = h(x_n)$. Luego $z \in \mathcal{O}_Q^*$ pues $v_Q(z) = v_Q(h(x_n)) = 0$ de modo que $z(Q) \in \mathbb{F}_q^*$. Notar que si $h(T) = h_{m-r}T^{m-r} + \cdots + h_1 T + h_0$ entonces $z(Q) = h_0 \in \mathbb{F}_q^*$.

Reduciendo la ecuación $T^m = \frac{\beta}{h(x_n)}$ módulo Q se obtiene que

$$T^m = \frac{\beta}{z(Q)} = \frac{\beta}{h_0}.$$

Como $\beta/h_0 \neq 0$ y $q \equiv 1 \mod m$ el polinomio $T^m - \beta/h_0 \in \mathbb{F}_q[T]$ es separable. Por hipótesis la ecuación $T^m = \beta/h_0$ tiene m raíces distintas en $\mathbb{F}_q$ y el Teorema de Kummer (Teorema 1.11) dice en este caso que Q se descompone completamente en F_{i+1}/F_i lo cual equivale a que P_{x_0} se descomponga completamente en F_i/F_0. En consecuencia $N(F_i) \geq m^i$ y por lo tanto $g(F_i) \to \infty$ si $i \to \infty$.

Esto demuestra que $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_q$ que satisface (a) y (c) del Teorema 3.4. Notar que también se cumple (b) gracias a la Proposición 3.3. Por lo tanto todo lugar de F_0 ramificado en la torre es P_∞ o el cero de $x_0 - \gamma$ para algún $\gamma \in S_0 \setminus \{0\}$ (recordar que P_{x_0} se descompone completamente).

Finalmente usando el Teorema 3.1 se deduce que

$$\lambda(\mathcal{F}) \geq \frac{2}{|S_0| - 2}\,.$$

□

Estos resultados nos permiten ahora demostrar la no trivialidad de la función de Ihara $A(q)$ para ciertos valores de q:

Teorema 3.5. *Sea $q > 2$ una potencia de un número primo y sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ la sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ definida por la ecuación*

$$y^{q-1} = \frac{x^{q-1}}{x^{q-1} - (x-\alpha)^{q-1}}, \tag{3.4}$$

con $\alpha \in \mathbb{F}_q^*$. Sea $S_0 = \mathbb{F}_q$. Entonces

I) $0 \in S_0$,
II) $Z_f \subset S_0$,
III) *para cada* $\gamma \in S_0$ *se tiene que* $Z_{H_\gamma} \subset S_0$ *donde* $H_\gamma(T) = h(T)\gamma^m - \beta T^m$. *Más precisamente si* $\gamma \in \mathbb{F}_q^*$ *entonces* $\gamma^{q-1} = 1$ *y por lo tanto* $T^{q-1} - f(T) = (T-\alpha)^{q-1}$ *tiene todas su raíces en* $\mathbb{F}_q$.

Por lo tanto

$$\lambda(\mathcal{F}) \geq \frac{2}{q-2}\,,$$

y en consecuencia

$$A(2^n) \geq \frac{2}{2^n-2} \qquad \textit{si } n \geq 2 \quad \textit{y} \quad A(p^{2n}) \geq \frac{2}{p^n-2} \qquad \textit{si } p \textit{ es un primo impar}.$$

Ejercicios.

1. Demostrar el Lema 3.2.
2. Demostrar la Proposición 3.3
3. Demostrar el Teorema 3.5
4. (Problema para una tesis doctoral): Determinar si existen torres recursivas asintóticamente buenas con ramificación infinita.
5. (Problema para otra tesis doctoral): Determinar si existen torres recursivas asintóticamente buenas sobre cuerpos primos (es decir sobre $\mathbb{F}_p$).

Referencias

[1] J. Bezerra, A. Garcia y H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, Journal für die Reine und Angewandte Mathematik, **Vol. 589**, 2005, 159–199.

[2] S. Vlăduţ y V. Drinfel'd, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen., *Vol. 17*, 1983, 68-69.

[3] A. Garcia y H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound*, Inventiones Mathematicae, **Vol. 121**, 1995, 211–222.

[4] A. Garcia y H. Stichtenoth, *Explicit towers of function fields over finite fields*, Topics in geometry, coding theory and cryptography, **Vol. 6**, pp 1-58, Springer, 2007.

[5] A. Garcia, H. Stichtenoth y M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields and their Applications, **Vol. 3**, 1997, 257–274.

[6] V. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl., **Vol. 24**, 1981, 170–172.

[7] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, Journal of the Faculty of Science. University of Tokyo. Section IA. Math. **Vol. 28**, 1981, 721–724.

[8] H. Niederreiter y C. Xing, *Rational points on curves over finite fields: theory and applications*, London Mathematical Society Lecture Note Series, **Vol. 285**, Cambridge University Press, 2001.

[9] M. Rosen, *Number theory in function fields*, GTM **Vol. 210**, Springer, 2002.

[10] J. P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique, **Vol. 296**, 1983, 397–402.

[11] H. Stichtenoth, *Algebraic function fields and codes*, GTM **Vol. 254**, Springer, 2009.

[12] M. Tsfasman, S. Vlăduţ y T. Zink, *Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound*, Mathematische Nachrichten, **Vol. 109**, 1982, 21–28.

[13] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Lecture Notes in Comput. Sci., **Vol. 199**, 503–511, Springer, 1985.

Departamento de Matemática. UNL-FIQ. Santiago del Estero 2928 e IMAL, Güemes 3450. Santa Fe.

E-mail address: ridatole@gmail.com