Universidad de Sevilla

Trabajo de Fin de Máster
Máster Universitario en Matemáticas

Funciones zeta de variedades sobre cuerpos finitos

Javier Linares Torres

Tutorizado por
Prof. Antonio Rojas León

Resumen

La función zeta de una variedad sobre un cuerpo finito se define como la función generatriz asociada a la sucesión obtenida al contar el número de puntos racionales de la variedad en las sucesivas extensiones finitas del cuerpo base. Dicho objeto codifica las propiedades aritméticas de la variedad y permite establecer una asombrosa conexión entre las mismas y la topología de la variedad cuando la vemos sobre los números complejas a través de las conjeturas de Weil, uno de los resultados matemáticas más importantes del siglo XX. En este trabajo estudiamos las principales características de la función zeta y demostramos las conjeturas en dos de los casos que motivaron al propio Weil a enunciarlas: las hipersuperficies diagonales y el caso de curvas.

Abstract

The zeta function of a variety over a finite field is defined as the generating function associated with the sequence obtained by counting the number of rational points of the variety over the successive finite extensions of the ground field. This object encodes the arithmetic properties of the variety and allows us to establish an amazing connection between them and the topology of the variety when we see it over the complex numbers through the Weil's conjectures, one of the most important mathematical results of the 20th century. In this dissertation we study the main characteristics of the zeta function and prove the conjectures in two of the cases that motivated Weil himself to state them: the diagonal hypersurfaces and the case of curves.

Índice

1 Introducción e historia de las conjeturas

La historia de las conjeturas de Weil se remonta hasta 1740, cuando Euler consideró el estudio de la suma infinita dada por

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p>0} \frac{1}{1-p^{-s}},$$

donde p recorre el conjunto de los números primos, para ciertos valores de s enteros y positivos. Posteriormente, Chebychev estudió esta suma como una función de variable real y Riemann, que conocía el trabajo de Euler y la relación de esta función con la teoría de números, escribe en 1859 su obra maestra «Über die anzahl der primzahlen unter einer gegebenen größe» [Rie59], donde considera la anterior suma como una función de variable compleja $\zeta(s)$, que converge para $\mathrm{Re}(s) > 1$ y prueba su continuidad analítica, además de demostrar que dicha extensión tiene ceros en los enteros pares y negativos, los denominados «ceros triviales». Riemann establece aquí su famosa conjetura: los ceros no triviales de $\zeta(s)$ tienen parte real $1/2$. Esta conjetura, aún abierta a día de hoy, ha tenido y tiene un impacto enorme en la historia y el desarrollo de las matemáticas, pues de ser cierta permitiría desvelar información acerca de la distribución de los números primos.

Motivado por la existencia de la factorización de $\zeta(s)$ como un producto en función de los números primos, Dedekind realiza una definición análoga para un anillo de enteros $\mathcal{O}_K$, donde ahora el producto se realiza sobre el conjunto de ideales primos de $\mathcal{O}_K$, y a partir de ese momento se empiezan a estudiar generalizaciones de la función ζ asociados a un álgebra R de tipo finito sobre $\mathbb{Z}$:

$$\zeta(R,s) = \prod_{\mathfrak{m}\subset R} \frac{1}{1-\#(R/\mathfrak{m})^{-s}},$$

donde ahora $\mathfrak{m}$ recorre el conjunto de ideales maximales de R. Gran parte del trabajo de la geometría aritmética de principios del siglo XX consistió en trasladar los resultados de tipo analítico (extensión meromorfa, ecuación funcional) que se conocían de las funciones zeta que aparecían en teoría de números a la función zeta asociada al cuerpo de funciones de variedades algebraicas sobre un cuerpo finito.

Esta versión «en característica p» de la hipótesis de Riemann comienza en 1924, en la tesis de Emil Artin [Art24], donde se define la función zeta de una curva sobre un cuerpo finito y se establece el análogo a la hipótesis de Riemann. Para una variedad X sobre un cuerpo finito $\mathbb{F}_q$, es interesante realizar el cambio de variable $T = q^{-s}$, de modo que la función zeta se transforma en una función generatriz del número de puntos de la variedad sobre las sucesivas extensiones de nuestro cuerpo base

$$\zeta(X, q^{-s}) = Z(X,T) = \mathrm{Exp}\left(\sum_{s=1}^{\infty} \frac{\mathcal{N}_s T^s}{s}\right).$$

Son notables las contribuciones realizadas en esta época por F.K. Schimidt y H. Hasse, el primero demostrando la racionalidad de la función zeta en el caso de curvas y el segundo probando la hipótesis de Riemann para curvas elípticas. La hipótesis de Riemann en curvas de género arbitrario se resistió hasta mediados de los 40, cuando André Weil la demostró en [Wei45] utilizando una desigualdad de Castelnuovo y Severi. Unos años más tarde y motivado por los resultados obtenidos para el caso de curvas y otros ejemplos concretos como el de variedades abelianas [Wei46] o hipersuperficies diagonales, Weil conjetura en

el famoso artículo [Wei49] que la función zeta de una variedad debe satisfacer cuatro propiedades, las desde entonces denominadas **Conjeturas de Weil**: racionalidad, ecuación funcional, hipótesis de Riemann y conexión con la topología de la variedad vista sobre $\mathbb{C}$; planteando así una profunda conexión entre las propiedades aritméticas y topológicas de la variedad. El propio Weil apuntó que con una teoría de cohomología adecuada para variedades sobre cuerpos finitos, similar a la cohomología singular de variedades sobre $\mathbb{C}$, se podrían deducir las conjeturas de manera directa. Por ejemplo, la racionalidad y la ecuación funcional serían consecuencia de resultados bien conocidos de Topología Algebraica como el Teorema del punto fijo de Lefschetz o la dualidad de Poincaré.

Esto propició que durante la segunda mitad del siglo XX se lograse un profundo desarrollo de la Geometría Algebraica mediante la introducción de diferentes teorías cohomológicas. La primera de ellas fue la cohomología de haces coherentes de Serre, que no cumplía los requisitos propuestos por Weil ya que los coefientes de dicha cohomología para una variedad sobre un cuerpo finito no estarían en un cuerpo de característica cero. El primer avance llego de mano de Dwork que, fuera de este programa, probó en [Dwo60] la racionalidad de la función zeta mediante técnicas de análisis p-ádico y sin usar aparentemente métodos cohomológicos. También a principios de los 60, Michael Artin y Grothendieck introdujeron la cohomología l-ádica, que resultó tener las propiedades adecuadas para probar las conjeturas de Weil salvo la hipótesis de Riemann [AGV73]. Esta teoría se basa en la construcción de la topología étale de un esquema, en la que sustituimos los abiertos típicos de la topología por morfismos étale. A pesar de estos avances, la hipótesis de Riemann seguía resistiéndose, hasta que finalmente en 1974 Pierre Deligne culminó los esfuerzos de la escuela de París impulsada por Grothendieck, entre otros, y consiguió probarla en [Del74], lo cual le valió la concesión de la medalla fields en 1978.

El objetivo principal de este trabajo es el de introducirnos en el estudio de la función zeta de una variedad sobre un cuerpo finito, familiarizarnos con sus propiedades básicas, enunciar las conjeturas de Weil y probar las mismas en dos casos concretos: el de hipersuperficies diagonales y el de curvas. En el desarrollo del mismo emplearemos el lenguaje de los esquemas, con la filosofía de introducir siempre los conceptos que vamos utilizando, aunque dada la limitación en extensión de este trabajo serán frecuentes las referencias a libros de Geometría Algebraica como [Har77] o [GW10].

En la Sección 2, definimos la función zeta de un esquema de tipo finito y vemos la relación que tiene con la función generatriz asociada a los puntos racionales cuando el esquema está definido sobre un cuerpo finito. Enunciamos las conjeturas de Weil y estudiamos algunos ejemplos concretos. En la Sección 3, desarrollamos las técnicas necesarias para contar los puntos en una hipersuperficie de tipo diagonal mediante la teoría de sumas de Gauss y Jacobi, pasando por la relación de Hasse-Davenport, para finalmente comprobar las conjeturas en este caso concreto. Seguidamente, en la Sección 4, desarrollamos la teoría de curvas necesaria para enunciar el Teorema de Riemann-Roch, clave en la demostración de la racionalidad y la ecucación funcional de la función zeta de una curva. Seguidamente, hacemos una rápida incursión en la teoría de intersección en superficies para desarrollar las herramientas que nos permitan probar la desigualdad de Hasse-Weil, y así terminar la demostración de las conjeturas para el caso de curvas.

2 La función zeta

En esta sección definimos la función zeta de un esquema de tipo finito y enunciamos las conjeturas de Weil. Antes de ello, hacemos un breve repaso sobre ciertos aspectos del anillo de series de potencias formales sobre un cuerpo así como de cuerpos finitos.

2.1 Series de potencias

A lo largo de este trabajo consideraremos series de potencias formales (con coeficientes en $\mathbb{Q}$ en la mayoría de los casos) sin preocuparnos por las cuestiones de convergencia. En este apartado repasamos algunas de las operaciones que necesitamos incorporar al anillo de series de potencias formales sobre un cuerpo, siguiendo básicamente [Niv69], que posteriormente nos ayudarán a manipular la función zeta de un esquema. Dado un cuerpo F, denotaremos $F[\![T]\!]$ al anillo de series de potencias formales sobre F, cuyos elementos serán representados de la forma $\sum_{i=0}^{\infty} a_i T^i$, $a_i \in F$. Definimos P_0 como el conjunto formado por aquellas series que tienen $a_0 = 0$ y P_1 aquellas en las que $a_0 = 1$. Recordemos que el producto en $F[\![T]\!]$ viene dado por

$$\left(\sum_{i=0}^{\infty} a_i T^i\right)\left(\sum_{j=0}^{\infty} b_j T^j\right) = \sum_{l=1}^{\infty}\left(\sum_{i+j=l} a_i b_j\right) T^l,$$

que las unidades de $F[\![T]\!]$ son $F[\![T]\!] \setminus P_0$ y que $(1 - aT^n)^{-1} = \sum_{i=0}^{\infty} a^i T^{ni}$. A menudo identificaremos al subanillo de series de potencias cuyos coeficientes son cero a partir de uno dado con $F[T]$, el anillo de polinomios en una variable sobre F. También será usual considerar $F[\![T]\!]$ y $F(T)$ (el cuerpo de fracciones de $F[T]$) como subanillos del cuerpo de fracciones de $F[\![T]\!]$, obteniéndose por ejemplo

$$F[\![T]\!] \cap F(T) = \{P/Q : P, Q \in F[T]; Q(0) \neq 0\}.$$

Definición 2.1. Dada una sucesión $\alpha_1, \alpha_2, \ldots$ de series en $F[\![T]\!]$,

$$\alpha_i = \sum_{j=0}^{\infty} a_{ij} T^j, \qquad \text{para } i = 1, 2, \ldots$$

decimos que $(\alpha_i)_{i=1}^{\infty}$ **admite suma** si para todo entero $r \geq 0$, existe otro entero $N(r)$ tal que para todo $l \geq N(r)$ se tiene que $a_{l0} = a_{l1} = \cdots = a_{lr} = 0$. En ese caso definimos $\sum_{i=1}^{\infty} \alpha_i$ como la serie cuyo coeficiente r-ésimo viene dado por $\sum_{i=1}^{N(r)} a_{ir}$.

Se puede comprobar que si $(\alpha_i)_{i=1}^{\infty}$ admite suma y τ es una permutación de $\mathbb{Z}_{\geq 1}$, entonces $(\alpha_{\tau(i)})_{i=1}^{\infty}$ también admite suma y además $\sum_{i=1}^{\infty} \alpha_i = \sum_{i=1}^{\infty} \alpha_{\tau(i)}$. De manera análoga también podemos definir productos infinitos:

Definición 2.2. Sea $\gamma_1, \gamma_2, \ldots$ una sucesión de series en $F[\![T]\!]$. Decimos que $(\gamma_i)_{i=1}^{\infty}$ **admite producto** si $\gamma_i \in P_1$ para todo $i = 1, 2, \ldots$ y $(\gamma_i - 1)_{i=1}^{\infty}$ admite suma. En ese caso definimos la serie $\prod_{i=1}^{\infty} \gamma_i$ como aquella cuyo coeficiente r-ésimo es el coeficiente r-ésimo de la serie $\prod_{i=1}^{N(r)} \gamma_i$, para $N(r)$ suficientemente grande.

De nuevo esta definición es satisfactoria en el sentido de que si permutamos los elementos de una sucesión que admite producto, de nuevo obtenemos una sucesión que admite producto y sendos productos coinciden.

Ejemplo 2.3. Dadas sucesiones $(b_i)_{i=1}^{\infty}$, $(a_i)_{i=1}^{\infty}$ de enteros no negativos, la sucesión de series dada por

$$\gamma_i = (1 - a_i T^i)^{-b_i} = (1 + a_i T^i + a_i^2 T^{2i} + \dots)^{b_i}, \quad i = 1, 2, \dots$$

admite producto.

A continuación definimos las tres operaciones que emplearemos a la hora de manipular series de potencias formales. Supondremos que F tiene característica 0.

Definición 2.4. Definimos la **derivada**, el **logaritmo** y la **exponencial** como las aplicaciones

$$\begin{aligned}
\frac{d}{dT} : F[\![T]\!] &\to F[\![T]\!] \\
\sum_{i=0}^{\infty} a_i T^i &\mapsto \sum_{i=0}^{\infty} (i+1) a_{i+1} T^i, \\
\mathrm{Log} : P_1 &\to P_0 \\
\alpha &\mapsto \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(\alpha - 1)^i}{i}, \\
\mathrm{Exp} : P_0 &\to P_1 \\
\beta &\mapsto \sum_{i=0}^{\infty} \frac{\beta^i}{i!}.
\end{aligned}$$

Notemos que las aplicaciones están bien definidas, pues si $\alpha \in P_1$, entonces $\left((-1)^{i+1} \frac{(\alpha-1)^i}{i}\right)_{i=1}^{\infty}$ es una suma admisible y análogamente si $\beta \in P_0$, entonces $\left(\frac{\beta^i}{i!}\right)_{i=1}^{\infty}$ también lo es. Algunas de las propiedades usuales de la derivada, logaritmo y exponencial usuales se mantienen para series formales (cf. [Niv69, Sec. 5,6,7]):

Proposición 2.5. *Sean $\alpha, \beta \in P$; $\gamma, \gamma' \in P_1$; $(\gamma_i)_{i=1}^{\infty}$ admitiendo producto; $\delta, \delta' \in P_0$ y $n \in \mathbb{Z}_{\geq 0}$. Se tiene que*

1. $\frac{d}{dT}(\alpha+\beta) = \frac{d}{dT}(\alpha) + \frac{d}{dT}(\beta)$, $\frac{d}{dT}(\alpha\beta) = \frac{d}{dT}(\alpha)\beta + \alpha\frac{d}{dT}(\beta)$, $\frac{d}{dT}(\alpha^n) = n\alpha^{n-1}\frac{d}{dT}(\alpha)$ *y si α tiene inverso,* $\frac{d}{dT}(\alpha^{-n}) = -n\alpha^{-n-1}\frac{d}{dT}(\alpha)$.
2. $\mathrm{Log}(\gamma\gamma') = \mathrm{Log}(\gamma) + \mathrm{Log}(\gamma')$, $\mathrm{Log}\left(\prod_{i=1}^{\infty}\gamma_i\right) = \sum_{i=1}^{\infty}\mathrm{Log}(\gamma_i)$, $\mathrm{Log}(\alpha^n) = n\,\mathrm{Log}(\alpha)$ *y si α tiene inverso,* $\mathrm{Log}(\alpha^{-n}) = -n\,\mathrm{Log}(\alpha)$.
3. $\mathrm{Exp}(\delta + \delta') = \mathrm{Exp}(\delta)\,\mathrm{Exp}(\delta')$.
4. $\frac{d}{dT}(\mathrm{Log}(\gamma)) = \gamma^{-1}\frac{d}{dT}(\gamma)$, $\frac{d}{dT}(\mathrm{Exp}(\gamma)) = \gamma\frac{d}{dT}(\gamma)$, $\mathrm{Log}(\mathrm{Exp}(\delta)) = \delta$, $\mathrm{Exp}(\mathrm{Log}(\gamma)) =$

2.2 Cuerpos finitos

Antes de vernos inmersos en el estudio de la función zeta y las conjeturas de Weil, hacemos un breve repaso de las propiedades básicas de los cuerpos finitos (véase, por ejemplo [Lor96, XII.7.5]). Recordemos que dado un cuerpo k finito, tenemos que $\#(k) = p^n$ para algún

$n \geq 1$, donde el primo p es la característica de k y se tiene que dos cuerpos finitos con la misma cardinalidad son isomorfos. Denotaremos al cuerpo finito con $q = p^n$ elementos como $\mathbb{F}_q$. Fijemos dicho cuerpo y consideremos una clausura algebraica, que denotaremos por $\mathbb{F}$. Para cada $s \geq 1$, existe una única extensión de $\mathbb{F}_q$ en $\mathbb{F}$ de grado s, el cuerpo de descomposición de $x^{q^s} - x$. Denotaremos por $\mathbb{F}_{q^s}$ a dicho cuerpo. La extensión $\mathbb{F}_{q^s}/\mathbb{F}_q$ es de Galois, pues es normal y separable, ya que $\mathbb{F}_q$ es perfecto. Además $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ es cíclico de orden s, y está generado por el denominado **automorfismo de Frobenius**, $F : \mathbb{F}_{q^s} \to \mathbb{F}_{q^s}$, $a \mapsto a^q$. Este automorfismo jugará un papel fundamental en este trabajo y en general en el estudio de las variedades sobre cuerpos finitos. Por otro lado, es bien conocido que el grupo multiplicativo $\mathbb{F}_q^\star = \mathbb{F}_q \setminus \{0\}$ es cíclico de orden $q - 1$.

2.3 La función zeta

En esta sección estableceremos el contexto en el que trabajaremos y definiremos la función zeta de un esquema de tipo finito sobre $\mathbb{Z}$. Recordemos que un **esquema** es un espacio anillado $(X, \mathscr{O}_X)$ que es localmente isomorfo al espectro de algún anillo. El **cuerpo residual** en un punto $x \in X$ se define como el cuerpo residual del anillo local $\mathscr{O}_{X,x}$ y se denotará como $\kappa(x)$. Si X es un esquema de tipo finito sobre $\mathbb{Z}$, es decir, existe un morfismo $X \to \operatorname{Spec} \mathbb{Z}$ de tipo finito, entonces para todo abierto afín $\operatorname{Spec} A$ de X se tiene que A es un anillo finitamente generado, es decir, finitamente generado como $\mathbb{Z}$-álgebra. Denotamos $|X|$ al conjunto de los puntos cerrados de X, es decir, puntos que corresponden con ideales maximales cuando tomamos un entorno afín que los contenga. Si $x \in |X|$, entonces $\kappa(x) = A/\mathfrak{m}$ para algún anillo finitamente generado A y $\mathfrak{m}$ ideal maximal. Se sigue que $\kappa(x)$ es finitamente generado y gracias al siguiente lema deducimos que es un cuerpo finito.

Lema 2.6. *Un cuerpo k que es finitamente generado como anillo es finito.*

Demostración. Si k tiene característica 0 entonces contiene a $\mathbb{Q}$, que no es finitamente generado como $\mathbb{Z}$-álgebra. Entonces $\mathrm{char}(k) = p > 0$, luego k es una $\mathbb{F}_p$-álgebra de generación finita y gracias a la versión del Teorema de los Ceros de Hilbert que nos dice que si K es un cuerpo y B una K-álgebra finitamente generada que también es un cuerpo, entonces B es una extensión finita de k (véase [AM89, Cor 5.24]), podemos concluir. □

Gracias a ello, dado X esquema de tipo finito sobre $\mathbb{Z}$, podemos realizar la siguiente definición de la **función zeta de** X, como una expresión formal para $s \in \mathbb{C}$

$$\zeta(X, s) = \prod_{x \in |X|} \frac{1}{1 - \#(\kappa(x))^{-s}}$$

Resulta que este producto converge absolutamente para $\mathrm{Re}(s) > \dim X$, véase [Mus11, 6.29] (recordemos que la dimensión de un esquema es su dimensión como espacio topológico).

Ejemplo 2.7. Cuando $X = \operatorname{Spec} \mathbb{Z}$, los puntos cerrados de X son los ideales primos no nulos de $\mathbb{Z}$ y $\zeta(X, s)$ se corresponde con la función zeta de Riemann clásica

$$\zeta(\operatorname{Spec} \mathbb{Z}, s) = \prod_{p > 0} \frac{1}{1 - p^{-s}}.$$

Si por el contrario tenemos una extensión finita de $\mathbb{Q} \to K$, podemos considerar el anillo de enteros $\mathcal{O}_K$ asociado, es decir, la clausura entera de $\mathbb{Z}$ en K. Es bien conocido que $\mathcal{O}_K$

es un $\mathbb{Z}$-módulo finitamente generado, luego también finitamente generado como anillo, por lo tanto $X = \operatorname{Spec} \mathcal{O}_K$ es un esquema sobre $\mathbb{Z}$ de tipo finito. Además, como $\mathcal{O}_K$ es un dominio de Dedekind, en particular tiene dimensión 1, luego todo ideal primo no nulo $\mathfrak{p}$ es maximal. La función zeta de X coincide con la función zeta de Dedekind

$$\zeta(\operatorname{Spec} \mathcal{O}_K, s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - \#(\mathcal{O}_K/\mathfrak{p})^{-s}}.$$

Nuestro siguiente paso es reducir el estudio de $\zeta(X, s)$ al caso en el que X es integral, es decir, $\mathscr{O}_X(U)$ es un dominio de integridad para todo $U \subset X$ abierto, o equivalentemente, es irreducible y reducido ($\mathscr{O}_X(U)$ no tiene elementos nilpotentes) [Har77, II.3.1]. Dado un esquema X, podemos considerar el esquema reducido asociado a X, que se obtiene hacificando el haz $U \mapsto \mathscr{O}_X(U)/\operatorname{nil}(\mathscr{O}_X(U))$, llamado X_{red}. Los cuerpos residuales de X y X_{red} coinciden en cada punto del espacio topológico subyacente. Se sigue que

$$\zeta(X, s) = \zeta(X_{\text{red}}, s).$$

Por otro lado, si tenemos X como unión de dos subesquemas cerrados[1] $X = X_1 \cup X_2$, entonces de nuevo los cuerpos residuales coinciden y si dotamos a $X_1 \cap X_2$ con la estructura de subesquema cerrado reducido [GW10, 3.52], tenemos que

$$\zeta(X, s) = \frac{\zeta(X_1, s)\zeta(X_2, s)}{\zeta(X_1 \cap X_2, s)}. \tag{2.1}$$

Por lo tanto podremos suponer sin pérdida de generalidad que X es integral. La imagen del único morfismo $X \to \operatorname{Spec} \mathbb{Z}$ es por lo tanto irreducible, luego es un punto cerrado (no puede ser el punto genérico pues en ese caso tendríamos que los cuerpos $\kappa(x)$ son extensiones de $\mathbb{Q}$) o un conjunto denso. El primer caso engloba las que se suele denominar funciones zeta ***locales***, pues X pasa a ser un esquema de tipo finito sobre algún $\mathbb{F}_p$ y por lo tanto están referidas a un primo p fijo, mientras que en el segundo tenemos funciones zeta ***globales***. En este trabajo nos centramos en el primer caso, en particular estudiaremos la función zeta cuando X es una variedad sobre algún cuerpo finito.

Sea $k \to K$ una extensión finita de cuerpos. Un **k-esquema** X es un esquema junto con un morfismo $X \to \operatorname{Spec} k$. En particular tenemos para cada punto $x \in X$ una extensión de cuerpos $k \to \kappa(x)$. Si además X es de tipo finito sobre k, podemos caracterizar los puntos cerrados de X como aquellos en los que dichas extensiones son algebraicas (cf. [GW10, 3.33]). Si $x \in X$ es un punto cerrado, definimos **el grado** de x como

$$\deg(x) = [\kappa(x) : k].$$

Un **punto K-racional** de X es un morfismo de k-esquemas $\operatorname{Spec} K \to X$ y el conjunto de todos ellos será denotado $X(K)$. Dar un punto K-racional es equivalente a dar un punto cerrado $x \in |X|$ y un morfismo de k-álgebras $\kappa(x) \to K$ (cf. [GW10, 3.8]), es decir, existe una biyección

$$X(K) \cong \bigcup_{x \in |X|} \operatorname{Hom}_{k-\text{álg}}(\kappa(x), K).$$

[1] Recordemos que la noción de subesquema cerrado es algo más sutil que la de subconjunto cerrado. Aquí usamos al definición de [GW10]: un subesquema cerrado de X viene dado por un conjunto cerrado $Z \subset X$ y un haz $\mathscr{O}_Z$ tal que $(Z, \mathscr{O}_Z)$ es un esquema y tal que el haz $i_*\mathscr{O}_Z$ es isomorfo a $\mathscr{O}_X/\mathcal{I}$ para algún haz de ideales, donde $i : Z \to X$ es la inclusión.

En particular, si $[K : k] = s$, entonces teniendo en cuenta los grados en las extensiones $k \to \kappa(x) \to K$ podemos separar la unión anterior:

$$X(K) \cong \bigcup_{\deg(x)|s} \mathrm{Hom}_{k-\text{álg}}(\kappa(x), K). \tag{2.2}$$

Por ejemplo, consideremos el esquema $X = \operatorname{Spec} A/I$, donde $A = k[x_1, \ldots, x_n]$ e $I \subseteq A$ es un ideal. Entonces los K-puntos racionales de X se corresponden con los puntos de K^n que satisfacen los polinomios de I, ya que tenemos biyecciones

$$\begin{aligned}&\mathrm{Hom}_{\operatorname{Spec} k}(\operatorname{Spec} K, X) \cong \mathrm{Hom}_{k-\text{álg}}(A/I, K) \cong \\ &\{a = (a_1, \ldots, a_n) \in K^n : f(a) = 0 \text{ para todo } f \in I\},\end{aligned}$$

la primera de ellas se deduce de la equivalencia de categorías entre la opuesta de las k-álgebras y k-esquemas afines y la segunda manda un homomorfismo de k-álgebras $\varphi : A/I \to K$ al punto $(\varphi(x_1), \ldots, \varphi(x_n))$.

Si ahora X es un k-esquema de tipo finito, podemos tomar un recubrimiento finito por abiertos afines $\{U_\alpha\}_\alpha$ para obtener

$$X(K) = \bigcup_\alpha U_\alpha(K).$$

En particular, si K es finito, $X(K)$ también. Si tenemos una variedad proyectiva $X = \operatorname{Proj} S$ para $S = k[x_0, \ldots, x_n]/I$, donde I es un ideal homogéneo, podemos recubrir X con los abiertos afines

$$D_{x_i} = \{\mathfrak{p} \in X \text{ tal que } x_i \notin \mathfrak{p}\},$$

de modo que

$$D_{x_i}(K) = \mathrm{Hom}_{\operatorname{Spec} k}(\operatorname{Spec} K, D_{x_i}) \cong \mathrm{Hom}_{k-\text{álg}}(S^0_{x_i}, K),$$

donde $S^0_{x_i}$ es el subanillo de elementos de grado cero de la localización S_{x_i}. No es difícil comprobar que este último conjunto se corresponde con los puntos $[a_0 : \cdots : a_n] \in \mathbb{P}^n(K)$ que verifican $a_i \neq 0$ y que anulan a los polinomios homogéneos de I. En definitiva, tenemos que

$$X(K) \cong \{a = [a_0 : \cdots : a_n] \in \mathbb{P}^n(K) : f(a) = 0 \text{ para todo } f \in I \text{ homogéneo}\}. \tag{2.3}$$

Sea ahora $q = p^n$ para algún primo p y consideremos el único (salvo isomorfismo) cuerpo $\mathbb{F}_q$ de q elementos. Fijemos una clausura algebraica $\mathbb{F}$ y sea $\mathbb{F}_{q^s}$ la extensión de grado s de $\mathbb{F}_q$ en $\mathbb{F}$. Consideremos X un $\mathbb{F}_q$-esquema de tipo finito, que por lo dicho anteriormente verifica que $X(\mathbb{F}_{q^s})$ es finito para todo $s \geq 1$. Además dado $x \in |X|$ con $\deg(x) = r|s$, el grupo $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ actúa transitivamente en $\mathrm{Hom}_{\mathbb{F}_q-\text{álg}}(\kappa(x), \mathbb{F}_{q^s})$ componiendo los homomorfismo por la izquierda. Es sencillo verificar que el estabilizador de cualquier homomorfismo coincide con $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_{q^r})$, por lo que

$$\#\,\mathrm{Hom}_{\mathbb{F}_q-\text{álg}}(\kappa(x), \mathbb{F}_{q^s}) = \frac{\#\,\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)}{\#\,\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_{q^r})} = \frac{s}{s/r} = r, \tag{2.4}$$

luego junto con 2.2 obtenemos

Proposición 2.8. *Sea X un $\mathbb{F}_q$-esquema de tipo finito. Entonces se tiene que*

$$\#X(\mathbb{F}_{q^s}) = \sum_{r|s} r \cdot \#\{x \in |X| : \deg(x) = r\}.$$

Esta proposición nos permitirá expresar $\zeta(X,s)$ en función de la sucesión de enteros $\mathcal{N}_s := \#X(\mathbb{F}_{q^s})$ haciendo el cambio de variable $q^{-s} = T$. Para ello definimos

$$Z(X,T) := \prod_{x\in|X|} \frac{1}{1-T^{\deg(x)}} \in \mathbb{Q}[\![T]\!],$$

de modo que $\zeta(X,s) = Z(X,q^{-s})$. Resulta mucho más conveniente estudiar la función $Z(X,T)$ para el caso de esquemas sobre $\mathbb{F}_q$, como muestra la siguiente proposición.

Proposición 2.9. *Sea X un $\mathbb{F}_q$-esquema de tipo finito, entonces se tiene la siguiente igualdad en $\mathbb{Q}[\![T]\!]$:*

$$Z(X,T) = \operatorname{Exp}\left(\sum_{s=1}^{\infty} \frac{\mathcal{N}_s T^s}{s}\right).$$

Demostración. Llamemos α a la serie que aparece a la derecha de la igualdad que queremos probar. Tomando derivada del logaritmo en $Z(X,T)$ y multiplicamos por T obtenemos que

$$\begin{aligned} T\cdot\frac{d}{dT}(\operatorname{Log}(Z(X,T))) &= T\sum_{x\in|X|}\frac{d}{dT}(\operatorname{Log}(1-T^{\deg(x)})^{-1}) = \sum_{x\in|X|}\deg(x)\frac{T^{\deg(x)}}{1-T^{\deg(x)}} \\ &= \sum_{x\in|X|}\deg(x)\sum_{s=1}^{\infty}T^{s\deg(x)} = \sum_{s=1}^{\infty}\left(\sum_{\substack{x\in|X|\\ \deg(x)|s}}\deg(x)\right)T^s \\ &= \sum_{s=1}^{\infty}|X(\mathbb{F}_{q^s})|\,T^n, \end{aligned}$$

donde en la última igualdad hemos tenido en cuenta la Proposicón 2.8, luego claramente se satisface $T\cdot\frac{d}{dT}(\operatorname{Log}(Z(X,T))) = T\cdot\frac{d}{dT}(\operatorname{Log}(\alpha))$. Dado que multiplicar por T y tomar derivada del logaritmo son funciones inyectivas en $\mathbb{Q}[\![T]\!]$, tenemos la igualdad. □

Notemos que $Z(X,T)$ codifica las «propiedades aritméticas» de X pues a partir de $Z(X,T)$ es posible recuperar la sucesión $\mathcal{N}_s$ (decimos que $Z(X,T)$ es una función generadora).

Ejemplo 2.10. Gracias a la anterior proposición, podemos calcular la función de zeta en algunos casos particulares donde sepamos contar puntos racionales.

- *El espacio proyectivo*: consideremos $\mathbb{P}^n_{\mathbb{F}_q} = \operatorname{Proj}\mathbb{F}_q[x_0,\dots,x_m]$, el espacio proyectivo de dimensión n sobre $\mathbb{F}_q$. Gracias a 2.3, sabemos que para $s\geq 1$

  $$\mathcal{N}_s = \#\mathbb{P}^n(\mathbb{F}_{q^s}) = \frac{q^{s(n+1)}-1}{q^s-1} = q^{sn}+q^{s(n-1)}+\cdots+q^s+1,$$

  por lo que el logaritmo de la función zeta de X viene dado por

  $$\begin{aligned} \operatorname{Log}(Z(\mathbb{P}^n_{\mathbb{F}_q},T)) &= \sum_{s=1}^{\infty}\sum_{r=0}^{n}\frac{(q^rT)^s}{s} \\ &= \sum_{r=0}^{n}\sum_{s=1}^{\infty}\frac{(q^rT)^s}{s} = \sum_{r=0}^{n}-\operatorname{Log}(1-q^rT), \end{aligned}$$

  por lo tanto se obtiene que la función zeta de $\mathbb{P}^n_{\mathbb{F}_q}$ puede expresarse como una función racional:

  $$Z(\mathbb{P}^n_{\mathbb{F}_q},T) = \frac{1}{(1-T)(1-qT)\dots(1-q^nT)}.$$

- *Curvas elípticas.* Sea E una curva elíptica sobre $\mathbb{F}_q$, es decir, una variedad no singular, proyectiva, de dimensión 1 y género[2] 1. En 4.2 probaremos que existe $\alpha \in \mathbb{C}$ entero algebraico de valor absoluto $\sqrt{q}$ tal que $N_s = 1 - \alpha^s - \overline{\alpha}^s + q^s$. Por lo tanto el logaritmo de la función zeta de E viene dado por

$$\begin{aligned}\operatorname{Log}(Z(E,T)) &= \sum_{s=1}^{\infty} \frac{(1-\alpha^s-\overline{\alpha}^s+q^s)T^s}{s} \\ &= \sum_{s=1}^{\infty} \frac{T^s}{s} + \sum_{s=1}^{\infty} \frac{(\alpha T)^s}{s} + \sum_{s=1}^{\infty} \frac{(\overline{\alpha} T)^s}{s} + \sum_{s=1}^{\infty} \frac{(qT)^s}{s} \\ &= -\operatorname{Log}(1-T) + \operatorname{Log}(1+\alpha T) + \operatorname{Log}(1+\overline{\alpha}T) - \operatorname{Log}(1-qT),\end{aligned}$$

  luego obtenemos

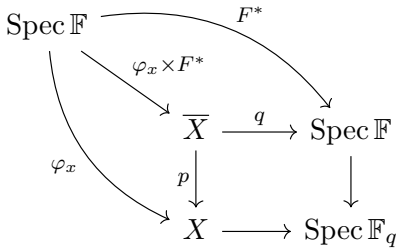
$$Z(E,T) = \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-qT)},$$

  de nuevo una expresión racional para la función zeta. Las conjeturas de Weil establecen precisamente que esto no es una casualidad; además nos dan información sobre las raíces de los polinomios en el numerador y denominador, una ecuación funcional para $Z(X,T)$ y una asombrosa relación entre los grados de dichos polinomios y la topología de la variedad cuando la vemos sobre los números complejos.

A continuación, debemos desarrollar otra herramienta fundamental en el estudio de los $\mathbb{F}_q$-esquemas, la del **cambio de base**, que nos permite pasar de esquemas sobre $\mathbb{F}_q$ a esquemas sobre la clausura algebraica $\mathbb{F}$. Sea X es un $\mathbb{F}_q$-esquema de tipo finito, definimos

$$\overline{X} := X \times_{\mathbb{F}_q} \mathbb{F},$$

es decir, el producto fibrado en la categoría de los $\mathbb{F}_q$-esquemas de X y $\operatorname{Spec}\mathbb{F}$. El automorfismo de Frobenius $F : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^q$ induce una acción en los puntos cerrados de $\overline{X}$ cuyas órbitas coinciden con las fibras de la proyección $p : \overline{X} \to X$. En efecto, dado un punto cerrado $x \in \overline{X}$, tenemos que $y = p(x)$ también es cerrado (pues p da lugar a una extensión $\psi_x : \kappa(y) \to \mathbb{F}$) y podemos definir un morfismo $\varphi_x : \operatorname{Spec}\mathbb{F} \to X$ cuya imagen es el punto y y a nivel de haces viene determinado por ψ_x. Si $F^* : \operatorname{Spec}\mathbb{F} \to \operatorname{Spec}\mathbb{F}$ es el morfismo asociado a F y llamamos q a la proyección $\overline{X} \to \operatorname{Spec}\mathbb{F}$, se sigue de la propiedad universal del producto fibrado que existe una única $\varphi_x \times F^*$ que hace conmutativo el siguiente diagrama



de modo que definimos $F \cdot x$ como la imagen del morfismo $\varphi \times F^*$. Comprobar que la órbita de x coincide son $p^{-1}(x)$ y que además son finitas se reduce a observar que si $p(x) = p(z) = y$, las extensiones ψ_x y ψ_z verifican $\psi_x = F^r \circ \psi_z$ para algún $1 \geq r \geq \deg(y)$. Otra forma de entender esta situación es considerar el **automorfismo de Frobenius en** X, $F_X : X \to X$, definido como la identidad a nivel de espacios topológicos y a nivel

[2] Más adelante concretaremos qué significan estos términos.

de haces de anillos por $a \mapsto a^q$. Dado que para $a \in \mathbb{F}_q$, $a \mapsto a^q$ es la identidad, tenemos que F_X es de hecho un morfismo de $\mathbb{F}_q$-esquemas. En particular, induce un morfismo de $\mathbb{F}$-esquemas

$$F_{\overline{X}} = F_X \times \mathrm{id}_X : \overline{X} \to \overline{X}. \tag{2.5}$$

Siguiendo un razonamiento análogo, vemos que los puntos $\mathbb{F}_{q^s}$-racionales de X se corresponden con los puntos de $\overline{X}$ que quedan fijos tras aplicar $F_{\overline{X}}^s$.

Si por ejemplo $X = \operatorname{Spec} A$, donde $A = \mathbb{F}_q[x_1 \ldots, x_n]/I$ para algún ideal $I \subset \mathbb{F}_q[x_1, \ldots, x_n]$, entonces $\overline{X} = \operatorname{Spec}(A \otimes_{\mathbb{F}_q} \mathbb{F})$, y sus puntos cerrados se corresponden con puntos de $\mathbb{F}^n$ que satisfacen los polinomios de I.

2.4 Las conjecturas de Weil

De aquí en adelante, dado un cuerpo k, entenderemos por **variedad sobre** k un k-esquema de tipo finito, geométricamente irreducible[3] y separado. Si X es una variedad sobre k, diremos que X es **no singular** si $\overline{X}$ no tiene puntos singulares, es decir, $\mathscr{O}_{\overline{X},x}$ es regular para todo $x \in \overline{X}$. También diremos que X es **proyectiva** si X es isomorfa a algún cerrado del espacio proyectivo sobre k.

Antes de dar el enunciado de las conjeturas debemos introducir un último concepto. Dado un esquema de tipo finito Y sobre un anillo de enteros R y un primo $\mathfrak{p} \subset R$ tal que $R/\mathfrak{p} \cong \mathbb{F}_q$, definimos **la reducción de** Y **módulo** $\mathfrak{p}$ o la **reducción de** Y **a** $\mathbb{F}_q$ como

$$Y_{\mathfrak{p}} := Y \times_R R/\mathfrak{p},$$

que resulta ser un $\mathbb{F}_q$-esquema de tipo finito. Si por ejemplo $Y = \operatorname{Proj} S$ para S un cociente de $R[x_0, \ldots, x_m]$ por un ideal homogéneo $(F_1, \ldots, F_n)$, entonces $Y_{\mathfrak{p}}$ viene definido por la reducción módulo $\mathfrak{p}$ de los coefientes de los polinomios F_i. Sin más dilación, vamos ya con el enunciado de las conjeturas:

Teorema 2.11 (Conjeturas de Weil)**.** *Sea X una variedad sobre $\mathbb{F}_q$ proyectiva, no singular y de dimensión n. La función zeta de X satisface:*

1. ***Racionalidad**: $Z(X,T)$ es una función racional con coeficientes enteros, es decir, existen $P(T), Q(T) \in \mathbb{Z}[T]$ tales que $Z(X,T) = P(T)/Q(T)$.*

2. ***Hipótesis de Riemann**: $Z(X,T)$ se descompone como*

$$Z(X,T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2n}(T)},$$

con $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$ y para cada $1 \leq i \leq 2n$ podemos escribir

$$P_i(T) = \prod_j (1 - \alpha_{ij} T) \in \mathbb{Z}[T],$$

con los α_{ij} enteros algebraicos que cumplen

$$|\alpha_{ij}| = q^{\frac{i}{2}}.$$

[3] Quiere decir que $X \times_k \overline{k}$ es irreducible o, equivalentemente, que $X \times_k K$ es irreducible para toda extensión finita y separable K/k.

3. ***Ecuación funcional**: Se tiene la siguiente igualdad en $\mathbb{C}(T)$:*

$$Z\left(X, \frac{1}{q^n T}\right) = \pm q^{\frac{nE}{2}} T^E Z(X,T), \tag{2.6}$$

donde $E = \sum_{i=0}^{2n} (-1)^i \deg P_i$.

4. ***Números de Betti**: Supongamos que X se ha obtenido como reducción a $\mathbb{F}_q$ de alguna variedad Y definida sobre un cuerpo de números R. Sea Y_a el conjunto de puntos cerrados de $Y \times_R \mathbb{C}$ y consideremos la topología euclídea inducida por la inclusión $Y_a \to \mathbb{P}^n(\mathbb{C})$. Entonces*

$$\deg(P_i) = \operatorname{rg} H^i(Y_a, \mathbb{Z}),$$

es decir, el grado del polinomio $P_i(T)$ coincide con $B_i(Y_a)$, el i-ésimo número de Betti del espacio topológico Y_a, que se define como el rango del i-ésimo grupo de cohomología singular de Y_a.

Recordemos que tras el cambio de variable $T = q^{-s}$, habíamos obtenido que $\zeta(X,s) = Z(X, q^{-s})$. Por lo tanto, la segunda conjetura implica que todos los ceros y polos complejos de $\zeta(X,s)$ tienen parte real $\frac{i}{2}$ para algún $i = 0, \ldots, 2n$, de ahí la justificación del nombre.

Vamos ahora a probar un par de lemas que nos dan caracterizaciones sobre la racionalidad y la ecuación funcional de la función zeta que nos serán más manejables. Decimos que $\alpha \in k^\star = k \setminus \{0\}$ es una **raíz recíproca** de un polinomio si α^{-1} es una raíz del mismo.

Lema 2.12. *$Z(X,T) = P(T)/Q(T)$ para $P(T), Q(T) \in \mathbb{Z}[T]$ si y sólo si existen conjuntos $\{\alpha_i\}_i$ y $\{\beta_j\}_j$ de enteros algebraicos, ambos invariantes por automorfismos de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, tales que*

$$\mathcal{N}_s = \sum_j \beta_j^s - \sum_i \alpha_i^s.$$

Es ese caso si $P(0) = Q(0) = 1$, se tiene que $P(T) = \prod_i (1 - \alpha_i T)$ y $Q(T) = \prod_j (1 - \beta_j T)$.

Demostración. Supongamos que $Z(X,T) = P(T)/Q(T)$ para $P(T), Q(T) \in \mathbb{Z}[T]$. Sabemos que el término independiente de $Z(X,T)$ es 1, por lo que sin pérdida de generalidad podemos suponer que $P(0) = Q(0) = 1$. Factorizamos P y Q en $\mathbb{C}[T]$ para obtener

$$Z(X,T) = \frac{\prod_i (1 - \alpha_i T)}{\prod_j (1 - \beta_j T)}.$$

Dado que $\{\alpha_i\}_i$ y $\{\beta_j\}_j$ son las raíces recíprocas de polinomios en $\mathbb{Z}$, deben ser invariantes por automorfismos de Galois. Tomando derivada del logaritmo y multiplicando por T en la igualdad anterior se sigue que

$$\sum_{s=1}^{\infty} \mathcal{N}_s T^s = \sum_i \frac{-\alpha_i T}{1 - \alpha_i T} + \sum_j \frac{-\beta_j T}{1 - \beta_j T} = \sum_{s=1}^{\infty} \left(\sum_j \beta_j^s - \sum_i \alpha_i^s \right) T^s,$$

de donde obtenemos la primera implicación.

Recíprocamente, si $\mathcal{N}_s = \sum_j \beta_j^s - \sum_i \alpha_i^s$, entonces

$$Z(X,T) = \operatorname{Exp}\left(\sum_{s=1}^{\infty}\left(\sum_j \beta_j^s - \sum_i \alpha_i^s\right)\frac{T^s}{s}\right) = \operatorname{Exp}\left(\sum_j\sum_{s=0}^{\infty}\frac{(\beta_j T)^s}{s} - \sum_i\sum_{s=0}^{\infty}\frac{(\alpha_i T)^s}{s}\right)$$
$$= \operatorname{Exp}\left(-\sum_j \operatorname{Log}(1-\beta_j T) + \sum_i \operatorname{Log}(1-\alpha_i T)\right) = \frac{\prod_i(1-\alpha_i T)}{\prod_j(1-\beta_j T)}.$$

Dado que los α_i y β_j son invariantes por cualquier automorfismo de Galois, se sigue que $\prod_i(1-\alpha_i T), \prod_j(1-\beta_j T) \in \mathbb{Z}[T]$. □

Lema 2.13. *Asumiendo la racionalidad y la hipótesis de Riemann de $Z(X,T)$, se verifica la ecuación funcional 2.6 si y sólo si la involución $\alpha \mapsto q^n/\alpha$ intercambia las raíces recíprocas contadas con multiplicidad de P_i y de P_{2n-i}.*

Demostración. Supongamos que se satisface la ecuación funcional, es decir, se tiene la siguiente igualdad en $\mathbb{C}(T)$

$$P_0(T)P_2(T)\cdots P_{2n}(T)P_1\left(\frac{1}{q^nT}\right)P_3\left(\frac{1}{q^nT}\right)\cdots P_{2n-1}\left(\frac{1}{q^nT}\right)$$
$$= \pm q^{\frac{nE}{2}}T^E P_0\left(\frac{1}{q^nT}\right)P_2\left(\frac{1}{q^nT}\right)\cdots P_{2n}\left(\frac{1}{q^nT}\right)P_1(T)P_3(T).\cdots P_{2n-1}(T).$$

Sea α una raíz recíproca con multiplicidad m de P_i, con i par (el caso impar es análogo); entonces por la igualdad anterior q^n/α es una raíz recíproca con multiplicidad m de algún P_j con j par o bien α es una raíz recíproca con multiplicidad m de algún P_j con j impar. La hipótesis de Riemann nos dice que las raíces recíprocas de P_j tiene módulo $q^{\frac{i}{2}}$, por lo que la única posibilidad es que q^n/α, que tiene módulo $q^{\frac{2n-i}{2}}$, sea una raíz recíproca de P_{2n-i}.

Recíprocamente, si $\alpha \mapsto q^n/\alpha$ intercambia las raíces recíprocas de P_i y P_{2n-i} teniendo en cuenta multiplicidades, se tiene que

$$P_i\left(\frac{1}{q^nT}\right) = \prod_j\left(1-\alpha_{ij}\frac{1}{q^nT}\right)$$
$$= \prod_j\left(1-T\frac{q^n}{\alpha_{ij}}\right)(-1)^{\deg P_i}(q^n)^{-\deg P_i}T^{-\deg P_i}\prod_j\alpha_{ij}$$
$$= P_{2n-i}(T)(-1)^{\deg P_i}(q^n)^{-\deg P_i}T^{-\deg P_i}\prod_j\alpha_{ij}$$
$$= \pm P_{2n-i}(T)T^{-\deg P_i}q^{-\frac{1}{2}(2n-1)\deg P_i},$$

donde hemos usado que $\prod_j \alpha_{ij} \in \mathbb{Z}$ y tiene módulo $q^{\frac{i}{2}\deg P_i}$. Por lo tanto tenemos que

$$Z\left(X,\frac{1}{q^nT}\right) = \frac{P_1\left(\frac{1}{q^nT}\right)\cdots P_{2n-1}\left(\frac{1}{q^nT}\right)}{P_0\left(\frac{1}{q^nT}\right)\cdots P_{2n}\left(\frac{1}{q^nT}\right)} = \pm\frac{\prod_{i\text{ impar}}^{2n} P_{2n-i}(T)T^{-\deg P_i}q^{-\frac{1}{2}(2n-1)\deg P_i}}{\prod_{i\text{ par}}^{2n} P_{2n-i}(T)T^{-\deg P_i}q^{-\frac{1}{2}(2n-1)\deg P_i}}$$
$$= \pm Z(X,T)T^E q^{\frac{1}{2}\sum_{i=0}^{2n}(-1)^i(2n-1)\deg P_i}.$$

Aprovechando ahora el hecho de que $\deg P_i = \deg P_{2n-i}$, tenemos que

$$\sum_{i=0}^{2n}(-1)^i(2n-1)\deg P_i = 2n\sum_{i=0}^{n-1}(-1)^i \deg P_i + n(-1)^n \deg P_n$$
$$= 2n\left(\frac{E-(-1)^n \deg P_n}{2}\right) + n(-1)^n \deg P_n = nE,$$

de donde se deduce el resultado. □

Ejemplo 2.14. Vamos a poner en relieve la importancia de las conjeturas calculando los números de Betti de el Grassmaniano contando sus puntos en las sucesivas extensiones de $\mathbb{F}_q$. Para cada $1 \leq r < n$, existe un esquema $\mathrm{Gr}(r,n)$ definido sobre $\operatorname{Spec}\mathbb{Z}$, denominado **Grassmaniano**, tal que para todo cuerpo k el conjunto de los puntos k-racionales está en biyección con los subespacios lineales r-dimensionales de k^n (véase [EH06, III.2.7]). Consideremos la reducción a $\mathbb{F}_q$ $\mathrm{Gr}(r,n)_{\mathbb{F}_q} = \mathrm{Gr}(r,n) \times_{\mathbb{Z}} \mathbb{F}_q$, que resulta ser una variedad sobre $\mathbb{F}_q$ proyectiva y no singular de dimensión $r(n-r)$, y la variedad compleja asociada $\mathrm{Gr}(r,n)_{\mathbb{C}} = \mathrm{Gr}(r,n) \times_{\mathbb{Z}} \mathbb{C}$.

Calculemos el número de subespacios lineales de dimensión r en $\mathbb{F}_q^n$. Notemos que el grupo $\mathrm{GL}_r(\mathbb{F}_q)$ actúa en el conjunto $\mathcal{U}$ de las r-uplas de vectores linealmente independientes de $\mathbb{F}_q^n$ mediante $A\cdot(v_1\ldots,v_n) = (Av_1,\ldots,Av_r)$, de modo que dos r-uplas están en la misma órbita si y sólo si generan el mismo subespacio. Dicha acción es libre, luego el número de órbitas, que coincide con $\mathcal{N}_1$, se calcula como $\#\mathcal{U}/\#\,\mathrm{GL}_r(\mathbb{F}_q)$.

Notemos que para seleccionar un elemento $(v_1,\ldots,v_r) \in \mathcal{U}$, existen $\#(\mathbb{F}_q^n \setminus \{0\}) = q^n - 1$ opciones para v_1; una vez seleccionado v_1, tenemos $\#(\mathbb{F}_q^n \setminus \operatorname{span}(v_1)) = q^n - q$ elementos disponibles y así sucesivamente hasta que nos quedan $q^n - q^{r-1}$ posibles elecciones para v_r. De igual modo dar un elemento de $\mathrm{GL}_r(\mathbb{F}_q)$ es dar una r-upla de vectores linealmente independientes en $\mathbb{F}_q^r$. En definitiva,

$$\mathcal{N}_1 = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-r+1}-1)}{(q^r-1)(q^{r-1}-1)\ldots(q-1)}.$$

Este número suele conocerse como el coeficiente binomial guassiano y se denota por $\binom{n}{r}_q$. Para cada $0 \leq j \leq r(n-r)$, sea $\lambda_{n,r}(j)$ el número de particiones de j en menos de $n-r$ partes, cada una de ellas de tamaño menor que r, entonces se tiene que [BF14, 13.5.6]:

$$\binom{n}{r}_q = \sum_{j=0}^{r(n-r)} \lambda_{n,r}(j) q^j.$$

Cambiando $\mathbb{F}_q$ por $\mathbb{F}_{q^s}$, obtenemos

$$\mathcal{N}_s = \sum_{j=0}^{r(n-r)} \lambda_{n,r}(j) q^{sj},$$

por lo que

$$\mathrm{Log}(Z(\mathrm{Gr}(r,n),T)) = \sum_{j=0}^{r(n-r)} \lambda_{n,r}(j) \sum_{s=1}^{\infty} \frac{(q^jT)^s}{s} = \sum_{j=0}^{r(n-r)} -\lambda_{n,r}(j)\,\mathrm{Log}(1-q^jT),$$

luego,

$$Z(\mathrm{Gr}(r,n),T) = \prod_{j=0}^{r(n-r)} (1-q^jT)^{-\lambda_{n,r}(j)}.$$

Utilizando la hipótesis de Riemann y la cuarta de las conjeturas, vemos finalmente que

$$B_j(\mathrm{Gr}(r,n)_{\mathbb{C}}) = \deg(P_j(T)) = \begin{cases} 0 & \text{si } j \text{ es impar.} \\ \lambda_{n,r}(j) & \text{si } j \text{ es par y } 0 \leq j \leq r(n-r). \\ 0 & \text{en otro caso.} \end{cases}$$

3 El caso de hipersuperficies diagonales

Nuestro objetivo en esta sección será estudiar el número de puntos de hipersuperficies proyectivas definidas por ecuaciones del tipo

$$a_1 x_1^{c_1} + \cdots + a_j x_j^{c_j} x_0^{c_1 - c_j} + \cdots + a_n x_n^{c_n} x_0^{c_1 - c_n} - a x_0^{c_1} = 0;$$

donde $a_i \in \mathbb{F}_q^\star$, $a \in \mathbb{F}_q$ y los exponentes $c_1 \geq \cdots \geq c_n$ satisfacen ciertas condiciones; y así verificar las conjeturas de Weil para el caso de hipersuperficies diagonales siguiendo las ideas del propio Weil en el famoso artículo [Wei49] donde enunció las conjeturas. Para ello, nos hemos basado principalmente en [BEW98, Ch. 10, 11] para los resultados de sumas de Gauss y Jacobi, [IR90, Ch. 10, 11] para el cálculo de $\mathcal{N}_s$ y algunas pinceladas de [Kow18].

Dado un polinomio $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, denotaremos $N(f)$ al número de puntos de $\mathbb{A}^{\tilde{n}}(\mathbb{F}_q)$ que anulan a f, donde $\tilde{n}$ es el número de variables que aparece en f. De manera análoga, dado $F \in k[x_0, \ldots, x_n]$ homogéneo, $\mathcal{N}(F)$ será el número de puntos de $\mathbb{P}^{\tilde{n}}(\mathbb{F}_q)$ que anulan a F, donde de nuevo $\tilde{n}$ es el número de variables que aparecen en F. $N_s(f)$ y $\mathcal{N}_s(F)$ se definen del mismo modo cambiando $\mathbb{F}_q$ por $\mathbb{F}_{q^s}$. De igual modo usaremos las notaciones $N_s(X)$ y $\mathcal{N}_s(X)$ para el número de puntos $\mathbb{F}_{q^s}$-racionales de una variedad X.

3.1 Caracteres, sumas de Gauss y Jacobi

Los caracteres de un cuerpo finito juegan un papel importante a la hora de expresar el número de raíces de un polinomio y obtener cotas sobre el mismo.

Definición 3.1. Un **caracter multiplicativo** es un homomorfismo de grupos $\chi : \mathbb{F}_q^\star \to \mathbb{C}^\star$. Denotaremos al caracter multiplicativo trivial como ε dado por $\varepsilon(t) = 1$. Será útil extender la definición de un caracter χ a todo el cuerpo $\mathbb{F}_q$, definiendo $\chi(0) = 0$ salvo $\varepsilon(0) = 1$. Un **caracter aditivo** es un homomorfismo de grupos $\psi : (\mathbb{F}_q, +) \to \mathbb{C}^\star$.

En cierto sentido un caracter multiplicativo de $\mathbb{F}_q$ es una forma de reordenar los elementos del cuerpo prestando importancia a la estructura multiplicativa del mismo y olvidándonos de la aditiva. Se deduce fácilmente que si χ es un caracter multiplicativo y ψ aditivo, entonces para $t \in \mathbb{F}_q^\star$ tenemos que $\chi(t)$ es una raíz $(q-1)$-ésima de la unidad y que $\psi(t)$ es una raíz q-ésima de la unidad. Además $\chi(1) = 1$, $\chi(t^{-1}) = \overline{\chi(t)}$ y si χ no es trivial, entonces

$$\sum_{t \in \mathbb{F}_q} \chi(t) = 0,$$

pues existe $a \in \mathbb{F}_q$ con $\chi(a) \neq 1$, por lo que $\chi(a) \sum_{t \in \mathbb{F}_q} \chi(t) = \sum_{t \in \mathbb{F}_q} \chi(at) = \sum_{t' \in \mathbb{F}_q} \chi(t')$, lo que implica que $\sum_{t \in \mathbb{F}_q} \chi(t) = 0$. Análogamente $\psi(0) = 1$, $\psi(-t) = \overline{\psi(t)}$ y si ψ es no trivial

$$\sum_{t \in \mathbb{F}_q} \psi(t) = 0.$$

Los caracteres se pueden definir para cualquier grupo G como la traza de una representación, es decir, una composición

$$\chi : G \xrightarrow{\mathfrak{X}} \mathrm{GL}_n(\mathbb{C}) \xrightarrow{\mathrm{Tr}} \mathbb{C},$$

donde $\mathfrak{X}$ es una representación de G, de decir, un homomorfismo de grupos y Tr es la aplicación traza. A priori, para $n > 1$ esta definición no coincide con 3.1, pero si nos restringimos a representaciones irreducibles, es decir, aquellas que sólo tienen subrepresentaciones triviales, sí coinciden ya que en un grupo abeliano los caracteres irreducibles

son lineales, es decir, $n = 1$ (cf. [Isa94, Cor 2.6]). Esta última referencia refleja la utilidad de la teoría de caracteres en el estudio de grupos finitos. Resulta que el producto elemento a elemento de caracteres es un caracter (cf. [Isa94, 4.1]) y en el caso de grupos abelianos finitos este producto da lugar a un grupo que es isomorfo (aunque no de manera canónica) al de partida (cf. [Con10, Th 3.9]). En particular, el conjunto de caracteres multiplicativo de $\mathbb{F}_q$ es un grupo cíclico de orden $q-1$. De hecho para cada divisor d de $q-1$ podemos expresar $N(x^d - a)$ de forma compacta sumando sobre los caracteres del subgrupo de orden d. Más generalmente,

Lema 3.2. *Sea c un entero positivo, $a \in \mathbb{F}_q$ y sea $d = \gcd(q-1, c)$. Tomemos un caracter multiplicativo de $\mathbb{F}_q$ de orden d. Se tiene que*

$$N(x^c - a) = \sum_{j=0}^{d-1} \chi^j(a).$$

Demostración. Notemos en primer lugar que existe una biyección $\left\{t \in \mathbb{F}_q : t^d = a\right\} \to \left\{t \in \mathbb{F}_q : t^c = a\right\}$ dada por $t \mapsto t^\alpha$, donde α verifica $\alpha c = d$ en $\mathbb{Z}/(q-1)$. Además, si $a \neq 0$ y existe $\gamma \in \mathbb{F}_q$ tal que $\gamma^d = a$, entonces $\left\{t \in \mathbb{F}_q : t^d = a\right\} = \left\{\gamma t : t \in \mathbb{F}_q, t^d = e\right\}$, y los elementos de $\mathbb{F}_q^\star$ cuyo orden divide a d forman un subgrupo cíclico de orden d. Por lo tanto

$$N(x^c - a) = N(x^d - a) = \begin{cases} 1 & \text{si } a = 0, \\ d & \text{si } a \neq 0 \text{ tiene una raíz } d\text{-ésima}, \\ 0 & \text{si } a \neq 0 \text{ no tiene una raíz } d\text{-ésima}. \end{cases}$$

En el primer caso, $\sum_{j=0}^{d-1} \chi^j(a) = \varepsilon(a) = 1$. En el segundo caso, si escribimos $a = \gamma^d$ para cierto $\gamma \in \mathbb{F}_q$ se tiene que

$$\sum_{j=0}^{d-1} \chi^j(a) = \sum_{j=0}^{d-1} \chi^{jd}(\gamma) = \sum_{j=0}^{d-1} \varepsilon(\gamma) = d.$$

Finalmente, si $a \neq 0$ no tiene raíces d-ésimas, veamos que $\chi(a) \neq 1$. Tomemos un generador g de $\mathbb{F}_q^\star$, de modo que $\chi(g) = \exp\left(\frac{2\pi i}{d}\beta\right)$ para β coprimo con d y $a = g^\alpha$ con d no diviendo a α. Entonces $\chi(a) = \exp\left(\frac{2\pi i}{d}\beta\alpha\right) \neq 1$. Con esto en mente,

$$\sum_{j=0}^{d-1} \chi^j(a) = \frac{1 - \chi^d(a)}{1 - \chi(a)} = 0.$$

□

A continuación vamos a definir dos aplicaciones, la traza y la norma, importantes en el estudio de los elementos enteros de una extensión finita del cuerpo de fracciones de un dominio, que aquí utilizaremos para definir caracteres en extensiones finitas de $\mathbb{F}_q$ a partir de los de $\mathbb{F}_q$.

Definición 3.3. Sea L/E una extensión finita de cuerpos. Definimos la **traza** y la **norma** de un elemento $t \in L$, y serán denotadas $T_{L/E}(t)$ y $N_{L/E}(t)$, a la traza y el determinante de la aplicación E-lineal $L \to L$ dada por $t' \mapsto tt'$.

Gracias a las propiedades de la traza y el determinante de una aplicación lineal, tenemos que $T_{L/E} : L \to E$ es una aplicación E-lineal y $N_{L/E} : L^\star \to E^\star$ un homomorfismo de grupos. Propiedades importantes de la traza y la norma son las siguientes (cf. [Neu99, I.2])

Proposición 3.4.

1. *Si L/E es una extensión finita y separable, entonces para $t \in L$*

$$f_t(x) = p_t^d(x) = \prod_\sigma (x - \sigma(t)), \quad T_{L/E}(t) = \sum_\sigma \sigma(t) \quad y \quad N_{L/E}(t) = \prod_\sigma \sigma(t),$$

   donde σ varía en el conjunto de posibles homomorfismos $\sigma : L \to \overline{E}$, $d = [L : E(x)]$, $f_t(x)$ es el polinomio característico de la aplicación $t' \mapsto tt'$ y $p_t(x)$ es el polinomio mínimo de t sobre E.

2. *Si $E \subset M \subset L$ son extensiones finitas, se tiene que*

$$T_{M/E} \circ T_{L/M} = T_{L/E} \quad y \quad N_{M/E} \circ N_{L/M} = N_{L/E}.$$

En el caso de que L/E sea de Galois, el primer apartado nos dice que

$$T_{L/E}(t) = \sum_{\sigma \in \mathrm{Gal}(L/E)} \sigma(t),$$

y análogamente

$$N_{L/E}(x) = \prod_{\sigma \in \mathrm{Gal}(L/E)} \sigma(t).$$

Volviendo al caso que nos concierne, para $t \in \mathbb{F}_{q^s}$

$$T_{\mathbb{F}_{q^s}/\mathbb{F}_q}(t) = t + t^q + t^{q^2} + \cdots + t^{q^{s-1}} \quad \text{y} \quad N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(t) = t^{1+q+q^2+\cdots+q^{s-1}} = t^{\frac{q^s-1}{q-1}},$$

donde hemos usado que $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ es el grupo cíclico generado por el automorfismo de Frobenius $\mathbb{F}_{q^s} \to \mathbb{F}_{q^s}$ dado por $x \mapsto x^q$. Además, de lo dicho en la anterior proposición se deduce que si $t \in \mathbb{F}_{q^s}$ es de grado d sobre $\mathbb{F}_q$ y $x^d - a_1 x^{d-1} + \cdots + (-1)^d a_d \in \mathbb{F}_q[x]$ es su polinomio mínimo entonces

$$T_{\mathbb{F}_{q^s}/\mathbb{F}_q}(t) = \frac{s}{d} a_1, \quad N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(t) = a_d^{\frac{s}{d}}. \tag{3.1}$$

Podemos usar la norma (traza) de la extensión $\mathbb{F}_{q^s}/\mathbb{F}_q$ para «levantar» los caracteres multiplicativos (aditivos) de $\mathbb{F}_{q^s}$:

Definición 3.5. Dado χ caracter multiplicativo de $\mathbb{F}_q$, definimos **el levantamiento de χ a $\mathbb{F}_{q^s}$** como $\chi' = \chi \circ N_{\mathbb{F}_{q^s}/\mathbb{F}_q}$, que resulta ser un caracter de $\mathbb{F}_{q^s}$. De igual modo, dado ψ caracter aditivo de $\mathbb{F}_q$, definimos $\psi' = \psi \circ T_{\mathbb{F}_{q^s}/\mathbb{F}_q}$.

Dado que los elementos de $\mathbb{F}_q$ quedan fijos por el automorfismo de Frobenius se tiene que $\chi'(a) = \chi(a)^s$ para $a \in \mathbb{F}_{q^s}$. Además, dado que $N_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ es sobreyectiva (pues $N_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ es un homomorfismo de grupos cuyo núcleo lo forman los $a \in \mathbb{F}_{q^s}$ tales que $a^{\frac{q^s-1}{q-1}} = 1$, el cual tiene orden $\frac{q^s-1}{q-1}$) se tiene que $\chi' = \rho'$ si y sólo si $\chi = \rho$. En particular, el orden de χ coincide con el de ρ.

Estamos en disposición de definir las sumas de Gauss, un tipo de sumas exponenciales, es decir, sumas de raíces de la unidad, que aparecen con frecuencia en diferentes ámbitos de la teoría de números. Por ejemplo pueden emplearse para dar una prueba de las leyes de reciprocidad cuadrática, cúbica y bicuadrática (cf. [IR90, Ch. 6,9]) o en la ecuación funcional de las funciones L asociada a un caracter de Dirichlet [Kow18, 3.4].

Definición 3.6. Sea χ un caracter multiplicativo de $\mathbb{F}_q$. Denotemos por $\mathbb{F}_p$ el cuerpo con p elementos. Para cada $a \in \mathbb{F}_q$ definimos la **suma de Gauss** del caracter χ respecto a a como

$$g_a(\chi) = \sum_{t \in \mathbb{F}_q} \chi(t)\psi(at),$$

donde $\psi : \mathbb{F}_q \to \mathbb{C}^\star$ es el caracter aditivo dado por $t \mapsto \exp\left(\frac{2\pi i}{p} T_{\mathbb{F}_q/\mathbb{F}_p}(t)\right)$. Denotaremos $g_1(\chi)$ simplemente como $g(\chi)$.

Se pueden definir sumas de Gauss generales para caracteres multiplicativos y aditivos χ y ψ cualesquiera y las propiedades que vamos a ver siguen siendo ciertas (cf. [Kow18, Sec. 2.1]). El motivo de usar $\exp\left(\frac{2\pi i}{p} T_{\mathbb{F}_q/\mathbb{F}_p}(t)\right)$ será justificado en la sección 3.2, donde relacionaremos las sumas de Gauss de un caracter con las correspondientes sumas de sus levantamientos. Veamos a continuación propiedades de las sumas de Gauss.

Proposición 3.7. *Sea χ un caracter multiplicativo de $\mathbb{F}_q$ y sea $a \in \mathbb{F}_q$. Se tiene que*

$$g_a(\chi) = \begin{cases} q & \text{si } a = 0 \text{ y } \chi = \varepsilon, \\ \chi(a^{-1})g(\chi) & \text{si } a \neq 0 \text{ y } \chi \neq \varepsilon, \\ 0 & \text{en caso contrario.} \end{cases}$$

Demostración. Si $a = 0$ y $\chi = \varepsilon$, es trivial. Si $a \neq 0$ y $\chi \neq \varepsilon$,

$$\chi(a)g_a(\chi) = \chi(a)\sum_{t \in \mathbb{F}_q} \chi(t)\psi(at) = \sum_{t \in \mathbb{F}_q} \chi(at)\psi(at) = g(\chi),$$

de donde se deduce el resultado. Si $a \neq 0$ y $\chi = \varepsilon$,

$$g_a(\varepsilon) = \sum_{t \in \mathbb{F}_q} \psi(at) = \sum_{t' \in \mathbb{F}_q} \psi(t') = 0.$$

Si $a = 0$ y $\chi \neq \varepsilon$,

$$g_0(\chi) = \sum_{t \in \mathbb{F}_q} \chi(t) = 0.$$

□

Proposición 3.8. *Si χ es un caracter multiplicativo no trivial de $\mathbb{F}_q$,*

$$|g(\chi)| = q^{1/2}.$$

Demostración. Tenemos por un lado que

$$\sum_{a \in \mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)} = \sum_{a \in \mathbb{F}_q^\star} \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)} = (q-1)\left|g(\chi)\right|^2.$$

Por otro lado,

$$\begin{aligned} \sum_{a \in \mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)} &= \sum_{a \in \mathbb{F}_q} \left(\sum_{t \in \mathbb{F}_q} \chi(t)\psi(at)\right) \overline{\left(\sum_{t' \in \mathbb{F}_q} \chi(t')\psi(at')\right)} \\ &= \sum_{t \in \mathbb{F}_q} \sum_{t' \in \mathbb{F}_q} \chi(t)\overline{\chi(t')} \sum_{a \in \mathbb{F}_q} \psi(a(t-t')) \\ &= \sum_{t \in \mathbb{F}_q} \sum_{t' \in \mathbb{F}_q} \chi(t)\overline{\chi(t')}q\delta_{tt'} = (q-1)q, \end{aligned}$$

donde $\delta_{tt'} = 1$ si $t = t'$ y 0 en otro caso. El resultado se deduce de igualar ambas expresiones. □

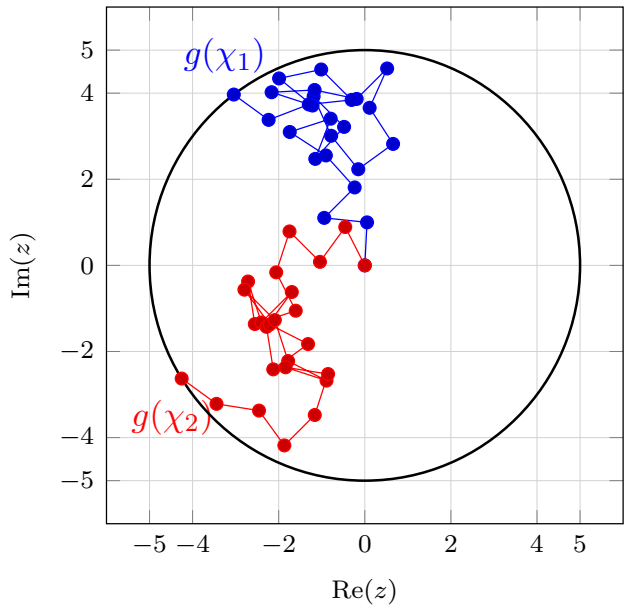


Figura 1: Sumas de Gauss de $\mathbb{F}_{25}$:
Para un generador g de $\mathbb{F}_{25}^{\star}$, $\chi_1(g) = e^{\frac{2\pi i}{24}}$ y $\chi_2(g) = e^{\frac{6\pi i}{24}}$.

Este resultado nos permite realizar la siguiente observación, descrita con más detalle en [Roj09]. Dado que el caracter $\psi : \mathbb{F}_q \to \mathbb{C}^{\star}$ distribuye de forma uniforme los elementos de $\mathbb{F}_q$ en el sentido de que para cada $a \in \{1, \ldots, p-1\}$ tenemos que $\sum_{t\in\mathbb{F}_q} \psi(at) = 0$, es natural pensar que una función f partiendo de un conjunto finito A en $\mathbb{F}_q$ estará «bien distribuida» si para cada $a \in \{1, \ldots, p-1\}$ el módulo del vector media

$$\frac{1}{\#A} \sum_{t\in\mathbb{F}_q} \psi(at) \# \{x \in A : f(x) = t\}$$

es pequeño respecto a 1. En particular para d divisor pequeño de $q-1$, la función $\mathbb{F}_q \to \mathbb{F}_q$ dada por $t \mapsto t^d$ está «bien distribuida» pues

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} \psi(at) \# \left\{x \in \mathbb{F}_q : x^d = t\right\} &= \sum_{t\in\mathbb{F}_q} \psi(at) N(x^d - t) = \sum_{t\in\mathbb{F}_q} \psi(at) \sum_{j=0}^{d} \chi^j(t) \\ &= \sum_{j=0}^{d} \sum_{t\in\mathbb{F}_q} \psi(at)\chi^j(t) = \sum_{j=0}^{d} g_a(\chi) = \sum_{j=1}^{d} g_a(\chi)\end{aligned}$$

tiene módulo menor o igual que $(d-1)q^{1/2}$.

También como consecuencia de las proposiciones anteriores obtenemos fácilmente que $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$ y por lo tanto

$$g(\chi)g(\overline{\chi}) = \chi(-1)q.$$

Esta igualdad puede recordarnos a la ecuación de reflexión de la función $\Gamma(z)$,

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)},$$

y es que existe una analogía entre el papel jugado por las sumas de Gauss $g(\chi)$ en cuerpos finitos y el de la función $\Gamma(z)$ para el caso continuo, que recordemos esta definida para cada $z \in \mathbb{C}$ con parte real positiva como

$$\Gamma(z) = \int_0^{+\infty} e^{-x} x^z \frac{dx}{x}.$$

Dicha analogía se sustenta en el hecho de que $x \mapsto e^{-x}$ es un caracter aditivo de $(\mathbb{R}, +)$ y para cada $z \in \mathbb{C}$, $x \mapsto x^z$ es un caracter multiplicativo del grupo multiplicativo de $\mathbb{R}^+$. Nótese que igual que para cada $a \in \mathbb{F}_q$ tenemos que $\sum_{t\in\mathbb{F}_q} f(at) = \sum_{t\in\mathbb{F}_q} f(t)$, en el lado continuo la medida $\frac{dx}{x}$ es invariante por «traslaciones multiplicativas», es decir, para $a > 0$,

$$\int_0^{+\infty} f(ax)\frac{dx}{x} = \int_0^{+\infty} f(x)\frac{dx}{x}.$$

La siguiente definición viene motivada por el hecho de que podemos expresar el número de soluciones de ecuaciones del tipo $x_1^{d_1} + \cdots + x_n^{d_n} = a$ en función de las tratadas en el Lema 3.2:

$$N(x_1^{d_1} + \cdots + x_n^{d_n} - a) = \sum_{c_1+\cdots+c_n=a} N(x^{d_1} - c_1)\cdots N(x^{d_n} - c_n).$$

Definición 3.9. Sean $\chi_1, \chi_2, \ldots, \chi_r$ caracteres multiplicativos de $\mathbb{F}_q$. Definimos las **sumas de Jacobi** como

$$J(\chi_1, \chi_2, \ldots, \chi_r) = \sum_{c_1+\cdots+c_r=1} \chi_1(c_1)\cdots\chi_r(c_r),$$
$$J_0(\chi_1, \chi_2, \ldots, \chi_r) = \sum_{c_1+\cdots+c_r=0} \chi_1(c_1)\cdots\chi_r(c_r),$$

donde los coeficientes c_i toman sus posibles valores en $\mathbb{F}_q$.

Nótese que cada suma de Jacobi tiene q^{r-1} sumandos, que $J(\chi) = \chi(1) = 1$ y que para cualquier $a \in \mathbb{F}_q^\star$

$$\sum_{c_1+\cdots+c_r=a} \chi_1(c_1)\cdots\chi_r(c_r) = \sum_{c_1'+\cdots+c_r'=1} \chi_1(c_1'a)\cdots\chi_r(c_r'a) = \chi_1\cdots\chi_r(a)J(\chi_1, \chi_2, \ldots, \chi_r). \tag{3.2}$$

Exploremos las principales propiedades de las sumas de Jacobi:

Proposición 3.10. *Sean $\chi_1, \chi_2, \ldots, \chi_r$ ($r \geq 2$) caracteres multiplicativos de $\mathbb{F}_q$. Se tiene que*

$$J_0(\chi_1, \ldots, \chi_r) = \begin{cases} q^{r-1} & \text{si } \chi_1 = \chi_2 = \cdots = \chi_r = \varepsilon, \\ -(q-1)J(\chi_1, \ldots, \chi_r) = & \\ \chi_r(-1)(q-1)J(\chi_1, \ldots, \chi_{r-1}) & \text{si } \chi_i \neq \varepsilon \text{ para todo } i = 1, \ldots, r \text{ y } \chi_1\cdots\chi_r = \varepsilon, \\ 0 & \text{en caso contrario.} \end{cases}$$

$$J(\chi_1, \ldots, \chi_r) = \begin{cases} q^{r-1} & \text{si } \chi_1 = \chi_2 = \cdots = \chi_r = \varepsilon, \\ -qJ(\chi_1, \ldots, \chi_{r-1}) & \text{si } \chi_i \neq \varepsilon \text{ para todo } i = 1, \ldots, r \text{ y } \chi_1\cdots\chi_{r-1} = \varepsilon, \\ J(\chi_1\cdots\chi_{r-1}, \chi_r)J(\chi_1, \ldots, \chi_{r-1}) & \text{si } \chi_i \neq \varepsilon \text{ para todo } i = 1, \ldots, r \text{ y } \chi_1\cdots\chi_{r-1} \neq \varepsilon, \\ 0 & \text{en caso contrario.} \end{cases}$$

Demostración. Empecemos con la primera de las igualdades. De nuevo el resultado se obtendrá al agrupar los sumandos de una determinada suma de dos formas diferentes. Por un lado tenemos que

$$\sum_{a\in\mathbb{F}_q}\sum_{c_1+\cdots+c_r=a}\chi(c_1)\cdots\chi(c_r)=\prod_{i=1}^{r}\sum_{c_i\in\mathbb{F}_q}\chi_i(c_i)=\begin{cases}q^r & \text{si } \chi_1=\chi_2=\cdots=\chi_r=\varepsilon,\\ 0 & \text{en caso contrario.}\end{cases}$$

Por otra parte,

$$\begin{aligned}\sum_{a\in\mathbb{F}_q}\sum_{c_1+\cdots+c_r=a}\chi(c_1)\cdots\chi(c_r)&=J_0(\chi_1,\ldots,\chi_r)+\sum_{a\in\mathbb{F}_q^\star}\sum_{c_1+\cdots+c_r=a}\chi_1(c_1)\cdots\chi_r(c_r)\\&=J_0(\chi_1,\ldots,\chi_r)+\sum_{a\in\mathbb{F}_q^\star}J(\chi_1,\ldots,\chi_r)\chi_1\cdots\chi_r(a)\\&=\begin{cases}J_0(\chi_1,\ldots,\chi_r)+(q-1)J(\chi_1,\ldots,\chi_r) & \text{si } \chi_1\ldots\chi_r=\varepsilon,\\ J_0(\chi_1,\ldots,\chi_r) & \text{en caso contrario.}\end{cases}\end{aligned}$$

De donde deducimos la primera igualdad salvo que $J_0(\chi_1,\ldots,\chi_r)=\chi_r(-1)(q-1)J(\chi_1,\ldots,\chi_{r-1})$ si $\chi_i\neq\varepsilon$ para todo $i=1,\ldots,r$ y $\chi_1\cdots\chi_r=\varepsilon$. Veamos esto último:

$$\begin{aligned}J_0(\chi_1,\ldots,\chi_r)&=\sum_{c_1+\cdots+c_r=0}\chi_1(c_1)\ldots\chi_r(c_r)=\sum_{c_r\in\mathbb{F}_q^\star}\chi_r(c_r)\sum_{c_1+\cdots+c_{r-1}=-c_r}\chi_1(c_1)\cdots\chi_{r-1}(c_{r-1})\\&=\sum_{c_r\in\mathbb{F}_q^\star}\chi_r(c_r)\chi_1\cdots\chi_{r-1}(-c_r)J(\chi_1,\ldots,\chi_{r-1})\\&=\chi_r(-1)J(\chi_1,\ldots,\chi_{r-1})\sum_{c_r\in\mathbb{F}_q^\star}\chi_1\cdots\chi_r(-c_r)\\&=\chi_r(-1)(q-1)J(\chi_1\ldots,\chi_{r-1}).\end{aligned}$$

Probemos ahora la segunda igualdad. Si todos los caracteres son triviales, se sigue inmeditamente que $J(\chi_1,\ldots,\chi_r)=q^{r-1}$. Si alguno de ellos es no trivial pero $\chi_r=\varepsilon$,

$$\begin{aligned}J(\chi_1,\ldots,\chi_{r-1},\varepsilon)&=\sum_{c_1+\cdots+c_r=1}\chi_1(c_1)\cdots\chi_{r-1}(c_{r-1})\varepsilon(c_r)\\&=\sum_{(c_1,\ldots,c_{r-1})\in\mathbb{F}_q^n}\chi_1(c_1)\cdots\chi_{r-1}(c_{r-1})=\prod_{i=1}^{r-1}\sum_{c_i\in\mathbb{F}_q}\chi_i(c_i)=0.\end{aligned}$$

Si todos ellos son no triviales,

$$\begin{aligned}J(\chi_1,\ldots,\chi_r)&=\sum_{c_1+\cdots+c_r=1}\chi_1(c_1)\cdots\chi_r(c_r)\\&=\sum_{c_1+\cdots+c_{r-1}=0}\chi_1(c_1)\cdots\chi_r(c_r)+\sum_{c_r\neq1}\sum_{c_1+\cdots+c_{r-1}=1-c_r}\chi_1(c_1)\cdots\chi_r(c_r)\\&=J_0(\chi_1,\ldots,\chi_{r-1})+J(\chi_1,\ldots,\chi_{r-1})\sum_{c_r\neq1}\chi_1\cdots\chi_r(1-c_r)\chi_r(c_r)\\&=J_0(\chi_1,\ldots,\chi_{r-1})+J(\chi_1,\ldots,\chi_{r-1})\left(J(\chi_1\cdots\chi_{r-1},\chi_r)-\chi_1\cdots\chi_{r-1}(0)\right).\end{aligned}$$

Si $\chi_1\cdots\chi_{r-1}=\varepsilon$, entonces $J_0(\chi_1,\ldots,\chi_{r-1})=-(q-1)J(\chi_1,\ldots,\chi_{r-1})$ y $J(\chi_1\cdots\chi_{r-1},\chi_r)=0$, por lo tanto

$$J(\chi_1,\ldots,\chi_r)=-(q-1)J(\chi_1,\ldots,\chi_{r-1})-J(\chi_1,\ldots,\chi_{r-1})=-qJ(\chi_1,\ldots,\chi_{r-1}).$$

Si por el contrario $\chi_1 \cdots \chi_{r-1} \neq \varepsilon$, entonces $J_0(\chi_1, \ldots, \chi_{r-1}) = \chi_1 \cdots \chi_{r-1}(0) = 0$, de donde deducimos finalmente

$$J(\chi_1, \ldots, \chi_r) = J(\chi_1, \ldots, \chi_{r-1}) J(\chi_1 \cdots \chi_{r-1}, \chi_r).$$

□

Se deduce de la primera igualdad de la anterior proposición que si $\chi_1, \ldots, \chi_r$ son no triviales y $\chi_1 \cdots \chi_r = \varepsilon$,

$$J(\chi_1, \ldots, \chi_r) = -\chi_r(-1) J(\chi_1 \ldots, \chi_{r-1}). \tag{3.3}$$

La siguiente proposición muestra la conexión existente entre las sumas de Gauss y de Jacobi, que será de gran importancia pues nos permitirá conocer el módulo de las mismas y también construir levantamientos vía Hasse-Daveport.

Proposición 3.11. *Sean $\chi_1, \ldots, \chi_r$ caracteres multiplicativos no triviales de $\mathbb{F}_q$. Se tiene que*

$$J(\chi_1, \ldots, \chi_r) = \begin{cases} \dfrac{-1}{q} g(\chi_1) \cdots g(\chi_r) & \text{si } \chi_1 \cdots \chi_r = \varepsilon, \\ \dfrac{g(\chi_1) \cdots g(\chi_r)}{g(\chi_1 \cdots \chi_r)} & \text{si } \chi_1 \cdots \chi_r \neq \varepsilon \end{cases}$$

Demostración. Lo probamos por inducción en r. Para $r = 1$, el resultado es trivial.

Supongamos ahora que $r \geq 2$. Si $\chi_1 \cdots \chi_r = \varepsilon$, entonces $\chi_1 \cdots \chi_{r-1} \neq \varepsilon$. Se sigue de la Proposición 3.10 y de la hipótesis de inducción que

$$\begin{aligned} J(\chi_1, \ldots, \chi_r) &= J(\chi_1 \cdots \chi_{r-1}, \chi_r) J(\chi_1, \ldots, \chi_{r-1}) \\ &= \frac{-1}{q} g(\chi_1 \cdots \chi_{r-1}) g(\chi_r) \frac{g(\chi_1) \cdots g(\chi_{r-1})}{g(\chi_1 \cdots \chi_{r-1})} = \frac{-1}{q} g(\chi_1) \cdots g(\chi_r). \end{aligned}$$

Si $\chi_1 \cdots \chi_r \neq \varepsilon$ pero $\chi_1 \cdots \chi_{r-1} = \varepsilon$, entonces $\chi_r = \chi_1 \cdots \chi_r$. De nuevo de la Proposición 3.10 y de la hipótesis de inducción

$$J(\chi_1, \ldots, \chi_r) = -q J(\chi_1, \ldots, \chi_{r-1}) = -q \frac{-1}{q} g(\chi_1) \cdots g(\chi_{r-1}) = \frac{g(\chi_1) \cdots g(\chi_{r-1}) g(\chi_r)}{g(\chi_1 \cdots \chi_r)}.$$

Finalmente, si $\chi_1 \cdots \chi_r \neq \varepsilon$ y $\chi_1 \cdots \chi_{r-1} \neq \varepsilon$, entonces

$$\begin{aligned} J(\chi_1, \ldots, \chi_r) &= J(\chi_1 \cdots \chi_{r-1}, \chi_r) J(\chi_1, \ldots, \chi_{r-1}) \\ &= \frac{g(\chi_1 \cdots \chi_{r-1}) g(\chi_r)}{g(\chi_1 \cdots \chi_r)} \frac{g(\chi_1) \cdots g(\chi_r)}{g(\chi_1 \cdots \chi_{r-1})} = \frac{g(\chi_1) \cdots g(\chi_r)}{g(\chi_1 \cdots \chi_r)}. \end{aligned}$$

□

Observemos que para el caso $r = 2$, si tenemos dos caracteres no triviales χ_1, χ_2 con $\chi_1 \chi_2 \neq \varepsilon$, la relación

$$J(\chi_1, \chi_2) = \frac{g(\chi_1) g(\chi_2)}{g(\chi_1 \chi_2)}$$

nos sugiere que el análogo de las sumas Jacobi para el caso continuo es la función beta definida para $z, w \in \mathbb{C}$ con parte real positiva como

$$B(z, w) = \int_0^1 x^z (1 - x)^w dx,$$

pues esta última verifica

$$B(z, w) = \frac{\Gamma(z) \Gamma(w)}{\Gamma(z + w)}.$$

Corolario 3.12. *Sean $\chi_1, \ldots, \chi_r$ caracteres multiplicativos no triviales de $\mathbb{F}_q$. Se tiene que*

$$|J(\chi_1, \ldots, \chi_r)| = \begin{cases} q^{\frac{r}{2}-1} & si\ \chi_1 \cdots \chi_r = \varepsilon, \\ q^{\frac{r-1}{2}} & si\ \chi_1 \cdots \chi_r \neq \varepsilon. \end{cases}$$

3.2 La relación de Hasse-Davenport

Recordemos que para cada caracter multiplicativo χ de $\mathbb{F}_q$, podemos definir $\chi' = \chi \circ N_{\mathbb{F}_{q^s}/\mathbb{F}_q}$, que resulta ser un caracter de $\mathbb{F}_{q^s}$. El objetivo de esta sección es comparar $g(\chi)$ con la suma de Gauss de χ' correspondiente, es decir,

$$g(\chi') = \sum_{t \in \mathbb{F}_{q^s}} \chi'(t)\psi'(t),$$

donde $\psi'(t) = \exp(\frac{2\pi i}{p} T_{\mathbb{F}_{q^s}/\mathbb{F}_p}(t)) = \psi \circ T_{\mathbb{F}_{q^s}/\mathbb{F}_q}$. Fijaremos χ un caracter multiplicativo de $\mathbb{F}_q$. Dado un polinomio mónico $f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_d \in \mathbb{F}_q[x]$, definimos $\lambda(f) = \psi(a_1)\chi(a_n)$. Empezamos por un lema previo:

Lema 3.13.

1. *Para polinomios mónicos $f, g \in \mathbb{F}_q[x]$, tenemos que $\lambda(fg) = \lambda(f)\lambda(g)$.*
2. *Sea $t \in \mathbb{F}_{q^s}$ y $d = [\mathbb{F}_{q^s} : \mathbb{F}_q(t)]$. Sea $f(x) \in \mathbb{F}_q[x]$ su polinomio mínimo sobre $\mathbb{F}_q$. Entonces*
$$\lambda(f)^{s/d} = \chi'(t)\psi'(t).$$
3. *Se tiene que*
$$g(\chi') = \sum_{d|s} \sum_{f \in A_d} d\lambda(f)^{s/d},$$
donde A_d es el conjunto de polinomios mónicos irreducibles de $\mathbb{F}_q[x]$ de grado d.

Demostración. 1. Escribamos $f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_d$ y $g(x) = x^m - b_1 x^{n-1} + \cdots + (-1)^d b_d$. Entonces $f(x)g(x) = x^{n+m} - (a_1 + b_1)x^{n+m-1} + \cdots + (-1)^{n+m} a_n b_m$, luego

$$\lambda(fg) = \psi(a_1 + b_1)\chi(a_n b_m) = \psi(a_1)\psi(b_1)\chi(a_n)\chi(b_m) = \lambda(f)\lambda(g).$$

2. Sea d el grado de t sobre $\mathbb{F}_q$ y $x^d - a_1 x^{d-1} + \cdots + (-1)^d a_d$ su polinomio mínimo. Recordando la relación 3.1, tenemos que

$$\lambda(f)^{s/d} = \psi(a_1)^{s/d}\chi(a_n)^{s/d} = \psi(\frac{s}{d}a_1)\chi(a_d^{s/d}) = \psi(T_{\mathbb{F}_{q^s}/\mathbb{F}_q}(t))\chi(N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(t)) = \psi'(t)\chi'(t).$$

3. Gracias al apartado anterior tenemos que

$$g(\chi') = \sum_{t \in \mathbb{F}_{q^s}} \chi'(t)\psi'(t) = \sum_{t \in \mathbb{F}_{q^s}} \lambda(f_t)^{s/\deg(f_t)},$$

donde $f_t \in \mathbb{F}_q[x]$ es el polinomio mínimo de t sobre $\mathbb{F}_q$. Dado que todo polinomio mínimo tiene grado un divisor de s y que dado un polinomio mónico irreducible de grado d divisor de s tiene sus d raíces en $\mathbb{F}_{q^s}$, deducimos el resultado.

□

El último ingrediente antes de probar la relación de Hasse-Davenport requiere de la utilización de series formales introducidas en la Sección 2.1. Además, para que el enunciado de la siguiente proposición tenga sentido, debemos definir $\lambda(1) = 1$.

Lema 3.14. *Se tiene la siguiente igualdad en* $\mathbb{C}[\![T]\!]$*:*

$$1 + g(\chi)T = \prod_{f \in A} \frac{1}{1 - \lambda(f)T^{\deg f}} \tag{3.4}$$

donde A *es el conjunto de polinomios mónicos irreducibles en* $\mathbb{F}_q[x]$*.*

Demostración. Notemos en primer lugar que el producto a la derecha de la igualdad tiene sentido gracias al Ejemplo 2.3. Desarrollando los denominadores, dicho producto es igual a

$$\prod_{f \in A} (1 + \lambda(f)T^{\deg f} + \lambda(f)^2 T^{2 \deg f} + \dots).$$

El coeficiente d-ésimo de la serie que define el producto coincide con $\sum_{f \in B_d} \lambda(f)$, donde B_d es el conjunto de polinomios mónicos en $\mathbb{F}_q[x]$ de grado d, ya que todo polinomio mónico se descompone de forma única como producto de polinomios mónicos irreducibles. Estudiemos ahora los coeficientes $\sum_{f \in B_d} \lambda(f)$ para $d \geq 1$. Si $d = 1$,

$$\sum_{f \in B_1} \lambda(f) = \sum_{t \in \mathbb{F}_{q^s}} \lambda(y - t) = \sum_{t \in \mathbb{F}_{q^s}} \chi(t)\psi(t) = g(\chi);$$

y para $d > 1$,

$$\begin{aligned} \sum_{f \in B_d} \lambda(f) &= \sum_{(a_1, \dots, a_d) \in \mathbb{F}_q^d} \lambda(y^d - a_1 y^{d-1} + \dots + (-1)^d a_d) \\ &= q^{d-2} \sum_{(a_1, a_d) \in \mathbb{F}_q^2} \chi(a_d)\psi(a_1) = q^{d-2} \left(\sum_{a_d \in \mathbb{F}_q} \chi(a_d) \right) \left(\sum_{a_1 \in \mathbb{F}_q} \psi(a_1) \right) = 0. \end{aligned}$$

□

Ya estamos en disposición de probar la relación de Hasse-Daveport:

Teorema 3.15 (Relación de Hasse-Daveport)**.**

$$g(\chi') = (-1)^{s+1} g(\chi)^s$$

Demostración. Partimos de la igualdad obtenida en la proposición anterior. Tomamos derivada del logaritmo y multiplicamos por T:

$$\frac{g(\chi)T}{1 + g(\chi)T} = \sum_{f \in A} \frac{\lambda(f) d T^d}{1 - \lambda(f)T^d}.$$

Ahora desarrollamos los denominadores en la anterior igualdad. Por un lado,

$$\frac{g(\chi)T}{1 + g(\chi)T} = g(\chi)T \sum_{s=0}^{\infty} (-1)^s g(\chi)^s T^s = \sum_{s=1}^{\infty} (-1)^{s+1} g(\chi)^s T^s.$$

Por otro lado, se tiene que

$$\sum_{f\in A}\frac{\lambda(f)dT^d}{1-\lambda(f)T^d}=\sum_{d=1}^{\infty}\sum_{f\in A_d}\lambda(f)dT^d\sum_{l=0}^{\infty}\lambda(f)^lT^{ld}=\sum_{l=1}^{\infty}\sum_{d=1}^{\infty}\sum_{f\in A_d}\lambda(f)^ldT^{ld}.$$

Igualando coeficientes llegamos a

$$(-1)^{s+1}g(\chi)^s=\sum_{d|s}\sum_{f\in A_d}\lambda(f)^{s/d}d,$$

luego del tercer apartado del Lema 3.13 obtenemos el resultado. □

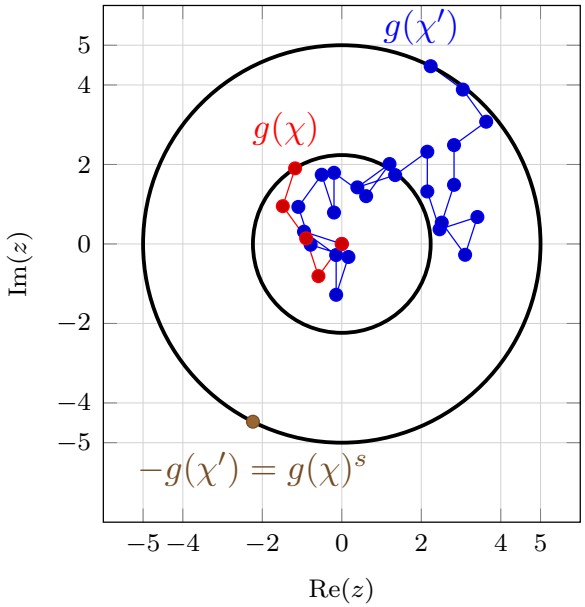


Figura 2: Relación de Hasse-Davenport, donde $q=5$, $s=2$ y $\chi(g)=e^{\frac{2\pi i}{4}}$ para un generador de $\mathbb{F}_5^\star$.

Finalmente, usaremos la Proposición 3.11, donde relacionábamos las sumas de Gauss y de Jacobi, para extender la relación de Hasse-Davenport a estas últimas.

Corolario 3.16. *Sean $\chi_1,\dots,\chi_r$ caracteres multiplicativos de $\mathbb{F}_q$. Se tiene que*

$$J(\chi_1',\dots,\chi_r')=(-1)^{(s+1)(r+1)}J(\chi_1,\dots,\chi_r)^s$$

Demostración. Si $\chi_1\cdots\chi_r=\varepsilon$, tenemos que

$$\begin{aligned}J(\chi_1',\dots,\chi_r')&=\frac{-1}{q^s}g(\chi_1')\cdots g(\chi_r')=\frac{-1}{q^s}(-1)^{r(s+1)}g(\chi_1)^s\cdots g(\chi_r)^s\\&=(-1)^{(r+1)(s+1)}\left(\frac{-1}{q}g(\chi_1)\cdots g(\chi_r)\right)^s=(-1)^{(r+1)(s+1)}J(\chi_1,\dots,\chi_r)^s.\end{aligned}$$

Si por el contrario $\chi_1\cdots\chi_r\neq\varepsilon$,

$$\begin{aligned}J(\chi_1',\dots,\chi_r')&=\frac{g(\chi_1')\cdots g(\chi_r')}{g(\chi_1'\cdots\chi_r')}=\frac{(-1)^{(s+1)r}g(\chi_1)^s\cdots g(\chi_r)^s}{(-1)^{(s+1)}g(\chi_1\cdots\chi_r)^s}\\&=(-1)^{(s+1)(r+1)}\left(\frac{g(\chi_1)\cdots g(\chi_r)}{g(\chi_1\cdots\chi_r)}\right)^s=(-1)^{(r+1)(s+1)}J(\chi_1,\dots,\chi_r).\end{aligned}$$

Nótese que hemos usado que $(\chi_1\cdots\chi_r)'=\chi_1'\cdots\chi_r'$. □

3.3 Cálculo de $\mathcal{N}_s$ y conjeturas para hipersuperficies diagonales

Una vez introducidas las principales propiedades de las sumas de Gauss y Jacobi, estamos en disposición de estudiar el número de puntos en hipersuperficies afines definidas por polinomios del tipo

$$a_1x_1^{c_1} + \cdots + a_nx_n^{c_n} - a$$

en las sucesivas extensiones finitas de $\mathbb{F}_q$.

Teorema 3.17. *Sean $c_1, \ldots, c_n$ enteros positivos. Sean $a_1, \ldots, a_n \in \mathbb{F}_q^\star$ y $a \in \mathbb{F}_q$. Sean $d_i = \gcd(q-1, c_i)$ y tomemos χ_i caracter multiplicativo de $\mathbb{F}_q$ de orden d_i. Sea*

$$f(x_1, \ldots, x_n) = a_1x_1^{c_1} + \cdots + a_nx_n^{c_n} - a.$$

Se tiene que

$$N(f) = \begin{cases} q^{n-1} + \displaystyle\sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(aa_1^{-1}) \ldots \chi_n^{j_n}(aa_n^{-1}) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}) & \text{si } a \neq 0, \\ q^{n-1} - (q-1) \displaystyle\sum_{\substack{j_1=1 \\ \chi_1^{j_1} \cdots \chi_n^{j_n} = \varepsilon}}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \ldots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}) & \text{si } a = 0. \end{cases}$$

Demostración. Tenemos que

$$\begin{aligned} N(f) &= \sum_{b_1+\cdots+b_n=a} N(a_1x_1^{c_1} - b_1) \cdots N(a_nx_n^{c_n} - b_n) \\ &= \sum_{b_1+\cdots+b_n=a} \left(\sum_{j_1=0}^{d_1-1} \chi_1^{j_1}(b_1a_1^{-1}) \right) \cdots \left(\sum_{j_n=0}^{d_n-1} \chi_n^{j_n}(b_1a_n^{-1}) \right) \\ &= \sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) \sum_{b_1+\cdots+b_n=a} \chi_1^{j_1}(b_1) \cdots \chi_n^{j_n}(b_n). \end{aligned}$$

Si a es no nulo, teniendo en cuenta 3.2 y la Proposición 3.10 la suma anterior es igual a

$$\begin{aligned} &\sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(a_1^{-1}a) \cdots \chi_n^{j_n}(a_n^{-1}a) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}) \\ &= q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}a) \cdots \chi_n^{j_n}(a_n^{-1}a) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}). \end{aligned}$$

Si $a = 0$, de nuevo gracias a la Proposición 3.10 lo que obtenemos es

$$\begin{aligned} &\sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J_0(\chi_1^{j_1}, \ldots, \chi_n^{j_n}) \\ &= q^{n-1} - (q-1) \sum_{\substack{j_1=1 \\ \chi_1^{j_1} \cdots \chi_n^{j_n} = \varepsilon}}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \ldots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}). \end{aligned}$$

□

Utilizando al relación de Hasse-Davenport y recordando que para $a \in \mathbb{F}_q$ se tiene que $\chi'(a) = \chi(a)^s$, obtenemos el siguiente corolario inmediato

Corolario 3.18. *En las condiciones del teorema anterior y suponiendo que para cada i $\gcd(q^s - 1, c_i)$ no depende de s, se tiene que*

$$N_s(f) = \begin{cases} \left(q^{n-1}\right)^s - (-1)^n \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} [(-1)^{n+1} \chi_1^{j_1}(aa_1^{-1}) \dots \chi_n^{j_n}(aa_n^{-1}) J(\chi_1^{j_1}, \dots, \chi_n^{j_n})]^s & \text{si } a \neq 0, \\ \left(q^{n-1}\right)^s - (-1)^{n+1} \sum_{\substack{j_1=1 \\ \chi_1^{j_1} \dots \chi_n^{j_n} = \varepsilon}}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} [q(-1)^{n+1} \chi_1^{j_1}(a_1^{-1}) \dots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \dots, \chi_n^{j_n})]^s \\ \quad -(-1)^n \sum_{\substack{j_1=1 \\ \chi_1^{j_1} \dots \chi_n^{j_n} = \varepsilon}}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} [(-1)^{n+1} \chi_1^{j_1}(a_1^{-1}) \dots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \dots, \chi_n^{j_n})]^s & \text{si } a = 0. \end{cases}$$

Necesitamos trabajar con variedades proyectivas a la hora de considerar las conjeturas de Weil. Por ello sea f como en el teorema anterior y consideremos la clausura proyectiva de la hipersuperficie asociada a f, cuyos puntos cerrados se corresponden con los ceros en $\mathbb{P}^n(\mathbb{F}_q)$ de

$$F(x_0, \dots, x_n) = a_1 x_1^{c_1} + \cdots + a_j x_j^{c_j} x_0^{c_1 - c_j} + \cdots + a_n x_n^{c_n} x_0^{c_1 - c_n} - a x_0^{c_1}.$$

Supondremos que los l primeros exponentes son iguales y máximos ($c_1 = \cdots = c_l > c_{l+1} \geq c_n$). Contando puntos afines y puntos en el hiperplano del infinito ($x_0 = 0$) por separado se tiene que

$$\mathcal{N}_s(F) = N_s(f) + (q^s)^{n-l} \mathcal{N}_s(a_1 x_1^{c_1} + \cdots + a_l x_l^{c_l}) + \mathcal{N}_s(\mathbb{P}^{n-l-1}(\mathbb{F}_{q^s}))$$

donde el último sumando aparece sólo si $l < n$ y corresponde con las soluciones en las que $x_0 = x_1 = \cdots = x_l = 0$ y el factor $(q^s)^{n-l}$ en el segundo sumando se debe a las q^s opciones que hay en cada uno de las últimas $n - l$ coordenadas correspondientes a las soluciones de $a_1 x_1^{c_1} + \cdots + a_l x_l^{c_l}$ en $\mathbb{P}^{l-1}(\mathbb{F}_{q^s})$.

Pasamos a probar las conjeturas de Weil para **hipersuperficies diagonales**, que son variedades proyectivas X definidas por polinomios del tipo

$$F(x_0, \dots, x_n) = a_0 x_0^m + \cdots + a_n x_n^m \tag{3.5}$$

para m divisor de $q - 1$. Recordemos que X tiene dimensión $n - 1$ básicamente por [GW10, 5.31]. Por otro lado es sencillo comprobar que se trata de una variedad no singular. Como sabemos contar puntos afines, la estrategia es trabajar con el cono de X, es decir el conjunto de ceros de F en $\mathbb{A}^{n+1}(\mathbb{F}_{q^s})$. Luego debemos restar el punto correspondiente al origen y dividir por el número de representantes que tiene cada punto proyectivo, es decir,

$$\mathcal{N}_s(X) = \frac{N_s(F) - 1}{q^s - 1}.$$

Aplicando el Corolario 3.18 (nótese que ahora el polinomio tiene $n + 1$ variables):

$$N_s(F) = (q^n)^s - (-1)^n (q^s - 1) \sum_{\substack{j_0=1 \\ \chi^{j_0} \dots \chi^{j_n} = \varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} [(-1)^n \chi^{j_0}(a_0^{-1}) \dots \chi^{j_n}(a_n^{-1}) J(\chi^{j_0}, \dots, \chi^{j_n})]^s,$$

para χ caracter multiplicativo de orden m en $\mathbb{F}_q$. Por lo tanto

$$\mathcal{N}_s(X) = \frac{(q^n)^s - 1}{q^s - 1} - (-1)^n \sum_{\substack{j_0=1 \\ \chi^{j_0}\dots\chi^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} [(-1)^n \chi^{j_0}(a_0^{-1}) \dots \chi^{j_n}(a_n^{-1}) J(\chi^{j_0}, \dots, \chi^{j_n})]^s$$
$$= (q^{n-1})^s + \cdots + 1 - (-1)^n \sum_{\substack{j_0=1 \\ \chi^{j_0}\dots\chi^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} [(-1)^n \chi^{j_0}(a_0^{-1}) \dots \chi^{j_n}(a_n^{-1}) J(\chi^{j_0}, \dots, \chi^{j_n})]^s.$$

Teniendo en mente los lemas 2.12 y 2.13 podemos ver:

1. **Racionalidad**: La función zeta de X es racional

   $$Z(X,T) = \frac{R(T)^{(-1)^n}}{(1-T)\cdots(1-q^{n-1}T)}$$

   donde

   $$R(T) = \prod_i (1 - \alpha_i T); \quad \alpha_i = (-1)^n \chi^{j_0}(a_0^{-1}) \dots \chi^{j_n}(a_n^{-1}) J(\chi^{j_0}, \dots, \chi^{j_n}).$$

   Además, si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma \circ \chi$ es otro caracter multiplicativo de $\mathbb{F}_q$ de orden m, por lo tanto existe $0 < c < m$ coprimo con m tal que $\sigma \circ \chi = \chi^c$. Por lo tanto

   $$\sigma(\alpha_i) = (-1)^n \chi^{cj_0}(a_0^{-1}) \dots \chi^{cj_n}(a_n^{-1}) J(\chi^{cj_0}, \dots, \chi^{cj_n})$$

   es otra de las raíces recíprocas de $R(T)$, de donde deducimos que $R(T) \in \mathbb{Z}[T]$.

2. **Hipótesis de Riemann**: Podemos escribir

   $$Z(X,T) = \frac{R(T)^{(-1)^n}}{P_0(T)\cdots P_{2n-2}(T)},$$

   con $P_{2j} = (1 - q^j T)$. Las raíces recíprocas de R verifican por 3.12

   $$|\alpha_i| = q^{\frac{n-1}{2}}.$$

3. **Ecuación funcional**: Dada $\alpha_i = (-1)^n \chi^{j_0}(a_0^{-1}) \dots \chi^{j_n}(a_n^{-1}) J(\chi^{j_0}, \dots, \chi^{j_n})$ raíz recíproca de $R(T)$, la involución $\alpha \mapsto q^{n-1}/\alpha$ nos lleva α_i en

   $$\begin{aligned} q^{n-1}/\alpha_i = \overline{\alpha_i} &= \overline{(-1)^n \chi^{j_0}(a_0^{-1}) \dots \chi^{j_n}(a_n^{-1}) J(\chi^{j_0}, \dots, \chi^{j_n})} \\ &= (-1)^n \overline{\chi^{j_0}}(a_0^{-1}) \dots \overline{\chi^{j_n}}(a_n^{-1}) J(\overline{\chi^{j_0}}, \dots, \overline{\chi^{j_n}}) \\ &= (-1)^n \chi^{m-j_0}(a_0^{-1}) \dots \chi^{m-j_n}(a_n^{-1}) J(\chi^{m-j_0}, \dots, \chi^{m-j_n}), \end{aligned}$$

   que es otra de las raíces recíprocas de R.

4. **Números de Betti**: Supongamos que los coeficientes a_i son obtenidos al reducir otros coefientes A_i en algún cuerpo de números módulo algún ideal primo. Denotemos por X_a al levantamiento de X sobre los números complejos, es decir, $X_a \subset \mathbb{P}^n(\mathbb{C})$ son los puntos donde se anula el polinomio $A_0 x_0^m + \cdots + A_n x_n^m$. Se sigue del Teorema del hiperplano de Lefschetz [Voi03, 1.23] que la inmersión $i : X \to \mathbb{P}^n(\mathbb{C})$ induce un homomorfismo

   $$i^* : H^i(\mathbb{P}^n(\mathbb{C}), \mathbb{Z}) \to H^i(X, \mathbb{Z}),$$

que es un isomorfismo para $i \leq n-2$ y es inyectivo para $i = n-1$. Recordemos que

$$B_i(\mathbb{P}^n(\mathbb{C})) = \begin{cases} 1 & \text{si } 0 \leq i \leq 2n \text{ es par,} \\ 0 & \text{si } 0 \leq i \leq 2n \text{ es impar.} \end{cases}$$

Notemos que X_a tiene dimensión compleja $n-1$ y dimensión real $2n-2$. Por la dualidad de Poincaré sabemos que $B_i(X_a) = B_{2n-2-i}(X_a)$, así que el único número de Betti que nos queda por calcular es $B_{n-1}(X_a)$. Para ello usamos el Ejericio [Dim12, 5.3.7], en el que se da una fórmula para la característica de Euler de X_a:

$$\chi(X) = \sum_{i=0}^{2n} (-1)^i B_i(X_a) = \frac{(1-m)^{n+1}-1}{d} + n + 1.$$

De aquí podemos despejar $B_{n-1}(X_a)$

$$B_{n-1}(X_a) = \begin{cases} -(\chi(X_a) - n) & \text{si } n \text{ es par,} \\ \chi(X_a) - (n-1) & \text{si } n \text{ es impar,} \end{cases} = \begin{cases} \frac{(m-1)^{n+1}+1-m}{m} & \text{si } n \text{ es par,} \\ \frac{(m-1)^{n+1}-1+2m}{m} & \text{si } n \text{ es impar.} \end{cases}$$

Juntando esto con el hecho de que el número de soluciones de la ecuación

$$j_1 + \cdots + j_n \equiv 0 \mod m \qquad 1 \leq j_i < m$$

es exactamente

$$\frac{(m-1)^{n+1} - (-1)^{n+1}(m-1)}{m} = \deg(R(T)),$$

tenemos que

$$B_{n-1}(X_a) = \begin{cases} \deg(R(T)) & \text{si } n \text{ es par,} \\ \deg(R(T)) + 1 & \text{si } n \text{ es impar,} \end{cases} = \deg(P_{n-1}(T)),$$

luego se verifica la cuarta conjetura.

Ejemplo 3.19. Vamos a dar una curva proyectiva singular en la que comprobamos que la hipótesis de Riemann no se satisface. Para ello fijemos un primo p tal que 4 divide a $p-1$ y sea $\mathbb{F}_p$ el cuerpo con p elementos, $\mathbb{F}_{p^s}$ la extensión de grado s y $\mathbb{F}$ su clausura algebraica. Consideremos la curva $X \subset \mathbb{P}^2_{\mathbb{F}_p}$ definida por

$$x_1^2x_0^2 + x_2^2x_0^2 + x_1^2x_2^2 - x_0^4.$$

Denotando los puntos de $\mathbb{P}^2(\mathbb{F})$ con coordenadas homogéneas $[x_0 : x_1 : x_2]$, es fácil comprobar que X tiene dos puntos singulares en la recta del infinito ($x_0 = 0$), a saber, $P_1 = [0:1:0]$ y $P_2 = [0:0:1]$. Para calcular el número de punto de $X(\mathbb{F}_{p^s})$, estableceremos un isomorfismo (de conjuntos algebraicos) entre el abierto afín $X_1 = X \setminus \{P_1, P_2\}$, que identificaremos con la curva afín $x_1^2 + x_2^2 + x_1^2x_2^2 = 1$, y el abierto afín $Y_1 = Y \setminus \{Q_1, Q_2\}$, donde Y es la curva afín dada por $y_1^4 + y_2^2 - 1$ y $Q_1 = (a, 0)$, $Q_2 = (-a, 0)$ son los puntos de intersección de Y con $y_1^2 = -1$, o lo que es lo mismo, a y $-a$ son las raíces de x^2+1 en $\mathbb{F}_{p^s}[x]$ ($a = g^{\frac{p^s-1}{4}}$ con g generador de $\mathbb{F}_{p^s}^\star$). Definamos

$$\begin{array}{rcl} \varphi : X_1 & \to & X_2 \\ (x_1, x_2) & \mapsto & (x_1, (1 + x_1^2)x_2), \end{array}$$

que está bien definida pues para $(x_1, x_2) \in X_1$, tenemos que $x_1^4 + x_2^2(1+x_1^2)^2 = x_1^4 + (1+x_1^2)(1-x_1^2) = x_1^4 + 1 - x_1^4 = 1$ y $x_1^2 \neq 1$, ya que en caso contrario la ecuación que define X_1 implicaría que $2 = 0$, pero estamos asumiendo que 4 divide a $p-1$. Este morfismo tiene una inversa dada por

$$(y_1, y_2) \mapsto \left(y_1, \frac{y_2}{1+y_1^2} \right),$$

por lo tanto tenemos que $\mathcal{N}_s(X) = N_s(Y)$. Para calcular el número de puntos de Y usamos las herramientas ya desarrolladas, a saber, el Corolario 3.18 ($n = 2$, $q = p^s$, $c_1 = 4$, $c_2 = 2$, $a_1 = a_2 = a = 1$):

$$\mathcal{N}_s(X) = p^s - (-J(\rho, \chi))^s - (-J(\rho, \chi^2))^s - (-J(\rho, \chi^3))^s,$$

donde χ y ρ son caracteres multiplicativos de $\mathbb{F}_p$ de orden 4 y 2, respectivamente. Además recordando la ecuación 3.3 tenemos que

$$J(\rho, \chi^2) = J(\rho, \rho) = -\rho(-1) = -1,$$

pues por el Lema 3.2 $\rho(-1) = N(x^2+1) - 1 = 1$. Por otro lado,

$$J(\rho, \chi^3) = J(\rho, \overline{\chi}) = \overline{J(\rho, \chi)},$$

pues ρ toma los valores $1, -1$. Llamando $\pi = -J(\rho, \chi)$, llegamos a

$$\mathcal{N}_s(X) = p^s - \pi^s - \overline{\pi}^s - 1.$$

Por lo tanto la función zeta de X viene dada por

$$Z(X, T) = \frac{(1-\pi T)(1-\overline{\pi} T)(1-T)}{1-pT}.$$

Vemos como el factor $(1-T)$ aparece en el numerador en lugar del denominador, luego no se verifican las conjeturas de Weil.

Este ejemplo tiene la siguiente interpretación geométrica: los puntos singulares de la curva son nodos simples que se pueden resolver explotando la curva y obteniendo un morfismo $Y \to X$, donde Y es otra curva no singular que verifica $Y(\mathbb{F}_{q^s}) = X(\mathbb{F}_{q^s}) + 2$. Dado que la función zeta de la unión disjunta de dos variedades es el producto de las funciones zeta por 2.1, tenemos que

$$Z(Y, T) = Z(X, T) Z(\{\text{pt}\}, T)^2.$$

Por otro lado, la función zeta de un punto es $1/(1-T)$, de modo que la función zeta de Y pasa a ser

$$Z(Y, T) = \frac{(1-\pi T)(1-\overline{\pi} T)}{(1-T)(1-pT)}$$

que sí verifica las conjeturas de Weil.

4 Conjeturas de Weil para curvas

Sea X una **curva** regular sobre un cuerpo k, que para nosotros significa una variedad sobre k no singular y de dimensión 1. A continuación introducimos el concepto de divisor en una curva, que juega un papel fundamental en el estudio de las mismas mediante el teorema de Riemann-Roch y que aquí utilizamos para dar la prueba de las conjeturas de Weil para curvas, aunque para conseguir la hipótesis de Riemann necesitaremos emplear resultados de teoría de intersección de curvas en superficies.

4.1 Divisores

Existen en geometría algebraica dos formas comunes de introducir este concepto, los divisores de Weil y los divisores de Cartier, aunque en nuestro contexto acaban siendo equivalentes. Un **divisor de Weil** es un elemento de grupo abeliano libre generado por los puntos cerrados de X, es decir, una suma finita de puntos cerrados de X con ciertos coefientes enteros. Si todos los coeficientes de D son positivos, decimos que D es un **divisor efectivo**. El grupo abeliano de los divisores de Weil será denotado $\mathrm{Div}(X)$, que además tiene un orden parcial dado por $D_1 \leq D_2$ si y sólo si $D_2 - D_1$ es efectivo. El **grado** de un divisor $D = \sum_{x\in|X|} n_x \cdot x$ se define como

$$\deg(D) = \sum_{x\in|X|} n_x \deg(x),$$

donde $\deg(x) = [\kappa(x) : k]$. Recordemos que el cuerpo de funciones racionales de X se define como $K(X) := \mathscr{O}_{X,\eta}$, donde η es el punto genérico de la curva, y coincide con el cuerpo de fracciones de $\mathscr{O}_{X,x}$ para $x \in |X|$. Además el anillo local $\mathscr{O}_{X,x}$ es regular de dimensión 1, por lo tanto es un dominio de valoración discreta [AM89, 9.2]. Esto nos permite asociar a cada función racional no nula un divisor del siguiente modo. Dada $f \in K(X)^\star$, para cada $x \in |X|$ podemos expresar $f = g/h$, con $g, h \in \mathscr{O}_{X,x}$. Definimos **la valoración de f en x** como $v_x(g) - v_x(h)$ y dado que $v_x(f)$ sólo puede ser distinto de cero en un número finito de puntos [Har77, II.6.1], podemos definir el divisor asociado a f como

$$\mathrm{div}(f) = \sum_{x\in|X|} v_x(f) \cdot x.$$

Además $\mathrm{div} : K(X)^\star \to \mathrm{Div}(X)$ es un homomorfismo de grupos y a los divisores que provienen de funciones racionales se les llama **principales**. Al cociente $\mathrm{Cl}(X) := \mathrm{Div}(X)/\operatorname{Im}(\mathrm{div})$ se le denomina **grupo de clases de divisores**.

Consideremos el conjunto de uplas (U_i, f_i) donde los U_i son un recubrimiento abierto de X y las f_i son funciones racionales de X que verifican la condición[4] $f_i f_j^{-1} \in \Gamma(U_i \cap U_j, \mathscr{O}_X^\star)$ para todo i, j. **Un divisor de Cartier** D es una clase de equivalencia de la relación definida por $D = (U_i, f_i) \sim E = (V_j, g_j)$ si $f_i g_j^{-1} \in \Gamma(U_i \cap V_j, \mathscr{O}_X^\star)$ para todo i, j. Dados dos divisores de Cartier $D = (U_i, f_i)$ y $E = (V_j, g_j)$, podemos definir su suma como $(U_i \cap V_j, f_i g_j)$. Esta operación está bien definida y junto con ella el conjunto de divisores de Cartier es un grupo abeliano que denotaremos $\mathrm{CaDiv}(X)$. Al igual que antes, se define el subgrupo de divisores principales como aquellos del tipo (X, f). Al cociente de $\mathrm{CaDiv}(X)$ por los divisores principales se le denota $\mathrm{CaCl}(X)$. Dado un divisor de Cartier $D = (U_i, f_i)$, podemos asociarle un divisor de Weil como $\sum_{x\in|X|} x \cdot v_x(f_i)$, donde para cada x escogemos

[4] Γ denota el funtor de secciones globales y $\mathscr{O}_X^\star$ el haz de elementos invertibles asociado a $\mathscr{O}_X$.

i tal que $x \in U_i$. Esta aplicación está bien definida y además es un isomorfismo de grupos [GW10, 11.38][5] que induce otro isomorfismo $\mathrm{CaCl}(X) \cong \mathrm{Cl}(X)$.

Por otro lado, el concepto de divisor está íntimamente ligado al de haz invertible. Recordemos que un **haz invertible** en un espacio anillado $(X, \mathscr{O}_X)$ es un haz de $\mathscr{O}_X$-módulos que es localmente isomorfo a $\mathscr{O}_X$. Si $\mathscr{L}$ y $\mathscr{M}$ son dos haces invertibles, entonces $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M}$ y el haz dual $\mathscr{L}^\vee := \mathscr{H}om_{\mathscr{O}_X}(\mathscr{L}, \mathscr{O}_X)$ también. El producto tensorial de $\mathscr{O}_X$-módulos dota al conjunto de clases de isomorfía de haces invertibles de estrucutra de grupo abeliano llamado **grupo de Picard** $\mathrm{Pic}(X)$, cuyo elemento neutro es $\mathscr{O}_X$ y el inverso de $\mathscr{L}$ viene dado por $\mathscr{L}^\vee$. Dado un divisor de Cartier $D = (U_i, f_i)$, podemos asociarle un haz invertible $\mathscr{O}_X(D)$ definido en cada abierto $V \subset X$

$$\mathscr{O}_X(D)(V) = \{f \in K(X) : f_i f \in \Gamma(U_i \cap V, \mathscr{O}_X) \text{ para todo } i\}.$$

Esta aplicación es sobreyectiva y factoriza a través de $\mathrm{CaCl}(X)$, luego establece un isomorfismo $\mathrm{CaCl}(X) \cong \mathrm{Pic}(X)$ [GW10, 11.27]. Componiendo los dos isomorfismos descritos, tenemos una aplicación $\mathrm{Cl}(X) \to \mathrm{Pic}(X)$ que a cada divisor D lo manda al haz invertible definido en cada abierto V por

$$\mathscr{O}_X(D)(V) = \{f \in K(X)^\star : D|_V + \mathrm{div}(f) \geq 0\} \cup \{0\}. \tag{4.1}$$

De hecho existe una correspondencia

$$\{D \in \mathrm{Div}(X) : D \geq 0\} \quad \longleftrightarrow \quad \{(\mathscr{L}, \gamma) : \mathscr{L} \in \mathrm{Pic}(X), 0 \neq \gamma \in \Gamma(X, \mathscr{L})\} / \sim \tag{4.2}$$

donde $\sim$ denota multiplicación por escalar no nulo de la sección global γ. La idea detrás de esta correspondencia es que si $D \geq 0$, entonces existe un morfismo no trivial $\mathscr{O}_X \to \mathscr{O}_X(D)$ y luego usar el isomorfismo canónico $\mathscr{L} \cong \mathscr{H}om_{\mathscr{O}_X}(\mathscr{O}_X, \mathscr{L})$. Si además X es proyectiva, se tiene que para $f \in K(X)^\star$ (cf. [GW10, 15.32])

$$\deg(\mathrm{div}(f)) = 0,$$

por lo tanto el homomorfismo $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ factoriza a través de $\mathrm{Cl}(X)$, luego podemos definir el grado de un haz invertible. Para cada $n \in \mathbb{Z}$, denotaremos $\mathrm{Pic}^n(X)$ aquellos que tienen grado n. En resumen, se tiene el siguiente diagrama

$$\begin{array}{ccccc}
\mathscr{O}_X(D) & \longleftarrow\!\shortmid & D = (U_i, f_i) & \longmapsto & \sum_{x \in |X|} x \cdot v_x(f_i) \\
\cap & & \cap & & \cap \\
\{\text{Haces inveribles}\} & \longleftarrow & \mathrm{CaDiv}(X) & \xrightarrow{\approx} & \mathrm{Div}(X) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Pic}(X) & \xleftarrow{\approx} & \mathrm{CaCl}(X) & \xrightarrow{\approx} & \mathrm{Cl}(X) \xrightarrow[(X \text{ proyectiva})]{\deg} \mathbb{Z}
\end{array}$$

A continuación recordamos el enunciado del Teorema de Riemann-Roch, fundamental a la hora de tratar con haces invertibles sobre una curva. Recordemos que los funtores de cohomología $H^i(X, \cdot)$ se definen como los funtores derivados por la derecha del funtor de sección globales $\Gamma(X, \cdot)$ que parte de la categoría de $\mathscr{O}_X$-módulos a la de grupos abelianos. En nuestro caso $\Gamma(X, \cdot)$ será un k-espacio vectorial, así que los grupos $H^i(X, \cdot)$ también. No será necesario profundizar en temas de cohomología, pues en lo sucesivo trataremos

[5] X cumple la hipótesis de localmente factorial (es decir, todos los anillos locales son factoriales) pues un anillo local y regular es factorial [Mat70, Th. 48].

solamente con los espacios $H^0(X, \cdot)$, que coinciden con $\Gamma(X, \cdot)$ al ser éste un funtor exacto a la izquierda. Dado un haz invertible $\mathscr{L}$, denotaremos $h^0(\mathscr{L}) = \dim H^0(X, \mathscr{L})$.

El último ingrediente que nos falta es el **haz de 1-formas** en X, denotado por Ω^1_X. Recordemos que un haz en un espacio topológico está unívocamente determinado por sus valores en los abiertos de una base de la topología. Definimos Ω^1_X en cada abierto afín $U \subset X$ como el módulo de formas diferenciables de $\mathscr{O}_X(U)$ sobre k, es decir, $\Omega^1_X(U)$ es el $\mathscr{O}_X(U)$-módulo libre generado por los símbolos $\{df : f \in \mathscr{O}_X(U)\}$ cocientado por las relaciones $d(f + f') = d(f) + d(f')$, $d(fg) = f dg + g df$ y $da = 0$ para $a \in k$. En el caso de curvas, Ω^1_X resulta ser un haz invertible que juega un papel fundamental, pues coincide con lo que se denomina el divisor canónico. Definimos **el género** de X como $g = h^0(\Omega^1_X)$.

Teorema 4.1 (Riemann-Roch)**.** *Sea X una curva proyectiva y $\mathscr{L}$ un haz invertible. Entonces*

$$h^0(\mathscr{L}) - h^0(\Omega^1_X \otimes_{\mathscr{O}_X} \mathscr{L}^\vee) = \deg(\mathscr{L}) + 1 - g. \tag{4.3}$$

Demostración. Véase [GW10, 15.36]. □

Sí probaremos el siguiente corolario con el fin de familiarizarnos con los conceptos involucrados en el teorema.

Corolario 4.2. *Sea $\mathscr{L} \in \mathrm{Pic}(X)$.*

1. *Si $\mathscr{L}$ admite secciones globales no nulas, entonces $\deg(D) \geq 0$.*
2. *Se tiene que $\deg(\Omega^1_X) = 2g - 2$.*
3. *Si $\deg(\mathscr{L}) > 2g - 2$, entonces $h^0(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g$.*
4. *Si $k = \mathbb{F}_q$, el homomorfismo $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$ es sobreyectivo.*

Demostración.

1. Sea $D \in \mathrm{Div}(X)$ tal que $\mathscr{O}_X(D) \cong \mathscr{L}$. Si $0 \neq f \in \Gamma(X, \mathscr{L})$, entonces por definición tenemos $\mathrm{div}(f) + D \geq 0$, por lo tanto
$$\deg(D) = \deg(\mathrm{div}(f) + D) \geq 0.$$
2. Basta sustituir en la fórmula de Riemann Roch para $\mathscr{L} = \Omega^1_X$.
3. Se sigue de la fórmula de Riemann-Roch que basta comprobar que $h^0(\Omega^1_X \otimes_{\mathscr{O}_X} \mathscr{L}^\vee) = 0$. Esto se deduce del primer apartado y de que
$$\deg\left(\Omega^1_X \otimes_{\mathscr{O}_X} \mathscr{L}^\vee\right) = \deg\left(\Omega^1_X\right) - \deg\left(\mathscr{L}\right) = 2g - 2 - \deg\left(\mathscr{L}\right) < 0.$$
4. Bastará probar que podemos encontrar un divisor de grado 1. Para ello utilizaremos la desigualdad de Hasse-Weil, que probaremos más adelante de forma independiente a todo lo que se deduzca de este corolario. La desigualdad nos dice que para todo $s \geq 1$, $|\#X(\mathbb{F}_{q^s}) - (q^s + 1)| \leq 2gq^{s/2}$, luego existe un s tal que para todo $r \geq s$ siempre existen puntos $\mathbb{F}_{q^r}$-racionales. En particular podemos encontrar primos $p_1, p_2 \geq s$ y dos puntos $x_1, x_2 \in |X|$ con $\deg(x_1) = p_1$ y $\deg(x_2) = p_2$ gracias a la Proposición 2.8. Tomemos ahora $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha p_1 + \beta p_2 = 1$ y consíderese el divisor $D = \alpha x_1 + \beta x_2$.

□

Corolario 4.3. *Si $k = \mathbb{F}_q$, para cada $n \in \mathbb{Z}$, $\mathrm{Pic}^n(X)$ es finito.*

Demostración. Los subconjuntos $\mathrm{Pic}^n(X)$ son las clases laterales del subgrupo $\mathrm{Pic}^0(X)$, por lo tanto basta probarlo para algún n. Tomemos $n > 2g-2$ y sea D un divisor de grado n. Del tercer apartado del lema anterior sabemos que $h^0(\mathscr{O}_X(D)) > 0$, luego podemos tomar $0 \neq f \in \Gamma(X, \mathscr{O}_X(D))$ de modo que $D + \mathrm{div}(f)$ es efectivo, luego todo divisor en $\mathrm{Pic}^n(X)$ admite como representante un divisor efectivo. Dado que en X hay un número finito de puntos que tienen grado $\leq n$, tenemos el resultado. □

4.2 Racionalidad y ecuación funcional

Ya hemos desarrollado todas las herramientas para dar la prueba de la racionalidad y la ecuación funcional de la función zeta de una curva proyectiva sobre $\mathbb{F}_q$, que como es habitual denotaremos por X.

Teorema 4.4. *La función zeta de X se puede escribir como*

$$Z(X,T) = \frac{P_1(T)}{(1-T)(1-qT)} \tag{4.4}$$

para cierto $P_1(T) \in \mathbb{Z}[T]$ de grado menor o igual que $2g$ y término constante 1.

Demostración. Partimos de la expresión de $Z(X,T)$ como producto sobre los puntos cerrados de X:

$$Z(X,T) = \prod_{x \in |X|} \frac{1}{1 - T^{\deg(x)}} = \prod_{x \in |X|} (1 + T^{\deg(x)} + T^{2\deg(x)} + \dots).$$

Tomemos una enumeración $\{x_i\}_{i \geq 0}$ de los puntos cerrados de X. Desarrollando este producto vemos que en la serie aparacen todos los posibles términos $T^{\sum_i k_i \deg(x_i)}$, donde los k_i son enteros no negativos y las sumas consideredas son finitas. Utilizando divisores, podemos escribir esta suma de forma más conveniente como

$$Z(X,T) = \sum_{D \geq 0} T^{\deg(D)}.$$

El siguiente paso es usar la equivalencia 4.2 entre divisores efectivos y pares de haces invertibles y secciones globales no nulas salvo multiplicación por escalar de modo que podamos agrupar los divisores por clases de equivalencia. En concreto dado $\mathscr{L} \in \mathrm{Pic}(X)$, existen $\#\mathbb{P}^{h^0(\mathscr{L})}(\mathbb{F}_q)$ divisores efectivos D tales que $\mathscr{O}_X(D) \cong \mathscr{L}$. Por lo tanto

$$\begin{aligned} Z(X,T) &= \sum_{\mathscr{L} \in \mathrm{Pic}(X), \mathscr{L} \geq 0} \frac{q^{h^0(\mathscr{L})} - 1}{q-1} T^{\deg(\mathscr{L})} \\ &= \sum_{0 \geq \deg(\mathscr{L}) \geq 2g-2} \frac{q^{h^0(\mathscr{L})} - 1}{q-1} T^{\deg(\mathscr{L})} + \sum_{2g-2 < \deg(\mathscr{L})} \frac{q^{h^0(\mathscr{L})} - 1}{q-1} T^{\deg(\mathscr{L})} \\ &= \sum_{0 \geq \deg(\mathscr{L}) \geq 2g-2} \frac{q^{h^0(\mathscr{L})} - 1}{q-1} T^{\deg(\mathscr{L})} + \sum_{2g-2 < \deg(\mathscr{L})} \frac{q^{\deg(\mathscr{L})+1-g} - 1}{q-1} T^{\deg(\mathscr{L})}, \end{aligned}$$

donde hemos usado el tercer apartado del Corolario 4.2. Dado que $\#\,\mathrm{Pic}^n(X) = \#\,\mathrm{Pic}^0(X)$ es finito vemos que el primer sumando es un polinomio de grado $2g-2$ o nulo en caso de que $g = 0$. En cuanto al segundo sumando, tenemos

$$\sum_{2g-2 < \deg(\mathscr{L})} \frac{q^{\deg(\mathscr{L})+1-g} - 1}{q-1} T^{\deg(\mathscr{L})} = \#\,\mathrm{Pic}^0(X) \sum_{2g-2 < n} \frac{q^{n+1-g}}{q-1} T^n.$$

Podemos sumar esta última serie del siguiente modo

$$\sum_{2g-2<n} \frac{q^{n+1-g}}{q-1} T^n = \frac{T^{2g-1}}{q-1} \sum_{2g-2<n} (q^{n+1-g}) T^{n-2g+1} = \frac{T^{2g-1}}{q-1} \sum_{n\geq 1} (q^{n+g}-1) T^n$$
$$= \frac{T^{2g-1}}{q-1} \left(\frac{q^g}{1-qT} - \frac{1}{1-T} \right) = \frac{h(T)}{(1-T)(1-qT)},$$

donde $h(T)$ es un polinomio de grado $\leq 2g$, de modo que obtenemos el resultado. □

Teorema 4.5. *La función zeta de X satisface la siguiente igualdad en $\mathbb{C}(T)$.*

$$Z\left(X, \frac{1}{qT}\right) = q^{1-g} T^{2-2g} Z(X,T).$$

Demostración. La idea es expresar $Z(X,T)$ como suma de dos términos ambos cumpliendo la ecuación funcional. Primero notemos que

$$\frac{q^{h^0(\mathscr{L})-1}}{q-1} = \frac{q^{h^0(\mathscr{L})} - q^{\deg(\mathscr{L})+1-g}}{q-1} + \frac{q^{\deg(\mathscr{L})+1-g}-1}{q-1}.$$

Por lo tanto,

$$Z(X,T) = \sum_{0\geq \deg(\mathscr{L}) \geq 2g-2} \frac{q^{h^0(\mathscr{L})}-1}{q-1} T^{\deg(\mathscr{L})} + \sum_{2g-2<\deg(\mathscr{L})} \frac{q^{\deg(\mathscr{L})+1-g}-1}{q-1} T^{\deg(\mathscr{L})}$$
$$= \sum_{0\leq \deg(\mathscr{L}) \leq g-1} \frac{q^{h^0(\mathscr{L})}-1}{q-1} T^{\deg(\mathscr{L})} + \sum_{g\leq \deg(\mathscr{L}) \leq 2g-2} \frac{q^{h^0(\mathscr{L})} - q^{\deg(\mathscr{L})+1-g}}{q-1} T^{\deg(\mathscr{L})}$$
$$+ \sum_{\deg(\mathscr{L})\geq g} \frac{q^{\deg(g)}-1}{q-1} T^{\deg(\mathscr{L})} = g_1(T) + g_2(T),$$

donde $g_1(T)$ es la suma de los dos primeros sumandos y $g_2(T)$ el tercero de ellos. Veamos que $g_1(T)$ satisface la ecuación funcional. Necesitaremos usar la simetría en el conjunto de los $\mathscr{L} \in \mathrm{Pic}(X)$ con $0 \leq \deg(\mathscr{L}) \leq 2g-2$ dada por $\mathscr{L} \mapsto \Omega^1_X \otimes \mathscr{L}^\vee$ (recordemos que $\deg(\Omega^1_X) = 2g-2$). Sea $\mathscr{L} \in \mathrm{Pic}(X)$ y llamemos $\mathscr{M} = \Omega^1_X \otimes \mathscr{L}^\vee$. Obervemos que

$$\frac{q^{h^0(\mathscr{L})}-1}{q-1} \left(\frac{1}{qT}\right)^{\deg(\mathscr{L})} = \frac{q^{h^0(\mathscr{M})-\deg(\mathscr{M})+g-1}-1}{q-1} \left(\frac{1}{qT}\right)^{-\deg(\mathscr{M})+2g-2}$$
$$= \frac{q^{h^0(\mathscr{M})} - q^{\deg(\mathscr{M})+1-g}}{q-1} T^{\deg(\mathscr{M})} q^{1-g} T^{2-2g}.$$

y análogamente

$$\frac{q^{h^0(\mathscr{M})} - q^{\deg(\mathscr{M})+1-g}}{q-1} \left(\frac{1}{qT}\right)^{\deg(\mathscr{M})} = \frac{q^{h^0(\mathscr{L})}-1}{q-1} T^{\deg(\mathscr{L})} q^{1-g} T^{2-2g}.$$

Por lo tanto $g_1(T)$ satisface la ecuación funcional. Finalmente,

$$g_2(T) = \sum_{\deg(\mathscr{L})\geq g} \frac{q^{\deg(\mathscr{L})+1-g}-1}{q-1} T^{\deg(\mathscr{L})}$$
$$= \#\,\mathrm{Pic}^0(X) \sum_{n\geq g} \frac{q^{n+1-g}-1}{q-1} T^n = \#\,\mathrm{Pic}^0(X) \frac{T^g}{(1-T)(1-qT)},$$

que verifica

$$g_2\left(\frac{1}{qT}\right) = \#\operatorname{Pic}^0(X)\left(\frac{1}{qT}\right)^g \frac{qT^2}{(qT-1)(T-q)} = g_2(T)q^{1-g}T^{2-2g}.$$

□

Corolario 4.6. *Se tiene que $P_1(T)$ tiene grado $2g$. Se sigue que*

$$E = \deg P_0 - \deg P_1(T) + \deg P_2(T) = 2g-2,$$

y por lo tanto se verifican las conjeturas 1 y 3 en 2.11.

Demostración. Aplicando la ecuación funcional a la expresión obtenida en el Teorema 4.5 tenemos que

$$\frac{P_1\left(q^{-1}T^{-1}\right)qT^2}{(1-qT)(1-T)} = \frac{T^{2-2g}q^{1-g}P_1(T)}{(1-T)(1-qT)},$$

y por lo tanto

$$T^{2g}q^gP_1(q^{-1}T^{-1}) = P_1(T). \tag{4.5}$$

Sabemos que $Z(X,T)$ tiene término independiente 1, luego $P_1(T)$ también. Se sigue que el grado es $2g$. □

De hecho podemos sacar todavía más información de la ecuación 4.5. Dado que sabemos que el término independiente de $P_1(T)$ es 1, podemos facotizarlo en $\mathbb{C}$ y escribir

$$P_1(T) = \prod_{i=1}^{2g}(1-\alpha_iT),$$

y por lo tanto

$$\begin{aligned} P_1(T) = \prod_{i=1}^{2g}(1-\alpha_iT) &= T^{2g}q^g\prod_{i=1}^{2g}\left(1-\alpha_i\frac{1}{qT}\right) = q^g\prod_{i=1}^{2g}\left(T-\frac{\alpha_i}{q}\right) \\ &= q^g\prod_{i=1}^{2g}\left(1-\frac{q}{\alpha_i}T\right)\frac{\alpha_i}{q} = \left[\prod_{i=1}^{2g}\left(1-\frac{q}{\alpha_i}T\right)\right]\left[\prod_{i=1}^{2g}\alpha_i\right]q^{-g}, \end{aligned}$$

lo cual nos indica que existe una permutación $\sigma \in S_{2g}$ tal que $\alpha_i\alpha_{\sigma(i)} = q$.

El objetivo de la siguiente sección es comprobar que en realidad $\alpha_{\sigma(i)} = \overline{\alpha_i}$, es decir, se verifica la hipótesis de Riemann. Para ello, gracia a la simetría de las raíces recíprocas de $P_1(T)$, bastará probar que cada α_i verifica $|\alpha_i| \leq q^{1/2}$. El siguiente lema nos asegura que dicha condición es equivalente a la Desigualdad de Hasse-Weil:

Lema 4.7. *Se tiene que $|\alpha_i| \leq q^{1/2}$ si y sólo si $|\mathcal{N}_s - (q^s+1)| \leq 2gq^{s/2}$.*

Demostración. Empecemos notando que si tomamos derivada del logaritmo en la función zeta de X obtenemos

$$\sum_{s=1}^{\infty}\frac{\mathcal{N}_s}{s}T^s = \sum_{i=1}^{2g}\operatorname{Log}(1-\alpha_i) - \operatorname{Log}(1-T) - \operatorname{Log}(1-qT) = \sum_{s=1}^{\infty}\left(1+q^s-\sum_{i=1}^{2g}\alpha_i^s\right)\frac{T^s}{s},$$

de donde deducimos que

$$\varepsilon_s := |\mathcal{N}_s - (q^s+1)| = \sum_{i=1}^{2g}\alpha_i^s.$$

Por lo tanto si cada α_i verifica $|\alpha_i| \leq q^{1/2}$, claramente obtenemos que $\varepsilon_s \leq 2gq^{s/2}$. Recíprocamente, notemos que

$$\sum_{s=1}^{\infty} \varepsilon_s T^s = \sum_{i=1}^{2g} \sum_{s=1}^{\infty} \alpha_i^s T^s = \sum_{i=1}^{2g} \frac{\alpha_i T}{1 - \alpha_i T}.$$

Veamos esta expresión como una función de variable compleja $T \in \mathbb{C}$. Dado que $|\varepsilon_s| \leq 2gq^{s/2}$ para todo s, obtenemos la siguiente cota para $|T| \leq q^{-1/2}$:

$$\left| \sum_{s=1}^{\infty} \varepsilon_s T^s \right| \leq 2g \sum_{s=1}^{\infty} (q^{1/2} |T|)^s = \frac{2gq^{1/2} |T|}{1 - q^{1/2} |T|},$$

por lo tanto los polos de $\sum_{s=1}^{\infty} \varepsilon_s T^s$ tienen módulo mayor o igual que $q^{-1/2}$, es decir, $|\alpha_i| \geq q^{1/2}$. □

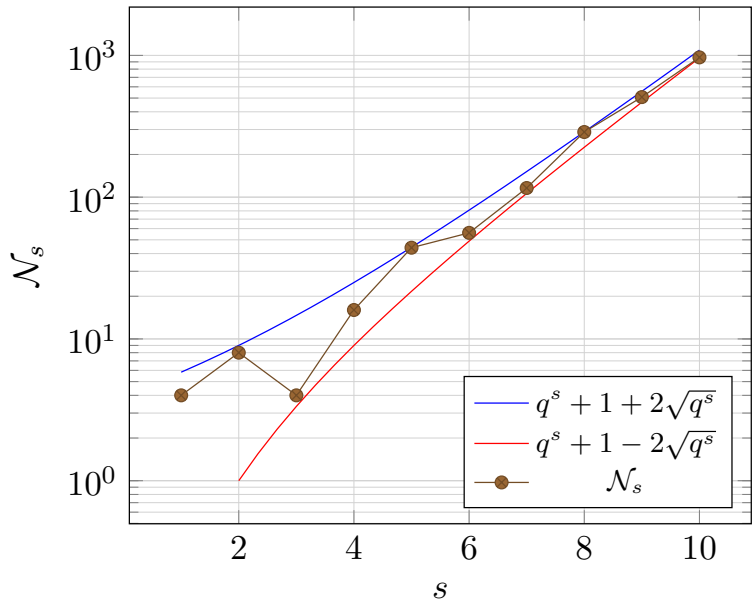


Figura 3: La Desigualdad de Hasse-Weil (para la curva elíptica $x_0x_2^2 + x_0x_1x_2 + x_0^2x_2 = x_1^3 + x_0x_1^2 + x_0x_1^2$ y $q = 2$) implica que $\mathcal{N}_s$ siempre se encuentra entre las curvas $q^s + 1 + 2\sqrt{q^s}$ y $q^s + 1 - 2\sqrt{q^s}$.

4.3 Intersecciones en superficies

Con el fin de desarrollar las técnicas que usaremos en la prueba de la desigualda de Hasse Weil, es necesario tratar algunos fundamentos de la teoría de intersección de superficies. El primer paso es el de generalizar la noción de divisor que hemos introducido en el caso de curvas y definir algunas operaciones entre ellos, para así aplicarlos a la superficie $\overline{X} \times_{\mathbb{F}} \overline{X}$, donde recordemos que en la notación que estamos siguiendo, $\mathbb{F}$ es una clausura algebraica de $\mathbb{F}_q$ y $\overline{X} = X \times_{\mathbb{F}_q} \mathbb{F}$.

Supongamos que X es una **superficie** proyectiva sobre un cuerpo k algebraicamente cerrado, es decir una variedad proyectiva sobre k de dimensión 2. Supondremos que X es **regular en codimensión 1**, es decir, que todo anillo local de dimensión 1 es regular o, equivalentemente, los puntos singulares son aislados. Un divisor primo en X es un

subesquema cerrado de dimensión 1, es decir, una curva, y se define el grupo de divisores (de Weil) $\mathrm{Div}(X)$ como el grupo abeliano libre generado por los divisores primos de X. Un elemento típico de $\mathrm{Div}(X)$ se escribe como una suma finita $D = \sum_i n_i C_i$.

Al igual que en el caso de curvas (los divisores primos eran los puntos cerrados), cada divisor primo tiene asociado un punto genérico η tal que $\mathscr{O}_{X,\eta}$ es un anillo de valoración discreta cuyo cuerpo de fracciones es $K(X)$ y así dada $f \in K(X)^\star$ podemos definir la valoración de f en Y, $v_Y(f)$. De nuevo $v_Y(f) \neq 0$ es un número finito de divisores primos de X de modo que podemos asociar un divisor a una función racional:

$$\mathrm{div}(f) = \sum_{Y \subset X} v_Y(f).$$

Definimos así una relación de dependencia lineal ($D_1 \sim D_2$ si y sólo si $D_1 - D_2 = \mathrm{div}(f)$ para alguna $f \in K(X)^\star$) y el correspondiente cociente $\mathrm{Cl}(X)$. Definimos el grupo de Picard de X exactamente de manera análoga a como lo hicimos para curvas. En el caso de que X sea localmente factorial (en particular si X es regular) tenemos un isomorfismo de grupos $\mathrm{Cl}(X) \to \mathrm{Pic}(X)$ como el descrito en 4.1.

Si C y D son dos curvas sobre X y $x \in C \cap D$ es un punto de intersección de C y D, decimos que C y D **intersectan transversalmente** en x si las ecuaciones locales f, g de C, D en x generan el ideal maximal $\mathfrak{m}_x$ de $\mathscr{O}_{X,x}$. A continuación introducimos un pairing en el grupo de divisores de X, denominado **número de intersección**. No nos preocuparemos de su definición, sólo utilizaremos que existe y alguna de sus propiedades:

Teorema 4.8. *Existe un único pairing* $\mathrm{Div}(X) \times \mathrm{Div}(X) \to \mathbb{Z}$*, denotado* $D.C$ *para cada par de divisores, tal que*

1. *Si* C *y* D *son dos curvas no singulares que se intersecan transversalmente, entonces*

$$C.D = \#(C \cap D).$$

2. *Es simétrico:* $C.D = D.C$.

3. *Es aditivo:* $(C_1 + C_2).D = C_1.D + C_2.D$.

4. *Sólo depende de la clase de equivalencia lineal: si* $C_1 \sim C_2$*, entonces* $C_1.D = C_2.D$.

Demostración. Véase [Har77, V.1.1]. □

También enunciamos dos resultados que utilizamos en la prueba de la desigualdad de Hasse-Weil cuya demostración también puede encontrarse en [Har77, V.1]. Definimos el **divisor canónico** K de X como el haz asociado a $\omega_X = \bigwedge^2 \Omega_{X/k}$ (cf. [Har77, II.8]).

Proposición 4.9 (Fórmula del adjunto)**.** *Sea* C *una curva no singular de género* g *sobre la superficie* X*, y sea* K *al divisor canónico en* X*. Entonces*

$$2g - 2 = C.(C + K).$$

Decimos que un $D \in \mathrm{Cl}(X)$ es **amplio** si $D^2 := D.D > 0$ y $D.C > 0$ para toda curva irreducible C en X. También diremos que D es **numéricamente equivalente a cero**, y se denotará $D \equiv 0$, si $D.E = 0$ para todo divisor E. Decimos que D y E son numéricamente equivalentes si $D - E$ es numéricamente equivalente a cero.

Teorema 4.10 (Teorema del índice de Hodge)**.** *Sea* H *un divisor amplio en* X *y sea* D *un divisor no numéricamente equivalente a cero tal que* $D.H = 0$ *. Entonces*

$$D^2 < 0.$$

Volviendo al caso que nos concierne, consideremos una curva X proyectiva y regular sobre $\mathbb{F}_q$ y definamos $S = \overline{X} \times_{\mathbb{F}} \overline{X}$, que resulta ser una superficie regular y proyectiva. Entran ahora en juego dos importantes morfismos, por un lado **la diagonal**

$$\Delta = \mathrm{id}_{\overline{X}} \times \mathrm{id}_{\overline{X}} : \overline{X} \to S, \tag{4.6}$$

y **el grafo** de $F^s_{\overline{X}}$

$$\Gamma^s_F = \mathrm{id}_{\overline{X}} \times F^s_{\overline{X}} : \overline{X} \to S, \tag{4.7}$$

donde recordemos $F_{\overline{X}} = \mathrm{id}_{\overline{X}} \times F$ es el automorfismo de Frobenius de $\overline{X}$ introducido en 2.5. Ambos morfismos son inmersiones cerradas, de modo que identificaremos las imágenes con divisores primos de S que por abuso de notación denominaremos Γ^s_F y Δ. Recordemos que los puntos $\mathbb{F}_{q^s}$-racionales, $X(\mathbb{F}_{q^s})$, se corresponden con los puntos cerrados de $\overline{X}$ que quedan fijos por $F^s_{\overline{X}}$, o dicho de otro modo aquellos que están en $\Gamma^s_F \cap \Delta$. En particular se sigue que $\Gamma^s_F \cap \Delta$ es finito. La siguiente proposición nos asegura que dicho número puede calcularse como $\Gamma^s_F.\Delta$.

Proposición 4.11. *Γ^s_F y Δ intersecan transversalmente.*

Demostración. Véase [Mus11, 2.4]. □

4.4 La desigualdad de Hasse-Weil

Ya estamos en disposición de probar la desigualdad de Hasse-Weil y por lo tanto la hipótesis de Riemann para curvas. Empecemos con una proposición preparatoria.

Proposición 4.12. *Sean C y C' dos curvas regulares y proyectivas sobre un cuerpo algebraicamente cerrado, y consideremos $X = C_1 \times C_2$. Sean $l = C_1 \times \{\mathrm{pt}\}$ y $m = \{\mathrm{pt}\} \times C_2$. Sea D un divisor de X y sean $a = D.l$ y $b = D.m$. Entonces se tiene que*

$$D^2 \leq 2ab.$$

Demostración. Definamos $H = l + m$ y $E = l - m$. Dado que $l^2 = m^2 = 0$ y $l.m = 1$, tenemos que $D.H = a + b$, $D.E = a - b$, $H^2 = 2$, $E^2 = -2$ y $H.E = 0$. Para toda curva $C'' \subset X$, si C'' no intersecta a ninguna curva $C \times \{\mathrm{pt}\}$ para ningún $\mathrm{pt} \in C'$, entonces claramente $C'' \subset C \times \{\mathrm{pt}\}$ para algún $\mathrm{pt} \in C'$. Entonces C'' debe intersecar a $\{\mathrm{pt}\} \times C'$ para algún $\mathrm{pt} \in C$. Dado que $H^2 = 2$, tenemos que H es amplio. Así que definimos

$$D' = (H^2)(E^2)D - (E^2)(D.H)H - (H^2)(D.E)E = -4D + 2(a+b)H - 2(a-b)E,$$

que verifica

$$D'.H = -4(a+b) + 4(a+b) = 0,$$

Se sigue del Teorema del índice de Hodge 4.10 que $D'^2 \leq 0$, es decir,

$$\begin{aligned} 0 &\geq (-4D + 2(a+b)H - 2(a-b)E)(-4D + 2(a+b)H - 2(a-b)E) \\ &= 16D^2 - 8(a+b)H.D + 8(a-b)E.D \\ &- 8(a+b)H.D + 4(a-b)^2H^2 + 8(a-b)E.D + 4(a-b)E^2 \\ &= 16D^2 - 8(a+b)^2 + 8(a-b)^2 = 16D^2 - 32ab, \end{aligned}$$

de donde obtenemos el resultado. □

Teorema 4.13 (Desigualdad de Hasse-Weil)**.** *Sea X una curva proyectiva y regular. Entonces para todo $s \geq 1$ se verifica*

$$|\mathcal{N}_s - (q^s + 1)| \leq 2gq^{s/2}$$

Demostración. Vamos a probar el resultado para $s = 1$, pues una vez probado podemos aplicarlo a la curva $X \times_{\mathbb{F}_q} \mathbb{F}_{q^s}$. Como viene siendo habitual consideramos la superficie $S = \overline{X} \times_{\mathbb{F}} \overline{X}$ y los divisores Γ_F y Δ introducidos en 4.6 y 4.7, que gracias a 4.9 verifican $\mathcal{N}_1 = \Gamma_F.\Delta$.

Aplicamos ahora la Proposición 4.12 a las curvas $C = C' = \overline{X}$, el divisor $D = c\Delta + d\Gamma_F$, con $c, d \in \mathbb{Z}$. Notemos que $\Delta.l = \Delta.m = 1$, mientras que $\Gamma_F.l = q$ y $\Gamma_F.m = 1$. Ahora calculamos Γ_F^2 y Δ^2 usando la fórmula del adjunto 4.9. Para ello notemos que el divisor canónico de S, K, es numéricamente equivalente a $(2g-2)(l+m)$. Dado que Δ y Γ_F son curvas de género g, tenemos que

$$\begin{aligned} 2g - 2 &= \Delta.(\Delta + K) = \Delta^2 + 2(2g-2), \\ 2g - 2 &= \Gamma_F.(\Gamma_F + K) = \Gamma_F^2 + (q+1)(2g-2). \end{aligned}$$

Por lo tanto $\Delta^2 = -(2g-2)$ y $\Gamma_F^2 = -q(2g-2)$. Se sigue que

$$-c^2(2g-2) - qd^2(2g-2) + 2cd\mathcal{N}_1 \leq 2(c+bd)(c+d),$$

simplificando llegamos a

$$|\mathcal{N}_1 - (q+1)| \leq \frac{c}{d}gq + \frac{d}{c}g \leq 2\sqrt{\frac{c}{d}gq \cdot \frac{d}{c}g} = 2gq^{1/2}.$$

□

Como consecuencia del Lema 4.7, obtenemos que X verifica las tres primeras conjeturas de Weil. Finalmente, en el caso de que X haya sido obtenida reduciendo módulo $\mathbb{F}_q$ alguna curva Y definida sobre un cuerpo de números K, es bien conocido que los número de Betti de $Y_a = Y \times_K \mathbb{C}$ que, topológicamente, es una superficie de Riemann compacta de género g, son (cf. [Mir95, pág. 191])

$$B_i(Y_a) = \begin{cases} 1 & \text{si } i = 0, \\ 2g & \text{si } i = 1, \\ 1 & \text{si } i = 2, \\ 0 & \text{si } i > 2. \end{cases}$$

luego también se verifica la última de las conjeturas.

5 Conclusiones

Una de las principales conclusiones que podemos sacar de este trabajo es la importancia que tiene la función zeta de una variedad sobre un cuerpo finito como objeto que codifica las propiedades ariméticas de la misma y la relevancia de las conjeturas de Weil a la hora de establecer un puente entre el enfoque que diferentes disciplinas matemáticas como la Geometría Algebraica o la Topología Algebraica pueden tomar del mismo objeto. A parte de su importancia matemática, que no es poca, el estudio de estas conjeturas son un buen punto de partida para comenzar estudios más avanzados en Geometría Algebraica, ya que los desarrollos realizados para alcanzar la demostración de las mismas implicó la aparición de técnicas cohomológicas que son la base de diferentes líneas de investigación actuales dentro de este campo.

De hecho, asumiendo la existencia de una teoría de cohomología adecuada, es decir, una en la que para una variedad proyectiva sobre $\mathbb{F}_q$ de dimensión n existen espacios vectoriales $H^0(X), \dots, H^{2n}(X)$ sobre un cuerpo K de característica cero en los que actúa $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$, podemos esbozar cómo generalizar las conjeturas a dimensiones mayor. Supogamos también que la diagonal y el grafo de automorfismo de Frobenius F intersecan transversalmente en $\overline{X} \times_{\mathbb{F}} \overline{X}$ (generalizando la Proposición 4.11). Los puntos de intersección son exactamente $\mathcal{N}_1 = X(\mathbb{F}_q)$ y, como la intersección es transversal, se sigue del Teorema del punto fijo de Lefschetz que dicho número se calcula como $\mathcal{N}_1 = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}(F^*; H^i(X))$. Cambiando ahora F por F^s, tendríamos

$$\mathcal{N}_s = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}(F^{s*}; H^i(X)),$$

y sustituyendo en la función zeta de X

$$Z(X,T) = \prod_{i=0}^{2n} \left(\operatorname{Exp}\left(\sum_{s=1}^{\infty} \operatorname{Tr}(F^{s*}; H^i(X)) \frac{T^s}{s} \right) \right)^{(-1)^i}.$$

Es un ejercicio sencillo comprobar que en $K[\![T]\!]$ se tiene la igualdad

$$\operatorname{Exp}\left(\sum_{s=1}^{\infty} \operatorname{Tr}(F^{s*}; H^i(X)) \frac{T^s}{s} \right) = \det(1 - FT; H^i(X))^{-1},$$

de donde deducimos directamente la racionalidad de $Z(X,T)$. De igual modo la ecuación funcional se deduce de la dualidad de Poincaré en esta teoría cohomológica. Para más detalles véase [Har77, Ap. C].

Por ello, una posible continuación de estudios pasaría por profundizar en temas de teoría de haces y esquemas, que aquí sólo hemos tratado tangencialmente, para después saltar al estudio de la cohomología étale y así aprender las técnicas involucradas en la prueba general de las conjeturas de Weil. A partir de ahí, se podrían abordar alguna de las aplicaciones que todas estas teorías fructíferas han propiciado, como por ejemplo el estudio de problemas de acotación y distribución de sumas exponenciales, a los que el director de este proyecto ha dedicado parte de su investigación matemática.

El contenido aquí expuesto es el resultado del trabajo realizado a lo largo del curso de máster. En una primera etapa del proyecto se adquirieron una serie de conocimientos teóricos que ampliaron el contenido de algunas asignaturas del grado y máster mediante el uso de bibliografía. En concreto, en una primera aproximación, ciertos capítulos del libro [Lor96] han sido de gran ayuda a la hora de familiarizarse con variedades definidas sobre

cuerpos finitos, ya que en la asignatura «Álgebra Conmutativa y Geometría Algebraica» del Grado en Matemáticas se tratan variedades definidas casi siempre sobre los números complejos. En este mismo periodo, los primeros capítulos de [IR90] han sido útiles para introducirse en Teoría de Números, principalmente con el objetivo de desarrollar la teoría de sumas de Gauss y Jacobi que posteriormente se usaría para la demostración de las conjeturas de Weil en el caso de hipersuperficies diagonales. Es importante mencionar aquí que los conocimientos adquiridos en esta referencia fueron de gran beneficio para el estudio de la asignatura «Criptografía», que se cursó en el segundo cuatrimestre del curso de máster.

En una segunda etapa, la idea principal era desarrollar la prueba de las conjeturas para curvas siguiendo las notas [ET11], donde se abordan mediante el lenguaje de las variedades algebraicas clásicas que se estudió en la asignatura del grado. A pesar de que el lenguaje de los esquemas no juega un papel fundamental en la prueba de las conjeturas que aquí presentamos, decidimos adoptar este estilo principalmente por dos motivos: en primer lugar, la perspectiva de los esquemas nos permite establecer la conexión entre las funciones zeta de variedades sobre cuerpos finitos y la función zeta de Riemann clásica u otras funciones zeta típicas de Teoría de Números; y en segundo lugar, porque el contenido de la asignatura del máster «Geometría Algebraica» se centró principalmente en el estudio de las superficies de Riemann que, aunque resultó altamente beneficioso para familiarizarse con conceptos de teoría de haces y cohomología, no incluyó teoría de esquemas, requisito indispensable para continuar con estudios más avanzados en Geometría Algebraica. En este sentido las referencias [Ras07] y [Mus11] han sido de gran importancia.

Este trabajo me ha dado la oportunidad de extender mis conocimientos y tener una visión más global de lo aprendido estos años. En particular, me gustaría remarcar la constante sensación de que la gran mayoría de dificultades que me he encontrado en la realización de este trabajo y a lo largo de mi formación han acabado reduciéndose a una cuestión referente al Álgebra Conmutativa, por ello desde mi humilde opinión creo que sería una buena idea reforzar los contenidos que se imparten en esta materia a lo largo del grado y el máster. Finalmente, es importante mencionar que durante el desarrollo de este proyecto, el autor fue beneficiario de una beca concedida por el Instituto de Matemáticas de la Universidad de Sevilla (IMUS) sin la cual el desempeño y el número de horas dedicadas al mismo hubiese sido menor.

Referencias

[AGV73] Michael Artin, Alexandre Grothendieck, and Jean Louis Verdier. *Théorie des topos et cohomologie etale des schémas: tome 3*. Springer-Verlag, 1973. 3

[AM89] Michael Francis Atiyah and Ian Grant Macdonald. *Introducción al álgebra conmutativa*. Reverté, 1989. 6, 32

[Art24] Emil Artin. Quadratische körper im gebiete der höheren kongruenzen. i. *Mathematische Zeitschrift*, 19(1):153–206, 1924. 2

[BEW98] Bruce C Berndt, Ronald J Evans, and Kenneth S Williams. *Gauss and Jacobi sums*. Wiley New York, 1998. 16

[BF14] Gerald Berman and Kenneth D Fryer. *Introduction to combinatorics*. Elsevier, 2014. 14

[Con10] Keith Conrad. Characters of finite abelian groups. *Lecture Notes*, 2010. 17

[Del74] Pierre Deligne. La conjecture de weil. i. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 43(1):273–307, 1974. 3

[Dim12] Alexandru Dimca. *Singularities and topology of hypersurfaces*. Springer Science & Business Media, 2012. 30

[Dwo60] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82(3):631–648, 1960. 3

[EH06] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197. Springer Science & Business Media, 2006. 14

[ET11] Bas Edixhoven and Lenny Taelman. Algebraic geometry. *Leiden University, The Netherlands, Version*, 2011. 43

[GW10] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry*. Springer, 2010. 3, 7, 28, 33, 34

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 1977. 3, 7, 32, 39, 42

[IR90] Kenneth Ireland and Michael Rosen. A classical introduction to modern number theory. 1990. *Grad. Texts in Math*, 1990. 16, 18, 43

[Isa94] I Martin Isaacs. *Character theory of finite groups*, volume 69. Courier Corporation, 1994. 17

[Kow18] E Kowalski. Exponential sums over finite fields, i: elementary methods. *preparation; available at www. math. ethz. ch/~ kowalski/exp-sums. pdf*, 2018. 16, 18, 19

[Lor96] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9. American Mathematical Soc., 1996. 5, 42

[Mat70] Hideyuki Matsumura. *Commutative algebra*, volume 56. Addison Wesley Longman, 1970. 33

[Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5. American Mathematical Soc., 1995. 41

[Mus11] Mircea Mustata. Zeta functions in algebraic geometry. *Lecture notes, University of Michigan*, 2011. 6, 40, 43

[Neu99] Jürgen Neukirch. Algebraic number theory. *Grundlehren der mathematischen Wissenschaften*, 322, 1999. 18

[Niv69] Ivan Nivel. Formal power series. *Am. Monthly*, 76, 1969. 4, 5

[Ras07] Sam Raskin. The weil conjectures for curves. *Lecture notes, University of Chicago*, 2007. 43

[Rie59] Bernhard Riemann. Ueber die anzahl der primzahlen unter einer gegebenen grosse. *Ges. Math. Werke und Wissenschaftlicher Nachlaß*, 2:145–155, 1859. 2

[Roj09] Antonio Rojas. Sumas exponenciales: otra forma de contar. *Memorias de la Real Academia Sevillana de Ciencias*, 2009. 20

[Voi03] Claire Voisin. *Hodge theory and complex algebraic geometry II*, volume 2. Cambridge University Press, 2003. 29

[Wei45] André Weil. *Sur les courbes algébriques et les variétés qui s' en déduisent*, volume 7. Pulc. Inst. Math. Univ. Strasbourg, 1945. 2

[Wei46] André Weil. *Variétés abéliennes et courbes algébriques*, volume 8. Pulc. Inst. Math. Univ. Strasbourg, 1946. 2

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc*, 55(5):497–508, 1949. 3, 16