Sumas de Gauss y funciones zeta de hipersuperficies diagonales

Olmo Chiara Llanos

Sumas de Gauss y funciones zeta de hipersuperficies diagonales

Olmo Chiara Llanos

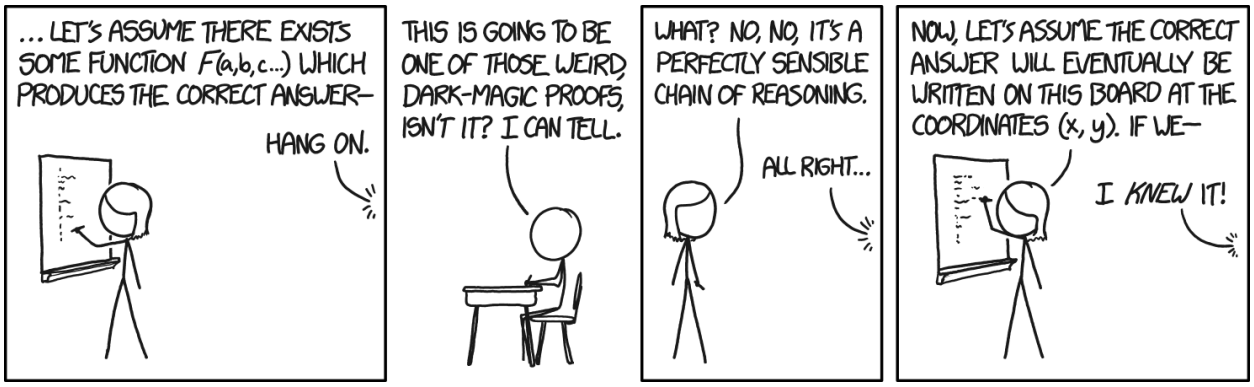
Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por Antonio Rojas León

Presentada el 21 de junio de 2017

Il faut bien que je supporte deux ou trois chenilles
si je veux connaître les papillons.

— *Le Petit Prince,* Antoine de Saint–Exupéry



xkcd 1724: Proofs
Randall Munroe

Índice

Resumen

A LO LARGO DE este trabajo abordaremos algunos casos particulares de las conjeturas de Weil. En primer lugar estudiaremos la definición de función zeta de una variedad y la formulación de las conjeturas de Weil, con su respectiva motivación.

Seguidamente, introduciremos toda la teoría de sumas de Gauss y de Jacobi, partiendo de la base de la teoría de caracteres de un grupo abeliano, para obtener resultados sobre el cálculo del número de puntos de ciertas variedades sobre cuerpos de característica positiva (y veremos por el camino otra aplicación de las sumas de Gauss: la demostración de la ley de reciprocidad cuadrática). Finalmente probaremos la relación de Hasse–Davenport, que nos permite *elevar* sumas de un cuerpo base a sus extensiones.

En el tercer capítulo, siguiendo la línea de Weil, utilizaremos sumas exponenciales para hallar el número de puntos de una hipersuperficie diagonal afín, es decir, dada por la ecuación

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} + \cdots + a_n x_n^{k_n} = a.$$

A partir de este resultado, mediante ciertas consideraciones sobre los exponentes, estaremos en condiciones de escribir de manera explícita el número de puntos de una hipersuperficie diagonal proyectiva, y comprobar que en efecto se cumplen las conjeturas de Weil.

Finalmente, utilizaremos herramientas más avanzadas de geometría algebraica para esbozar la prueba de las conjeturas de Weil para curvas proyectivas, dando por conocidos algunos resultados de mayor profundidad como el teorema de Riemann–Roch o la dualidad de Serre.

English Abstract

THROUGHOUT THIS DISSERTATION we will be addressing several particular instances of the Weil conjectures. First we will study the definition of the zeta function of a variety and the formulation (and the motivation) of the Weil conjectures.

Afterwards, we introduce the theory Gauss and Jacobi sums, starting from the theory of characters of an abelian group, to get results on the number of points of certain varieties over fields of positive characteristic (developping on the way another application of Gauss sums: the law of quadratic reciprocity). We also prove the celebrated Hasse–Davenport relation, that allows us to lift sums from a base field to its extensions.

In the third chapter, following Weil's path, we use exponential sums to find the number of affine points in a diagonal hypersurface defined by

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} + \cdots + a_n x_n^{k_n} = a.$$

From this result, by studying the behavior with respect to the exponents, we can describe the number of projective points of the homogeneization of the variety, which allows us to find the zeta function and check that the four conjectures by Weil are indeed true.

Finally, we use some more advanced tools from algebraic geometry to sketch the proof of the Weil conjectures for curves, without proving some results like the Riemann–Roch theorem or Serre duality.

Reseña histórica

VEAMOS, EN PRIMER lugar, una pequeña introducción histórica del trabajo. La base fundamental son las *funciones zeta*, en sus diferentes interpretaciones en ramas del álgebra o el análisis. La historia de las funciones zeta podría remontarse al estudio de la *función zeta de Riemann*, dada por

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

iniciado por Euler para el caso de s real e impulsado con el estudio de Riemann de la relación de $\zeta(s)$ con $\pi(x)$, que tiene como implicación final una relación entre los ceros de ζ y la distribución de los números primos. La existencia de una *factorización* de la función ζ en función de los números primos, dada por

$$\zeta(s) = \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}},$$

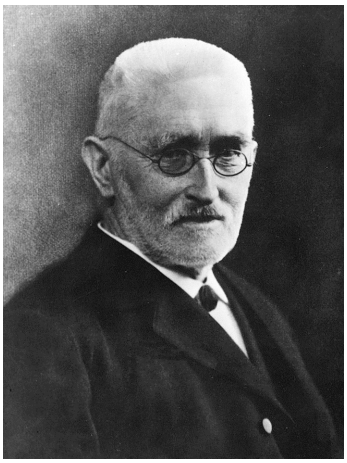
lleva a Richard Dedekind a generalizar la definición de función zeta (cf. [Dir99; Neu99]): partiendo de un cuerpo de números K con anillo de enteros $\mathcal{O}_K$, podemos tomar como *primos de K* los ideales primos $\mathfrak{p}$ de $\mathcal{O}_K$, y asociarles una noción de tamaño (la norma) dada por la dimensión del cociente

$$\mathrm{N}(\mathfrak{p}) = \left|\mathcal{O}_K/\mathfrak{p}\right| = p^r, \quad p \text{ primo}, r \in \mathbb{Z}.$$

Dedekind define entonces la función zeta asociada a K como

$$\zeta_X(s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}}.$$

Es evidente que se trata de una *extensión* de la función zeta tradicional, que se obtendría tomando $K = \mathbb{Q}$ y $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Partiendo de esta generalización aparece la teoría de funciones zeta que estudiaremos en este trabajo, debida a Emil Artin.



Richard Dedekind

La tesis doctoral de Artin se compone de dos partes que desarrollan una idea común: la extensión de la teoría de números desarrollada sobre cuerpos de números a extensiones de cuerpos de funciones (i.e. $K = \mathbb{F}_p(x, \sqrt{D})$, con $\mathbb{F}_p$ un cuerpo finito). Considerando la clausura integral R de $\mathbb{F}_p[x]$ en K obtiene, en la primera parte de su tesis, resultados sobre descomposición y ramificación de ideales primos, número de clase o reciprocidad.

La segunda parte de su tesis (cf. [Art24]) comienza con la introducción de la *función zeta de Artin* como

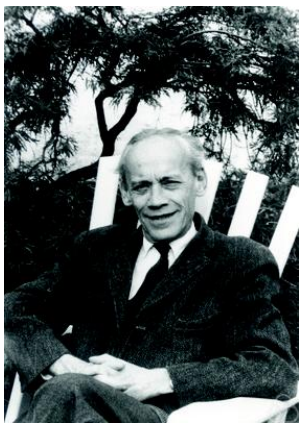
$$\zeta(s) = \prod_{\mathfrak{p} \subset R} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}},$$

que utiliza para estudiar el número de clase o la distribución de los ideales primos, y para la cual obtiene una ecuación funcional (cf. [Roq02]).

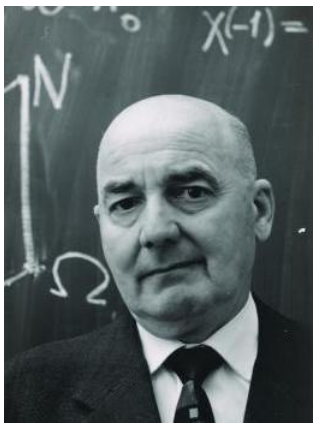
A partir de entonces se logran avances en la comprensión de $\zeta(s)$ gracias al trabajo de varios matemáticos: Friedrich Karl Schmidt con su definición de función zeta, para la que prueba la racionalidad y la ecuación funcional, o el uso del número de puntos *de grado 1*; Helmut Hasse obtiene una desigualdad de la forma

$$\left|N - (q+1)\right| \leq 2g\,q^{\theta}, \quad \theta \geq \frac{1}{2};$$

posteriormente su trabajo con Harold Davenport les permite probar un análogo de la hipótesis de Riemann (los ceros de ζ tienen parte real $1/2$) para el caso de cuerpos de funciones de curvas elípticas, utilizando la teoría de sumas exponenciales. La demostración general de este hecho para cuerpos de funciones de curvas arbitrarias tardará más, y recibirá aportaciones de otros matemáticos como Ernst Witt o Max Deuring (cf. [Roq04; Roq06; Roq12]). Finalmente, ya entrados los 40 André Weil publica una respuesta positiva a la hipótesis de Riemann para curvas (cf. [Wei48]).



Emil Artin



Helmut Hasse

André Weil

En 1949, Weil, que conocía de primera mano el trabajo realizado con la función zeta, *redefine* en concepto para adaptarlo a una variedad X arbitraria, tomando como función $Z(X)$ una *función generatriz* del número de puntos de una variedad sobre extensiones del cuerpo base en el que está definida (cf. [Wei49]). Sobre esa definición indica cuatro conjeturas:

1. Racionalidad.
2. Ecuación funcional.
3. Hipótesis de Riemann.
4. Relación con la homología de X.

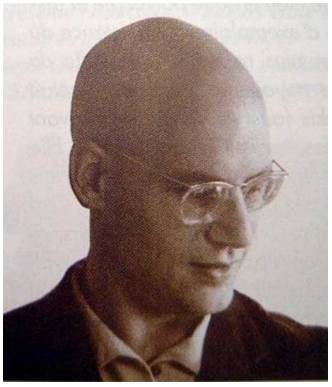
Como ejemplo, desarrolla la teoría de la función zeta de hipersuperficies de Fermat, y comprueba que las cuatro conjeturas son válidas expresando Z en función de sumas de Gauss.

La demostración de estas cuatro conjeturas (que pasarían a ser llamadas *conjeturas de Weil*) requeriría de grandes avances en geometría algebraica durante los siguientes 25 años. En el ICM de Ámsterdam en 1954, Weil explicó que la demostración podía venir de un nuevo tipo de homología. Esencialmente, los puntos de la variedad son *los que quedan fijos por el automorfismo de Frobenius* (adecuadamente particularizado en función de la extensión), con el teorema del punto fijo de Lefschetz se obtendría

$$\Big|\{\text{puntos de } X\}\Big| = \sum_{k\geq 0} (-1)^k \operatorname{tr}\big(\text{Frob} \mid H_k(X)\big),$$

donde quedaría por determinar la homología H con la que trabajar.

Bernard Dwork

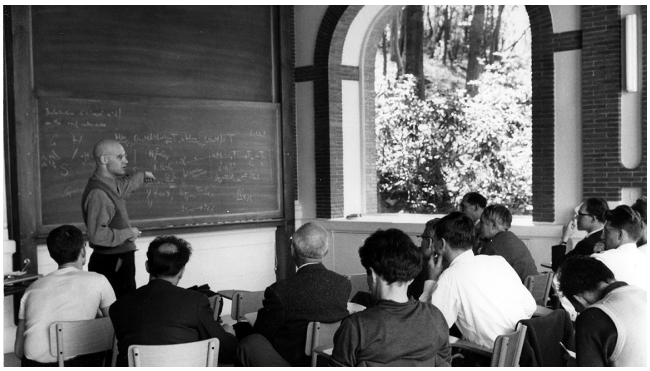


Alexander Grothendieck

Pierre Deligne

En 1960, Bernard Dwork demostró la racionalidad de la función zeta con métodos relativamente elementales de análisis p-ádico (cf. [Dwo60; Kob84]), aunque la prueba no

abrió paso a más estudios y no se realizaron más avances hacia las demás conjeturas por este camino.



Grothendieck impartiendo uno de sus seminarios en Bois Marie (IHES)

Durante la segunda mitad de los 60, Alexander Grothendieck y otros (incluyendo a Michael Artin, hijo de Emil Artin, o a Jean–Pierre Serre, medallista Fields y Abel) realizaron importantes avances utilizando la *cohomología étale* a través del *Seminario de Geometría Algebraica de Bois Marie* (cf. [Mil16; Gro95]). Con ella logran probar tanto la racionalidad como la ecuación funcional, pero la hipótesis de Riemann sigue pareciendo inaccesible.

Grothendieck *sugiere* una nueva línea de ataque basada en una serie de conjeturas más generales de las cuales se deducirían las conjeturas de Weil, pero su propuesta no logra tracción.

Finalmente, en 1973, Pierre Deligne, que tenía tan sólo 5 años cuando Weil formuló sus conjeturas, concluyó la demostración de la hipótesis de Riemann, aunque alejándose de las conjeturas propuestas por Grothendieck (cf. [Gro88, § III.18.5.2.2.]), convirtiendo las conjeturas en teorema (cf. [Del74]).

A pesar de haber sido demostradas con total generalidad a día de hoy, las conjeturas de Weil mantienen su numbre inicial. Una exposición más extensa de la historia de las demostraciones puede leerse en los artículos de Milne ([Mil16]) y Oort ([Oor14]), o en [Har77, § C.2].

1

Funciones zeta y conjeturas de Weil

If there is one thing in mathematics that fascinates me more than anything else (and doubtless always has), it is neither "number" nor "size", but always form. And among the thousand-and-one faces whereby form chooses to reveal itself to us, the one that fascinates me more than any other and continues to fascinate me, is the structure hidden in mathematical things.

— Alexander Grothendieck

En este capítulo introduciremos las nociones fundamentales para el trabajo: el concepto de variedad algebraica proyectiva, las particularidades que puede presentar al estar definida sobre un cuerpo finito, su función zeta (interpretada de diferentes maneras) y finalmente las conjeturas de Weil.

Como notación, tomaremos p un número primo, y $q = p^r$, con r un entero positivo. Llamaremos $\mathbb{F}_q$ al único cuerpo (salvo isomorfismo) con q elementos, y $\mathbb{F}_{q^s}$ a una extensión de $\mathbb{F}_q$ de grado s.

1.1. Variedades proyectivas

Empezamos recordando el concepto de variedades proyectivas. En el espacio afín es inmediato definir el valor de un polinomio f en un punto $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1}$ como $f(a_0, \ldots, a_n)$. En el caso proyectivo esta identificación no puede hacerse, porque a un mismo punto le corresponden varios representantes multiplicando por un escalar.

Pese a ello, si f es homogéneo, es posible definir el cero de un polinomio, porque si

$[a_0 : \cdots : a_n] \in \mathbb{P}^n$ es un representante de un punto proyectivo que anula a f, entonces

$$f(\lambda[a_0 : \cdots : a_n]) = f(\lambda a_0, \ldots, \lambda a_n) = \lambda^{\deg f} f(a_0, \ldots, a_n) = 0.$$

Por lo tanto, si para un polinomio f homogéneo, el conjunto algebraico proyectivo

$$\mathcal{V}(f) = \{a \in \mathbb{P}^n \mid f(a) = 0\} \subset \mathbb{P}^n$$

está bien definido. Si en lugar de tomar un único polinomio tomamos un ideal $I \subset k[x_0, \ldots, x_n]$ homogéneo (es decir, tal que sus generadores, de los cuales hay una cantidad finita por ser el anillo noetheriano, sean todos homogéneos), tiene también asociado un conjunto algebraico proyectivo

$$\mathcal{V}(I) = \{a \in \mathbb{P}^n \mid f(a) = 0 \forall f \in I\} \subset \mathbb{P}^n.$$

Si I es además primo, entonces decimos que $X = \mathcal{V}(I)$ es una variedad algebraica. Esta condición hace que X sea en cierto sentido irreducible, es decir, que no podamos descomponer

$$X = U_1 \cup U_2,$$

con U_1 y U_2 conjuntos algebraicos tales que no están contenidos uno no está contenido en el otro. Esta definición de irreducibilidad es análoga a la que se formularía en términos de espacios topológicos.

1.1.1. Dimensión de una variedad

A cada variedad podemos asignarle un entero que codifique el concepto de dimensión. Lo haremos a través de la topología de Zariski, que tiene como cerrados a los conjuntos algebraicos.

DEFINICIÓN 1.1.1 ***(Dimensión de una variedad).*** **—** Sea $X \subset \mathbb{P}^n(k)$ una variedad proyectiva. Definimos la *dimensión* de X, que escribimos como $\dim X$, como la longitud de la mayor cadena de cerrados irreducibles contenidos en X, es decir, el mayor entero n tal que existen cerrados $X_1, \ldots, X_n$ que cumplen

$$\emptyset \neq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n = X.$$

OBSERVACIÓN 1.1.2. — Es posible también dar una noción de dimensión basada en álgebra conmutativa. Hacemos esto utilizando la correspondencia biunívoca entre variedades e ideales primos.

DEFINICIÓN 1.1.3. **—** Sea A un anillo. La altura de un ideal primo $\mathfrak{p}$ es el mayor entero

n tal que existe una cadena de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}.$$

Llamamos *dimensión de Krull* de A al supremo (no necesariamente finito) de las alturas de los ideales primos de A.

PROPOSICIÓN 1.1.4. — *Sea $X \subset \mathbb{P}^n(k)$ una variedad proyectiva, y sea $I = \mathcal{I}(X) \subset k[x_0, \ldots, x_n]$ su ideal primo correspondiente en el anillo de polinomios. Entonces* $\dim X$ *se corresponde con la dimensión de Krull del anillo cociente $k[x_0, \ldots, x_n]/I$ menos 1.*

Intuitivamente, cada subvariedad X_i se corresponde con un ideal $\mathcal{I}(X_i) \subset k[x_0, \ldots, x_n]$ que contiene a I, por lo tanto una cadena de cerrados equivale a una cadena de ideales. Nótese que restamos uno para descartar el *ideal irrelevante* dado por $\langle x_0, x_1, \ldots, x_n \rangle$, cuya variedad proyectiva es el vacío, pero que admitimos en el cálculo de la dimensión de Krull.

La definición anterior es consistente con algunas propiedades que le pedimos a la dimensión, como por ejemplo que la dimensión de $\mathbb{A}^n$ y de $\mathbb{P}^n$ sea exactamente n. Además,

PROPOSICIÓN 1.1.5. — *Una variedad proyectiva X en un espacio de dimensión n tiene dimensión $n-1$ si y sólo si $X = \mathcal{V}(f)$, con $f \in k[x_0, \ldots, x_n]$ homogéneo e irreducible.*

Demostración. La demostración requiere de herramientas alejadas del objetivo de este trabajo, por lo que la omitimos y referimos a [Har77, § I.2]. □

Esta proposición nos permite establecer la dimensión de variedades generadas por un único polinomio, que conforman el núcleo del trabajo.

1.1.2. Variedades no singulares

Una variedad no singular (o lisa) es, como uno podría esperar, una variedad sin puntos singulares, es decir, que en cierto sentido puede ser vista como un equivalente de las variedades diferenciables en $\mathbb{C}^n$.

DEFINICIÓN 1.1.6. — Sea $X = \mathcal{V}\left(\langle f_1, \ldots, f_l \rangle\right)$ una variedad algebraica. Se dice que es *no singular* si, para cada $P \in X$, la matriz jacobiana

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i,j}$$

tiene rango $n - \dim X$.

En el caso de una hipersupericie (por ejemplo, una curva en el plano), ser no singular es equivalente a que no todas las derivadas parciales se anulen simultáneamente.

1.1.3. Cuerpos finitos

En general, es común definir las variedades algebraicas sobre cuerpos algebraicamente cerrados (donde tenemos resultados muy fuertes como el Nullstellensatz). No obstante, vamos a trabajar con cuerpos finitos, que nunca son algebraicamente cerrados (de manera trivial, basta tomar un polinomio de grado mayor que el número de elementos y sin raíces múltiples). A pesar de esto, es posible obtener resultados interesantes en cuerpos finitos.

PROPOSICIÓN 1.1.7. — *Sea $\mathbb{F}_q \supset \mathbb{F}_p$ un cuerpo finito con p^r elementos. Llamamos* automorfismo de Frobenius *a*

$$\begin{array}{rccc} \varphi & : & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & x^p. \end{array}$$

Se cumple que φ genera $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/r\mathbb{Z}$. Además, si $\mathbb{F}_{q^s}$ es una extensión de grado s de $\mathbb{F}_q$, entonces φ^r genera el correspondiente grupo $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) \cong \mathbb{Z}/s\mathbb{Z}$.

Demostración. Para la primera parte, es claro que φ es un homomorfismo, y además es inyectivo, porque

$$a^p = b^p \implies a^p - b^p = (a-b)^p = 0 \implies a - b = 0 \implies a = b.$$

Por tratarse de un homomorfismo inyectivo entre cuerpos finitos sabemos que será también isomorfismo. Y por el teorema de Euler, sabemos también que actúa como la identidad en $\mathbb{F}_p$, luego $\varphi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Como $\mathbb{F}_q$ es el cuerpo de descomposición de $x^{p^r} - 1 = 0$ sobre $\mathbb{F}_p$, es claro que φ^r es trivial. Y, por otra parte, si una potencia menor de φ (por ejemplo φ^k) fuera trivial entonces se tendría que

$$a^{p^k} - 1 = 0 \quad \forall a \in \mathbb{F}_q,$$

lo cual es imposible porque un polinomio de grado p^k no puede tener $p^r > p^k$ raíces. Entonces $\varphi, \varphi^2, \ldots, \varphi^r$ son diferentes, y como $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p] = r$ se tiene el resultado.

Para la segunda, la inclusión de cuerpos $\mathbb{F}_p \subset \mathbb{F}_q \subset \mathbb{F}_{q^s}$ genera una inclusión de grupos $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) \subset \mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_p)$, y como sabemos que φ tiene orden $r \cdot s$ en $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_p)$, es evidente que φ^r genera un subgrupo de orden s. Como $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ tiene también

orden s, y en un grupo cíclico no puede haber más de un subgrupo de un orden dado, se deduce que $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) = \langle \varphi^r \rangle \cong \mathbb{Z}/s\mathbb{Z}$. □

A partir de ahora, si trabajamos en el cuerpo base $\mathbb{F}_q$, llamaremos φ al automorfismo de Frobenius en $\mathbb{F}_q$, $\varphi : x \mapsto x^q$. Además de la del grupo de Galois, es posible dar una caracterización sencilla de la clausura algebraica de $\mathbb{F}_p$.

PROPOSICIÓN 1.1.8. — *Sea $\mathbb{F}_q$ un cuerpo con q elementos. Entonces, su clausura algebraica es*

$$\overline{\mathbb{F}} = \bigcup_{s=1}^{\infty} \mathbb{F}_{q^s}.$$

Además, $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^s}$ si y solo si $d \mid s$.

Demostración. Para la segunda parte, es evidente que si $d \mid s$, entonces $\mathbb{F}_{q^d}$ es el subcuerpo de $\mathbb{F}_{q^s}$ que queda fijo por $\langle \varphi^d \rangle$. Y en la otra dirección,

$$\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^s} \implies s = [\mathbb{F}_{q^s} : \mathbb{F}_{q^d}]\, d \implies d \mid s.$$

Para la primera, es evidente que $\overline{\mathbb{F}}$ es un cuerpo. Consideremos el polinomio

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \overline{\mathbb{F}}[x].$$

Si cada a_i está en la extensión $\mathbb{F}_{q^{s_i}}$, escribiendo $s = s_0 \cdot s_1 \cdot \cdots \cdot s_n$, se tendrá que todos los coeficientes están en $\mathbb{F}_{q^s}$, y por lo tanto todas las raíces de f estarán en un cuerpo $\mathbb{F}_{q^N}$, con $s \mid N$, luego en efecto $\overline{\mathbb{F}}$ es algebraicamente cerrado, y que es lo más pequeño posible es evidente porque debe contener al menos a todos los $\mathbb{F}_{q^s}$. □

Supongamos entonces que tenemos un ideal homogéneo primo $I \subset \mathbb{F}_q[x_0, \ldots, x_n]$. Este ideal define una variedad algebraica proyectiva $X \subset \mathbb{P}^n(\overline{\mathbb{F}})$ que podemos expresar como

$$X = \bigcup_{s=1}^{\infty} X(\mathbb{F}_{q^s}),$$

donde entendemos por $X(\mathbb{F}_{q^s})$ el conjunto de puntos de X cuyas coordenadas pertenecen todas a $\mathbb{F}_{q^s}$. Consideremos un punto $a = [a_0 : \cdots : a_n] \in X(\mathbb{F}_{q^d})$, tal que $\mathbb{F}_{q^d}$ es la menor extensión de $\mathbb{F}_{q^d}$ que contiene a todas sus coordenadas. Llamamos $\varphi(a) = [a_0^q : \cdots : a_n^q]$. Entonces se tiene que

$$\begin{aligned} f(\varphi(a)) = f(a_0^q, \ldots, a_n^q) = f(a)^{q^{\deg f}} = \\ = \varphi^{\deg f}(f(a)) = 0 \quad \forall f \in I \implies a^q \in X(\mathbb{F}_{q^d}), \end{aligned}$$

porque φ no afecta a los coeficientes de f que están en $\mathbb{F}_q$, y $(x+y)^q = x^q + y^q$. Aplicando φ sucesivamente para hallar la órbita de a obtenemos el *divisor primo*

$$\mathfrak{D} = \{a, \varphi(a), \varphi^2(a), \ldots, \varphi^d(a) = a\},$$

donde obtenemos la última igualdad utilizando que, al estar todas las coordenadas en $\mathbb{F}_{q^d}$, el automorfismo de $\overline{\mathbb{F}}$ dado por φ^d restringido a $\mathbb{F}_{q^d}$ coincide con la identidad. Llamamos grado del divisor primo $\mathfrak{D}$, $\deg\mathfrak{D}$, al número de puntos (diferentes) de $\mathfrak{D}$.

PROPOSICIÓN 1.1.9. — *Se cumple que* $\deg\mathfrak{D} = d$.

Demostración. Es evidente por construcción que hay como mucho d puntos diferentes. Tomemos $0 \le i < j$, entonces

$$\begin{aligned}\varphi^i(a) = \varphi^j(a) &\implies \varphi^i(a - \varphi^{j-i}(a)) = 0 \implies \varphi^{j-i}(a) = a \implies \\ &\implies d \mid j-i \implies j = i + kd \ge d.\end{aligned}$$

Por lo tanto, como no puede haber dos iguales entre los d primeros, concluimos que $\deg\mathfrak{D} = d$. □

OBSERVACIÓN 1.1.10. — Podemos identificar el conjunto de divisores primos $\mathfrak{D}$ con las órbitas de X por la acción de φ. Como cada elemento en $X(\overline{\mathbb{F}})$ pertenecerá a una única órbita, se tiene que

$$X = \bigsqcup_{\mathfrak{D}\in X} \mathfrak{D}.$$

1.1.4. *Reducción desde un cuerpo de números*

Sea X una variedad definida sobre un cuerpo de números $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, con $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}} \subset \mathbb{C}$. Si denotamos por $\mathcal{O}_K$ a su anillo de enteros, es evidente que los elementos de K se pueden escribir como un cociente a/b, con $a, b \in \mathcal{O}_K$ (es decir, K es el cuerpo de fracciones de $\mathcal{O}_K$).

OBSERVACIÓN 1.1.11. — Partiendo de una variedad definida $X \subset \mathbb{P}^n(K)$, podemos considerar la inclusión natural $X \subset \mathbb{P}^n(K) \hookrightarrow \mathbb{P}^n(\mathbb{C})$. Aunque vista en los complejos no es una variedad, lo que sí que se tiene es que, definiendo $\overline{X}$ de manera natural como

$$X \hookrightarrow \overline{X} = \mathcal{V}(\mathcal{I}(X)) \subset \mathbb{P}^n(\mathbb{C}),$$

entonces $\overline{X}$ es una variedad algebraica proyectiva compleja que *extiende* a X.

Sea I un ideal en $K[x_0, \ldots, x_n]$. Por tratarse de un anillo Noetheriano I estará generado por unos polinomios $f_1, \ldots, f_l$. Escojamos un primo $\mathfrak{p} \in \mathcal{O}_K$ tal que no divida a ninguno

de los denominadores de los coeficientes de los polinomios que generan el ideal I. Entonces $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo con $\mathrm{N}(\mathfrak{p}) = p^r = q$ elementos, y podemos escribir los f_i como polinomios en $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$ ya que los denominadores son invertibles – denotamos g_i al polinomio f_i reducido en $\mathbb{F}_q$.

Si $X \subset \mathbb{P}^n(K)$ es una variedad tal que $I = \mathscr{I}(I)$, entonces los g_i definen su *reducción* a $\mathbb{F}_q$. Por lo tanto, hemos pasado de una variedad X a otra $X_\mathfrak{p} = \mathcal{V}(\langle g_1, \ldots, g_l \rangle) \subset \mathbb{P}^n(\mathbb{F}_q)$. Llamamos a este proceso *reducción módulo* $\mathfrak{p}$.

1.2. Función zeta de una variedad

La idea de función zeta es la de agrupar en una única función información sobre la variedad de la que proviene, mediante el número de puntos N_s de la variedad en una extensión de grado s del cuerpo base. Uno podría plantearse entonces definir

$$Z(X,u) = \sum_{i=1}^{\infty} N_s u^s,$$

pero la definición real es ligeramente diferente.

DEFINICIÓN 1.2.1. — Sea X una variedad proyectiva no singular en $\mathbb{P}^n(\mathbb{F}_q)$, y sea N_s el número de puntos de la variedad en una extensión de grado s de $\mathbb{F}_q$. Entonces se define la *función zeta de* X como

$$Z(X,u) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\right).$$

Por comodidad daremos por entendida la variedad cuando no cause confusión, y escribiremos simplemente $Z(u)$. Aunque esta definición parezca artificial, está fuertemente relacionada con la que imaginamos previamente.

PROPOSICIÓN 1.2.2. — $u \dfrac{\mathrm{d}}{\mathrm{d}u} \log Z(u) = \displaystyle\sum_{s=1}^{\infty} N_s u^s.$

Demostración. $\dfrac{\mathrm{d}}{\mathrm{d}u} \log Z(u) = \dfrac{\mathrm{d}}{\mathrm{d}u} \displaystyle\sum_{s=1}^{\infty} \frac{N_s u^s}{s} = \sum_{s=1}^{\infty} \frac{\mathrm{d}}{\mathrm{d}u} \frac{N_s u^s}{s} = \sum_{s=1}^{\infty} N_s u^{s-1}.$ □

En algunos casos es posible encontrar la función zeta definida a partir de la fórmula anterior (por ejemplo, [Wei49]). Aunque la definición con la exponencial parezca más complicada, en realidad simplifica notablemente los cálculos en la gran mayoría de casos.

EJEMPLO 1.2.3. — Si X es una variedad tal que, para toda extensión del cuerpo base, $N_s(X) = \alpha(s) + \beta(s) = N_s(A) + N_s(B)$, entonces

$$Z(X,u) = \exp\left(\sum_{s=1}^{\infty} \frac{(\alpha(s)+\beta(s))u^s}{s}\right) = \exp\left(\sum_{s=1}^{\infty} \frac{\beta(s)u^s}{s} + \sum_{s=1}^{\infty} \frac{\beta(s)u^s}{s}\right) =$$
$$= \exp\left(\sum_{s=1}^{\infty} \frac{\alpha(s)u^s}{s}\right) \cdot \exp\left(\sum_{s=1}^{\infty} \frac{\beta(s)u^s}{s}\right) = Z(A,u) \cdot Z(B,u).$$

EJEMPLO 1.2.4. — Supongamos ahora que tenemos X tal que $N_s = \alpha^s$. Entonces

$$Z(u) = \exp\left(\sum_{s=1}^{\infty} \frac{(\alpha u)^s}{s}\right).$$

Utilizando que la serie formal del logaritmo es

$$-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n},$$

llegamos a

$$Z(u) = \exp\big(-\log(1-\alpha u)\big) = \frac{1}{1-\alpha u}.$$

EJEMPLO 1.2.5. — Expandiendo el ejemplo anterior, supongamos que $N_s = \sum \alpha_i^s - \sum \beta_j^s$. Entonces es fácil ver que

$$Z(u) = \frac{(1-\beta_1 u)\cdots(1-\beta_m u)}{(1-\alpha_1 u)\cdots(1-\alpha_n u)} \in \mathbb{C}(u),$$

imitando el cálculo anterior en base a la serie formal del logaritmo. Lo verdaderamente interesante (y sorprendente) es que el recíproco también es cierto.

PROPOSICIÓN 1.2.6. — *Si $Z(u) \in \mathbb{C}(u)$, entonces $N_s = \sum \alpha_i^s - \sum \beta_j^s$.*

Demostración. Para probarlo, supongamos que tenemos $Z(u) = P(u)/Q(u)$, con P y Q polinomios. Como $Z(0) = 1$ (basta ver la definición para llegar a $Z(0) = e^0$), tenemos que $P(0) = Q(0)$, luego podemos suponer que $P(0) = Q(0) = 1$ – en caso contrario, bastaría dividir ambos polinomios por el término independiente y Z se mantendría invariante. Podemos entonces escribir P y Q como

$$P(u) = \prod_{j=1}^{\deg P} (1-\beta_j u) \quad \text{y} \quad Q(u) = \prod_{i=1}^{\deg Q} (1-\alpha_i u),$$

es decir, como producto de sus respectivas *raíces inversas*. Si denotamos los grados

como $m = \deg P$ y $n = \deg Q$, con la derivada logarítmica llegamos a

$$u\frac{\mathrm{d}}{\mathrm{d}u}\log Z(u) = \sum_{i=1}^{n}\frac{\alpha_i u}{1-\alpha_i u} - \sum_{j=1}^{m}\frac{\beta_j u}{1-\beta_j u} = \\ = \sum_{i=1}^{n}\left(\sum_{s=1}^{\infty}(\alpha_i u)^s\right) - \sum_{j=1}^{m}\left(\sum_{s=1}^{\infty}(\beta_j u)^s\right).$$

Agrupando términos en u^s y por la proposición 1.2.2 llegamos a

$$u\frac{\mathrm{d}}{\mathrm{d}u}Z(u) = \sum_{s=1}^{\infty}\left(\sum_{i=1}^{n}\alpha_i^s - \sum_{j=1}^{m}\beta^s\right)u^s = \sum_{s=1}^{\infty}N_s u^s \implies N_s = \sum\alpha_i^s - \sum\beta_j^s. \qquad \square$$

El nombre de función zeta no es casual. Recordemos que podemos escribir la función ζ de Riemann como el producto sobre todos los primos

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}.$$

Si llamamos X_p a la variedad dada por $x_0 = 0$ en $\mathbb{P}(\mathbb{F}_p)$, es inmediato que $Z(u) = (1-u)^{-1}$. Haciendo el cambio de variable

$$\zeta(X_p, s) = Z(X_p, q^{-s}) = \frac{1}{1-p^{-s}},$$

se obtiene

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \prod_p \zeta(X_p, s).$$

Es posible de hecho dar un resultado más general que ponga de manifiesto la relación entre ambas funciones. Recordemos que en la sección anterior vimos cómo dividir los puntos de una variedad en una serie de divisores primos $\mathfrak{D}$ disjuntos. Podemos entonces enunciar la siguiente

PROPOSICIÓN 1.2.7. — $Z(u) = \prod_{\mathfrak{D}} \frac{1}{1-u^{\deg\mathfrak{D}}}$.

Demostración. Agrupando todos los términos del producto con el mismo grado obtenemos

$$\prod_{\mathfrak{D}}\frac{1}{1-u^{\deg\mathfrak{D}}} = \prod_{n=1}^{\infty}\left(\frac{1}{1-u^n}\right)^{a_n},$$

donde a_n es el número de divisores de grado n. Si tomamos la derivada logarítmica

del producto tendremos

$$\frac{\mathrm{d}}{\mathrm{d}u}\log\prod_{n=1}^{\infty}\left(\frac{1}{1-u^n}\right)^{a_n}=\sum_{n=1}^{\infty}\frac{na_nu^{n-1}}{1-u^n}=\frac{1}{u}\sum_{n=1}^{\infty}\left(na_nu^n\sum_{k=0}^{\infty}u^k\right).$$

Expandiendo la última expresión como serie en u obtenemos que el término correspondiente a u^n será $\sum_{d|n}da_d$, que por la proposición 1.1.8 coincide con N_s, llegando a

$$\frac{1}{u}\sum_{n=1}^{\infty}\left(\sum_{d|n}da_d\right)u^n=\sum_{s=1}^{\infty}N_su^{s-1},$$

que es precisamente la expresión de $Z(u)$ como función generatriz de N_s. □

Para apreciar mejor la analogía podemos utilizar de nuevo el cambio de variable $u=q^{-s}$. Si, dado un divisor primo, definimos su norma como $\mathrm{N}(\mathfrak{D})=q^{\deg\mathfrak{D}}$, el número de elementos del menor cuerpo en el que está contenidp. Entonces la función zeta queda escrita como

$$Z(X,q^{-s})=\zeta(X,s)=\prod_{\mathfrak{D}}\frac{1}{1-q^{-s\deg\mathfrak{D}}}=\prod_{\mathfrak{D}}\frac{1}{1-\mathrm{N}(\mathfrak{D})^{-s}}.$$

OBSERVACIÓN 1.2.8. — Al principio de la sección veíamos que la definición de función zeta no es la *natural* a partir de la función generatriz de N_s, pero lo cierto es que la verdadera función zeta natural es la dada por

$$\zeta(s)=\prod_{\mathfrak{p}}\frac{1}{1-\mathrm{N}(\mathfrak{p})^{-s}}=\sum_{\mathfrak{a}}\frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{p}$ recorre los ideales primos de un cuerpo de números, y $\mathfrak{a}$ todos los ideales de ese mismo cuerpo (cf. [Neu99, § VII.5]). Lo sorprendente por lo tanto es la conexión entre la función zeta y la función generatriz de N_s.

EJEMPLO 1.2.9. — Calculemos la función zeta del espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$. Sabemos que en una extensión de grado s de $\mathbb{F}_q$ el espacio proyectivo tiene $N_s=q^{ns}+q^{(n-1)s}+\cdots+1$ puntos (q^{ns} en el afín, $q^{(n-1)s}$ en el afín del hiperplano del infinito, y siguiendo hasta llegar al punto en el infinito). Podemos escribir la función zeta de $\mathbb{P}^n$ como

$$\begin{aligned}Z(\mathbb{P}^n,u)&=\exp\left(\sum_{s=1}^{\infty}\sum_{k=0}^{n}\frac{(q^ku)^s}{s}\right)=\exp\left(\sum_{k=0}^{n}-\log(1-q^ku)\right)\\&=\frac{1}{(1-u)(1-qu)\cdots(1-q^nu)}.\end{aligned}$$

1.3. Conjeturas de Weil

En el ejemplo anterior podemos ver que la función zeta de $\mathbb{P}^n$ es de hecho una función racional. Esto no es casualidad: se trata de una de las propiedades que estudiaremos de las funciones zeta.

TEOREMA 1.3.1 ***(Conjeturas de Weil).*** — *Sea X una variedad proyectiva no singular n-dimensional definida en $\mathbb{F}_q$. La función zeta de X satisface*

1. *Racionalidad: $Z(u)$ es una función racional de u, con coeficientes enteros.*
2. *Ecuación funcional: si E es la característica de Euler de la variedad que define X, entonces*
$$Z\left(\frac{1}{q^n u}\right) = \pm q^{nE/2} u^E Z(u).$$
3. *Hipótesis de Riemann: es posible escribir*
$$Z(u) = \frac{P_1(u)\cdots P_{2n-1}(u)}{P_0(u)\cdots P_{2n}(u)},$$
con $P_0(u) = 1-u$, $P_{2n}(u) = 1-q^n u$, y para cada $1 \le i \le 2n$ podemos escribir
$$P_i(u) = \prod_{j=1}^{\deg P_i} (1-\alpha_{ij}u) \in \mathbb{Z}[u],$$
con los α_{ij} enteros algebraicos que cumplen $|\alpha_{ij}| = q^{i/2}$.
4. *Números de Betti: con la notación del punto anterior, escribimos $B_i(X) = \deg P_i$. Entonces $E = \sum(-1)^i B_i$, y si X es la reducción módulo $\mathfrak{p}$ de una variedad definida sobre un cuerpo de números $Y \subset \mathbb{Q}(\alpha_1,\dots,\alpha_m)^k \subset \mathbb{C}^k$, entonces B_i se corresponde con el i-ésimo número de Betti de la variedad $\mathcal{V}(\mathcal{I}(Y)) \subset \mathbb{C}^k$.*

Las conjeturas de Weil permiten, por lo tanto, obtener información sobre la variedad a partir de su función zeta, y enlazan propiedades aritméticas (número de soluciones de una ecuación) con propiedades geométricas (números de Betti de una variedad).

Veamos una serie de detalles que podemos deducir de las conjeturas.

OBSERVACIÓN 1.3.2. — Si $Z(u)$ es una función racional en u, debe tenerse necesariamente que
$$N_s = \sum_{i=1}^{k} \alpha_i^s - \sum_{j=1}^{\ell} \beta_j^s.$$

Para $s=1$, teniendo en cuenta que $\alpha_1 = 1, \alpha_k = q^n$, se cumple que

$$\left|N-(q^n+1)\right| \leq \sum_{i=2}^{k-1} |\alpha_i| + \sum_{j=1}^{\ell} |\beta_j| \leq \sum_{r=1}^{2n-1} B_r q^{r/2},$$

es decir, conociendo la homología de X podemos *aproximar* el número de puntos de la variedad como $N \approx q^n+1$ y estudiar el error cometido.

Este enfoque puede no parecer demasiado interesante, pero su particularización para curvas (cuyos números de Betti son $1, 2g, 1$) tiene una serie de profundas consecuencias, que estudiaremos en el último capítulo.

OBSERVACIÓN 1.3.3. — La hipótesis de Riemann *clásica* establece que los ceros no triviales de la función ζ de Riemann se encuentran todos en la recta $\mathrm{Re}(z) = 1/2$. En la tercera conjetura de Weil, tenemos que $|\alpha_{ij}| = q^{i/2}$ (aquí i es un índice, no la unidad imaginaria), luego

$$\zeta(X,s) = 0 \implies 1-\alpha_{ij}q^{-s} = 0 \implies |q^{-s}| = q^{-i/2} \implies \mathrm{Re}(s) = \frac{i}{2}.$$

Con respecto a la ecuación funcional, de nuevo con el cambio de variable se tiene que

$$Z\left(\frac{1}{q^n u}\right) = \zeta(n-s) = \pm q^{nE/2} q^{-sE} \zeta(s) = q^{E(n/2-s)}\zeta(s) \implies$$
$$\implies \zeta(n-s)q^{-(n-s)E/2} = \zeta(s)q^{-sE/2},$$

luego hay una simetría en el cambio $s \mapsto n-s$ de manera similar a la simetría alrededor de $\mathrm{Re}(z) = 1/2$ de la ζ de Riemann con

$$\zeta(s)\Gamma\left(\frac{s}{2}\right)\pi^{-s/2} = \zeta(1-s)\Gamma\left(\frac{1-s}{2}\right)\pi^{-(1-s)/2}.$$

Veamos finalmente con el ejemplo anterior que, en efecto, las conjeturas de Weil se cumplen para el proyectivo.

EJEMPLO 1.3.4. — Recordamos que la función zeta del espacio proyectivo de dimensión n es

$$\frac{1}{(1-u)(1-qu)\cdots(1-q^n u)}.$$

Entonces se cumple que

1. $Z(u)$ es una función racional con coeficientes enteros.
2. Como la característica de Euler del espacio proyectivo complejo es $E = n+1$, se

puede verificar que $Z(u)$ cumple la ecuación funcional haciendo

$$\begin{aligned} Z\left(\frac{1}{q^n u}\right) &= \frac{1}{\left(1-\frac{1}{q^n u}\right)\left(1-q\frac{1}{q^n u}\right)\cdots\left(1-q^n\frac{1}{q^n u}\right)} = \\ &= \frac{\left(q^n u\right)^{n+1}}{(q^n u-1)(q^n u-q)\cdots(q^n u-q^n)} = \\ &= \frac{(-1)^{n+1}\left(q^n u\right)^{n+1}}{(1-q^n u)q(1-q^{n-1}u)\cdots q^n(1-u)} = \\ &= \frac{(-1)^{n+1}\left(q^n u\right)^{n+1}}{q^{n(n+1)/2}}\frac{1}{(1-q^n u)(1-q^{n-1}u)\cdots(1-u)} = \\ &= (-1)^{n+1}q^{n(n+1)/2}u^{n+1}Z(u) = \pm q^{nE/2}u^E Z(u). \end{aligned}$$

3. En efecto, $P_{2i+1}(u) = 1$ y $P_{2i}(u) = 1 - q^i u$, con $|q^i| = q^i = q^{2i/2}$.

4. Se cumple que $E = \sum \deg P_i = n+1$, y además los números de Betti del espacio proyectivo (complejo) son

$$B_i(\mathbb{P}^n(\mathbb{C})) = \begin{cases} 1 & \text{si } 0 \le i \le 2n, i \equiv 0 \mod 2, \\ 0 & \text{en otro caso,} \end{cases}$$

luego se tiene que $B_i(\mathbb{P}^n(\mathbb{C})) = \deg P_i(u)$.

2

Sumas de Gauss y Jacobi

Algebra is the offer made by the devil to the mathematician. The devil says: "I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvellous machine."

— Michael Atiyah

SI NUESTRO OBJETIVO es hallar la función zeta de una variedad X mediante el cálculo del número de puntos de la variedad en una extensión $\mathbb{F}_{q^s}$, necesitaremos herramientas que nos ayuden a calcular las soluciones de una ecuación sobre un cuerpo.

Por ello introducimos primero la teoría de caracteres, y después las sumas de Gauss y Jacobi, que nos permiten expresar las soluciones de ciertos polinomios. Además, podremos *elevarlas* a las extensiones del cuerpo base gracias a la relación de Hasse–Davenport.

2.1. Caracteres, norma y traza

Para la teoría de sumas exponenciales es fundamental la noción de los caracteres. Un carácter en un grupo abeliano finito G con m elementos es una función

$$\chi : G \to \mathbb{C}^\times,$$

que cumple que $\chi(ab) = \chi(a)\chi(b)$ para cualesquiera a y b en G. Utilizaremos de ahora en adelante para G de notación multiplicativa.

EJEMPLO 2.1.1. — Consideremos ε la función tal que, para todo $a \in G$, hace $\varepsilon(a) = 1$. Es evidente que ε es un carácter, que llamaremos carácter trivial.

La importancia de la noción de carácter multiplicativo viene a partir del siguiente teorema, que demostraremos más adelante, y que nos ayudará calcular el número de puntos de algunas variedades en cuerpos finitos (es decir, los coeficientes N_s de la función zeta de la variedad).

TEOREMA 2.1.2. — *Sea $a \in \mathbb{F}_p^\times$ y $n \mid p-1$. Entonces el número de soluciones de $x^n = a$ es*

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a),$$

donde la suma se extiende sobre todos los caracteres de $\mathbb{F}_p^\times$ tales que $\chi^n = \varepsilon$. Para extender la definición de χ a todo $\mathbb{F}_q$ definimos $\varepsilon(0) = 1$, y $\chi(0) = 0$ para cualquier otro $\chi \neq \varepsilon$.

Se tienen las siguentes propiedades.

PROPOSICIÓN 2.1.3. — *Sea χ un carácter y $a \in G$. Se cumplirán:*

1. $\chi(1) = 1$.
2. *$\chi(a)$ es una raíz de la unidad m-ésima.*
3. *$\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$, donde $\overline{z}$ denota el complejo conjugado de z.*
4. *La suma $\sum_t \chi(t)$, donde t recorre todos los valores de G, vale m si $\chi = \varepsilon$, y 0 en cualquier otro caso.*

Demostración.

1. $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$, y como $\chi(1) \neq 0$, debe tenerse que $\chi(1) = 1$.
2. G es un grupo con m elementos, luego $a^m = 1$ y se cumple que $\chi(a^m) = \chi(a)^m = \chi(1) = 1$.
3. La primera igualdad se obtiene haciendo $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$. Para la segunda, basta tener en cuenta que si z es un número complejo de módulo 1, entonces $z\overline{z} = e^{\theta i}e^{-\theta i} = e^0 = 1$, es decir, $z^{-1} = \overline{z}$.
4. El caso de ε es trivial. Supongamos por lo tanto que $\chi \neq \varepsilon$, y denotemos $S = \sum_t \chi(t)$. Como podemos escoger al menos un a tal que $\chi(a) \neq 1$ (porque no estamos en el carácter trivial) hacemos

$$\chi(a)T = \sum_{t \in G} \chi(a)\chi(t) = \sum_{t \in G} \chi(at) = \sum_{r \in G} \chi(r) = T \implies T = 0. \qquad \square$$

Aunque en la definición de caracteres admitíamos que tomaran cualquier valor complejo, la proposición anterior nos limita el rango de valores que puede tomar. Podemos mejorar el estudio de los caracteres dándoles estructura de grupo abeliano. Definimos las operaciones entre caracteres

$$\chi_1 \circ \chi_2(a) = \chi_1\chi_2(a) = \chi_1(a)\chi_2(a),\ \chi^{-1}(a) = \chi(a)^{-1} \quad \forall a \in G.$$

Es trivial ver que con las dos operaciones el conjunto de los caracteres en G es un grupo, cuyo elemento neutro es el carácter trivial ε, y que es abeliano por serlo $\mathbb{C}^\times$. Denotamos este grupo como $\hat{G}$.

Veamos algunas de las propiedades del grupo de caracteres. En primer lugar, su tamaño.

PROPOSICIÓN 2.1.4. — *El número de caracteres de un grupo G es igual al orden del grupo.*

Demostración. Necesitaremos un lema previo.

LEMA 2.1.5 *(Extensión de caracteres).* — *Si H es un subgrupo de G y $\chi \in \hat{H}$, entonces existe un $\tilde{\chi} \in \hat{G}$ tal que*

$$\tilde{\chi}(h) = \chi(h)\ \forall h \in H,$$

es decir, podemos extender χ a un carácter de G.

Demostración. Sea $x \in G \setminus H$, y sea d el mínimo entero con $x^d \in H$. Este entero existe siempre porque $1 \in H$. Tomamos $y \in \mathbb{C}^\times$ tal que $y^d = \chi(x^d)$, y en $K = \langle H, x\rangle$ definimos

$$\tilde{\chi}(x^n h) = y^n \chi(h).$$

Es evidente que $\tilde{\chi} \in \hat{K}$, ya que está bien definido porque

$$\begin{aligned} x^n h = x^m h' &\implies h'h^{-1} = x^{n-m} \in H \implies d \mid n-m = rd \\ &\implies \chi(h')\chi(h)^{-1} = \chi(x^{rd}) = \chi(x^d)^r = (y^d)^r = y^{n-m} \implies \tilde{\chi}(x^n h) = \tilde{\chi}(x^m h'). \end{aligned}$$

Por lo tanto, extendemos χ a un subgrupo estrictamente mayor. Repitiendo este proceso llegamos a la demostración del lema. □

Vayamos ahora a la demostración de la proposición, que haremos por inducción. Recordemos que, dado G, podemos construir una cadena de subgrupos

$$\{e\} = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_r = G,$$

con $G_{i+1} = \langle G_i, x_{i+1}\rangle$. Evidentemente G_0 tiene únicamente un carácter: el trivial. Supongamos que G_i tiene exactamente $n = |G_i|$ caracteres, y analicemos cómo se extienden a G_{i+1} (que cuenta con $n \cdot d$ elementos. Si $\chi \in \hat{G}_i$ es un carácter, su extensión a $\widehat{G_{i+1}}$ estará dada por

$$\tilde{\chi}(x_{i+1}^k g) = \chi(g)\tilde{\chi}(x_{i+1})^k.$$

Si $x_{i+1}^d = g_{i+1} \in G_i$, entonces $\tilde{\chi}(x_{i+1})^d = \chi(g_{i+1})$, luego hay d elecciones para $\tilde{\chi}(x_{i+1})$, y cada una determinará un carácter $\tilde{\chi}$ diferente, luego en $\widehat{G_{i+1}}$ habrá $n \cdot d$ caracteres provenientes de $\hat{G}_i$. Y por otra parte, cualquier carácter λ de $\widehat{G_{i+1}}$ la restricción $\lambda|_{G_i}$ es un carácter de G_i, luego debe ser la extensión de un carácter, con lo que llegamos a que

$$|\widehat{G_{i+1}}| = |G_{i+1}|,$$

lo que completa la demostración. □

Uno podría plantearse que la anterior proposición da mucha información sobre los caracteres de un grupo, pero lo cierto es que podemos afinar el estudio bastante más.

TEOREMA 2.1.6. — $\hat{G} \cong G$.

Demostración. Por el teorema fundamental de grupos abelianos finitamente generados, podemos escribir

$$G \cong \mathbb{Z}/p_1\mathbb{Z} \oplus \mathbb{Z}/p_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k\mathbb{Z} = Z,$$

con los p_i primos no necesariamente diferentes. Probaremos que $\hat{Z} \cong Z$, construyendo el isomorfismo

$$\begin{array}{rccc} \psi & : & Z & \longrightarrow & \hat{Z} \\ & & (a_1,\ldots,a_k) & \longmapsto & \left\{ \chi_a \ : \begin{array}{rcl} G & \longrightarrow & \mathbb{C}^\times \\ (x_1,\ldots,x_k) & \longmapsto & \zeta_{p_1}^{a_1x_1}\cdots\zeta_{p_k}^{a_kx_k} \end{array} \right\}. \end{array}$$

Es decir, ψ lleva un punto $(a_1,\ldots,a_k)$ en el carácter que lleva cada punto a

$$\chi_a(x_1,\ldots,x_k) = \exp\left(\frac{2\pi i}{p_1\cdots p_k}\left(a_1x_1p_2\cdots p_k + \cdots + a_kx_kp_1\cdots p_{k-1}\right)\right).$$

Es evidente que se trata de un carácter, puesto que al expandir $\chi(x+y)$ acabamos con dos sumandos que, por la exponencial, se convierten en producto de exponenciales, de donde llegamos a $\chi(x)\chi(y)$.

Para comprobar que ψ es un isomorfismo basta ver que es inyectiva (puesto que va entre dos grupos finitos con la misma cantidad de elementos). Y en efecto, si $\chi_a = \chi_b$,

entonces

$$\chi_a(1,0,\dots,0) = \exp\left(\frac{2\pi i}{p_1}a_1\right) = \exp\left(\frac{2\pi i}{p_1}b_1\right) = \chi_b(1,0,\dots,0). \implies a_1 = b_1$$

$$\vdots$$

$$\chi_a(0,\dots,0,1) = \exp\left(\frac{2\pi i}{p_k}a_k\right) = \exp\left(\frac{2\pi i}{p_k}b_k\right) = \chi_b(0,\dots,0,1). \implies a_k = b_k \implies$$

$$\implies a = (a_1,\dots,a_k) = (b_1,\dots,b_k) = b.$$

Finalmente, si φ es un isomorfismo entre G y H, se tiene que

$$\begin{array}{rccc} \hat{\varphi} & : & \hat{G} & \longrightarrow & \hat{H} \\ & & \chi & \longmapsto & \chi \circ \varphi^{-1} \end{array}$$

es un isomorfismo entre $\hat{G}$ y $\hat{H}$, luego

$$G \cong Z \cong \hat{Z} \cong \hat{G}. \qquad \square$$

Veamos cómo se traduce esto en el caso de caracteres multiplicativos de $\mathbb{F}_q$.

COROLARIO 2.1.7. — $\widehat{\mathbb{F}_q^\times} \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

COROLARIO 2.1.8. — *Para todo $a \in \mathbb{F}_q^\times \setminus \{1\}$ existe un carácter χ de $\mathbb{F}_q$ tal que $\chi(a) \neq 1$.*

Demostración. Basta tomar $\chi : g^k \mapsto \zeta_{q-1}^k$ para un generador g de $\mathbb{F}_q^\times$. $\square$

COROLARIO 2.1.9. — *Para todo $a \in \mathbb{F}_q^\times \setminus \{1\}$, se tiene $\sum_\chi \chi(a) = 0$, donde la suma recorre todos los caracteres de $\mathbb{F}_q$.*

Demostración. Sea $S = \sum_\chi \chi(a)$. Escojamos un carácter λ tal que $\lambda(a) \neq 1$. Entonces

$$\lambda(a)S = \sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a) = \sum_{\chi'} \chi'(a) = S \implies S = 0. \qquad \square$$

Hasta ahora hemos estudiado numerosas propiedades de los caracteres en un cuerpo fijo $\mathbb{F}_q$. Pero, a partir de la definición de función zeta, cabe preguntarse: ¿cómo podemos relacionar los caracteres de $\mathbb{F}_q$ con los de $\mathbb{F}_{q^s}$, un cuerpo que contenga a $\mathbb{F}_q$ con q^s elementos? Para analizar la relación entre los caracteres introducimos dos nuevas funciones: la norma y la traza.

DEFINICIÓN 2.1.10. — Sea k un cuerpo, y sea K/k una extensión de Galois. Se definen la traza y la norma de K a k como

$$\mathrm{tr}_{K/k}(\alpha) = \sum_{\sigma} \sigma(\alpha) \quad \text{y} \quad \mathrm{N}_{K/k} = \prod_{\sigma} \sigma(\alpha),$$

respectivamente, donde la suma y el producto recorren los automorfismos $\sigma \in \mathrm{Gal}(K/k)$.

En ocasiones denotaremos $\mathrm{tr}_{K/k}$ y $\mathrm{N}_{K/k}$ para evitar posibles confusiones sobre a qué cuerpos nos referimos, pero en general escribiremos tr y N, dando por entendidos los cuerpos.

OBSERVACIÓN 2.1.11. — Si k es un cuerpo finito con q elementos, y $[K:k] = s$ entonces, a partir de la proposición 1.1.7, es inmediato ver que

$$\mathrm{tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}} \quad \text{y} \quad \mathrm{N}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{s-1}}.$$

De ahora en adelante utilizaremos con frecuencia esta caracterización.

PROPOSICIÓN 2.1.12. — *Sean $\alpha, \beta \in K$ y $a \in k$. Entonces,*

1. $\mathrm{tr}(\alpha) \in k$.
2. $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$.
3. $\mathrm{tr}(a\alpha) = a\,\mathrm{tr}(\alpha)$.
4. $\mathrm{tr}(K) = k$.

Demostración.

1. $\mathrm{tr}(\alpha)^q = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^s} = \alpha^q + \alpha^{q^2} + \cdots + \alpha = \mathrm{tr}(\alpha)$, es decir, $\mathrm{tr}(\alpha)$ anula el polinomio $x^q - x$, y por lo tanto debe suceder que $\mathrm{tr}(\alpha) \in k$.

2. Como $(\alpha+\beta)^q = \alpha^q + \beta^q$, por estar en un cuerpo de característica divisora de q,

$$\begin{aligned}\mathrm{tr}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{s-1}} = \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{s-1}} + \beta^{q^{s-1}} = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta).\end{aligned}$$

3. Como $a \in k$, se cumple que $a^q = a$, y por lo tanto

$$\mathrm{tr}(a\alpha) = a\alpha + a\alpha^q + \cdots + a\alpha^{q^{s-1}} = a\,\mathrm{tr}(\alpha).$$

4. Bastaría hallar γ tal que $\mathrm{tr}(\gamma) = c \neq 0$, porque en ese caso para todo $a \in k$ podríamos hacer $\mathrm{tr}(\gamma a/c) = a\,\mathrm{tr}(\gamma)/c = a$. La existencia de este γ la tenemos porque

$$f(x) = x + x^q + \cdots + x^{q^{s-1}}$$

es un polinomio de grado q^{s-1}, y por lo tanto todos los q^s elementos de K no pueden ser simultáneamente raíces. □

PROPOSICIÓN 2.1.13. — *Sean $\alpha, \beta \in K$ y $a \in k$. Entonces,*

1. $\mathrm{N}(\alpha) \in k$.
2. $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.
3. $\mathrm{N}(a\alpha) = a^s \mathrm{N}(\alpha)$.
4. $\mathrm{N}(K^*) = k^*$.

Demostración. Los apartados 1 y 2 son iguales a la demostración anterior.

3. $\mathrm{N}(a\alpha) = a\alpha \cdot a\alpha^q \cdot \cdots \cdot a\alpha^{q^{s-1}} = a^s \cdot \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{s-1}} = a^s \mathrm{N}(\alpha)$.
4. Consideremos el homomorfismo $\mathrm{N}^* : K^* \to k^*$. El núcleo de la aplicación son los elementos α de K^* tales que

$$\mathrm{N}^*(\alpha) = 1 \implies \alpha^{\frac{q^s-1}{q-1}} = 1.$$

Como K^* es cíclico, habrá exactamente $\varphi(d)$ elementos de orden d para cada divisor de $|K^*|$, y por lo tanto el número de soluciones para α será

$$\sum_{d \mid \frac{q^s-1}{q-1}} \varphi(d) = \frac{q^s-1}{q-1} \quad \text{porque} \quad \frac{q^s-1}{q-1} \mid q^s - 1 = |K^*|,$$

luego $K^*/\ker \mathrm{N}^*$ tiene exactamente $q-1$ elementos. Y como N establece un isomorfismo canónico entre $K^*/\ker \mathrm{N}^*$ y su imagen, debe suceder que

$$|\mathrm{Im}(\mathrm{N}^*)| = q-1 \text{ y } \mathrm{Im}(\mathrm{N}^*) \subset k^* \implies \mathrm{Im}(\mathrm{N}^*) = k^*. \qquad \square$$

Tanto la norma como la traza se comportan bien con respecto a la composición de extensiones de cuerpos. Supongamos que tenemos los cuerpos $K \supset k' \supset k$, con $[K : k'] = s$ y $[k' : k] = l$.

PROPOSICIÓN 2.1.14. — $\mathrm{tr}_{K/k} = \mathrm{tr}_{k'/k} \circ \mathrm{tr}_{K/k'}$, *y* $\mathrm{N}_{K/k} = \mathrm{N}_{k'/k} \circ \mathrm{N}_{K/k'}$.

Demostración. La proposición se basa en

$$\{k \in \mathbb{Z} : 1 \le k \le l \cdot s\} = \{i \cdot s + j : 1 \le i \le s, 1 \le j \le l\},$$

ya que partiendo del automorfismo φ que genera $\mathrm{Gal}(K/k)$, podemos descomponer cualquier otro como

$$\varphi^k = \varphi^{il+j},$$

haciendo

$$\varphi^k : a \mapsto a^{q^k} = a^{q^{il+j}} = \left(a^{q^j}\right)^{q^{il}} = \tilde{\varphi}^i \circ \varphi^j(a),$$

donde $\tilde{\varphi} = \varphi^l$, que es la composición de un automorfismo de $\mathrm{Gal}(k'/k)$ con otro de $\mathrm{Gal}(K/k')$. □

Estos resultados están enunciados en general para cualesquiera tres cuerpos finitos $K \supset k' \supset k$. En nuestro caso, nos será especialmente útil para estudiar el caso $\mathbb{F}_{q^s} \supset \mathbb{F}_q \supset \mathbb{F}_p$ con p primo.

Volvamos ahora al motivo por el que empezamos a estudiar la traza y la norma: la relación entre los caracteres de un cuerpo y los de una extensión suya. Consideremos los cuerpos $K \supset k$, con $[K : k] = s$. Supongamos que tenemos χ un carácter de k, definimos entonces $\chi' = \chi \circ \mathrm{N}_{K/k}$. Como la norma es una función multiplicativa, es evidente que χ' es un carácter de K.

PROPOSICIÓN 2.1.15. — *Con la notación anterior,*

1. $\chi_1 \neq \chi_2 \implies \chi_1' \neq \chi_2'$.
2. $\chi^m = \varepsilon \implies \chi'^m = \varepsilon$.
3. $\chi'(a) = \chi(a)^s$ *para todo* $a \in k$.

Demostración. En primer lugar, nótese que $\mathrm{N}(a) = a^s$ para $a \in k$.

1. Supongamos que $\chi_1 \neq \chi_2$. Si se diera que $\chi_1' = \chi_2'$, como N es sobreyectiva en k^*, se tendría que χ_1 coincide con χ_2 en k^*, y por lo tanto en todo k (porque o bien ambas son cero en el cero si no son iguales a ε, o bien son 1), con lo que llegamos a una contradicción.
2. $\chi'^m(\alpha) = \chi(\mathrm{N}(\alpha))^m = \varepsilon(\mathrm{N}(\alpha)) = 1 \implies \chi'^m = \varepsilon$, porque $\mathrm{N}(\alpha) \in k$.
3. $\chi'(a) = \chi(\mathrm{N}(a)) = \chi(a^s) = \chi(a)^s$. □

Volvamos ahora al teorema que enunciamos al principio del capítulo.

TEOREMA 2.1.16. — *Sea* $a \in \mathbb{F}_q$, *y* $n \mid q-1$. *Entonces, el número de soluciones de la ecuación* $x^n = a$ *es*

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a),$$

donde la suma recorre todos los caracteres de orden divisor de n.

Demostración. En primer lugar, es claro que hay exactamente n sumandos (por el mismo argumento utilizado en el último apartado de la proposición 2.1.13). Si $a = 0$, la única solución es $x = 0$ (porque no puede haber elementos nilpotentes en un cuerpo), y

$$\sum_{\chi^n=\varepsilon} \chi(0) = \varepsilon(0) + \sum_{\chi\neq\varepsilon} \chi(0) = 1 + 0 = 1.$$

Si $a \neq 0$ y existe al menos una solución, es decir, un $b \in \mathbb{F}_q$ tal que $b^n = a$, entonces habrá exactamente n soluciones (hay n números $c_1, \ldots, c_n \in \mathbb{F}_q^*$ de grado divisor de n, luego $(c_i b)^n = a$, y no puede haber más soluciones por el grado del polinomio). Además, $\chi(a) = \chi(b^n) = \chi(b)^n = \varepsilon(b) = 1$, luego

$$\sum_{\chi^n=\varepsilon} \chi(a) = \sum_{\chi^n=\varepsilon} 1 = n.$$

Finalmente, supongamos que $a \neq 0$ y la ecuación no tiene solución. Sean β y λ generadores del grupo multiplicativo y del grupo de caracteres respectivamente, que cumplan $\lambda(\beta^k) = e^{2\pi i k/(q-1)}$, y definimos $\tilde{\chi} = \lambda^{(q-1)/n}$. Si escribimos $a = \beta^l$, con $n \nmid l$ (porque $x^n - a$ no tiene soluciones), vemos que $\tilde{\chi}(a) = \lambda(\beta^l)^{(q-1)/n} = e^{2\pi i l/n} \neq 1$.

Como $\chi^n = \varepsilon$, podemos hacer

$$\tilde{\chi}(a) \sum_{\chi^n=\varepsilon} \chi(a) = \sum_{\chi^n=\varepsilon} \chi(a) \implies \left(\tilde{\chi}(a) - 1\right) \sum_{\chi^n=\varepsilon} \chi(a) = 0 \implies$$
$$\implies \sum_{\chi^n=\varepsilon} \chi(a) = 0. \qquad \square$$

EJEMPLO 2.1.17. — Volvamos al teorema 2.1.2. Supongamos que queremos encontrar la función zeta de la variedad definida por la ecuación $x^n = a$ en $\mathbb{F}_q$, con $n \mid q-1$, hallando para ello el número de puntos de la variedad en una extensión de grado s. Sabemos que

$$N_1 = \sum_{\chi^n=\varepsilon} \chi(a).$$

Por otra parte, el número en una extensión de dimensión s será

$$N_s = \sum_{(\chi^{(s)})^n=\varepsilon} \chi^{(s)}(a),$$

donde los $\chi^{(s)}$ son caracteres en $\mathbb{F}_{q^s}$, porque claramente

$$n \mid q-1 \implies n \mid q^s - 1 = (q-1)(q^{s-1} + \cdots + 1).$$

Cada uno de los χ define un $\chi^{(s)}$ a partir de la definición de χ'. Además, el número de caracteres de un determinado orden es fijo al ser el grupo de caracteres cíclico, con lo

que llegamos a que cada $\chi^{(s)}$ se corresponde con un χ'. Por lo tanto podemos escribir

$$N_s = \sum_{\chi^n=\varepsilon} \chi'(a) = \sum_{\chi^n=\varepsilon} \chi(a)^s,$$

es decir, logramos el objetivo de expresar N_s en función de los caracteres de $\mathbb{F}_q$, y no los de sus extensiones.

Veamos ahora una versión más general del teorema anterior.

TEOREMA 2.1.18. — *Sea $a \in \mathbb{F}_q$, y sea $d = \gcd(n, q-1)$. Tomemos un carácter χ de orden d en $\mathbb{F}_q$ (existe por la proposición 2.1.4). Entonces el número de soluciones de la ecuación $x^n = a$ es*

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

Demostración. Suponemos en primer lugar que $a = 0$. Entonces la única solución será $x = 0$, y en efecto

$$\sum_{i=0}^{d-1} \chi^i(0) = 0 + \cdots + 0 + \varepsilon(0) = 1.$$

Si $a \neq 0$ y la ecuación no tiene solución, debe tenerse que $\chi(a) \neq 1$, y por lo tanto

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

Si tiene al menos una, debe tener exactamente d, entonces $\chi(a) = \chi(x^d) = \chi(x)^d = \varepsilon(x) = 1$, luego

$$\sum_{i=0}^{d-1} \chi^i(a) = \sum_{i=0}^{d-1} 1 = d. \qquad \square$$

2.2. Sumas de Gauss

Acabamos de ver que la teoría de caracteres da información sobre ecuaciones del tipo $x^n - a = 0$, pero para tratar ecuaciones más complejas necesitamos una maquinaria más avanzada: en este caso, las sumas de Gauss y de Jacobi. Empezamos la sección describiendo las sumas de Gauss en cuerpos $\mathbb{F}_p$.

DEFINICIÓN 2.2.1. — Sea χ un carácter en $\mathbb{F}_p$, y $a \in \mathbb{F}_p$. Definimos

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at},$$

con $\zeta = e^{2\pi i/p}$. Decimos que $g_a(\chi)$ es una suma de Gauss en $\mathbb{F}_p$ del carácter χ.

Si queremos generalizar la definición a cualquier cuerpo finito, el problema no estará en χ (en el capítulo anterior vimos que la norma nos permite relacionar caracteres en $\mathbb{F}_p$ con los de $\mathbb{F}_q$) sino en ζ^{at}. Veamos cómo solventar este problema.

DEFINICIÓN 2.2.2. — Sea $\mathbb{F}_q \supset \mathbb{F}_p$. Se define $\psi : \mathbb{F}_q \to \mathbb{C}$ como $\psi(t) = \zeta^{\mathrm{tr}(t)}$.

DEFINICIÓN 2.2.3. — Definimos la suma de Gauss del carácter χ en $\mathbb{F}_q$ como

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

Veamos algunas de las propiedades de g_a:

PROPOSICIÓN 2.2.4. — *Si $a \neq 0$, $g_a(\varepsilon) = 0$ y $g_a(\chi) = \chi(a^{-1})g_1(\chi)$. Si no, $g_0(\varepsilon) = q$ y $g_0(\chi) = 0$.*

Demostración. Los dos asertos sobre ε son triviales, utilizando que la suma de raíces de la unidad es cero al tenerse $e^{2\pi i((p-1)+1)/p} - 1 = 0$.

Por otra parte, $\chi(a)g_a(\chi) = \sum \chi(at)\psi(at) = g_1(\chi)$, luego $g_a(\chi) = \chi(a^{-1})g_1(\chi)$. Finalmente, $g_0(\chi) = \sum \chi(t) = 0$. □

A partir de ahora escribiremos $g(\chi)$ para referirnos a $g_1(\chi)$.

PROPOSICIÓN 2.2.5. — *Si χ no es trivial, entonces $|g(\chi)| = q^{1/2}$.*

Demostración. Vamos a calcular una suma de dos maneras diferentes.

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

$$\sum_{a\in\mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(a(x-y)) =$$

$$= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\chi(y^{-1})\delta_{x,y}q = (q-1)q \implies$$

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

donde utilizamos que $\sum_{a\in\mathbb{F}_q} \psi(a(x-y)) = q\delta_{x,y}$ ([IR90, § 10.3]). □

Esta última proposición tiene una gran importancia: nos dice que podemos siempre hallar el valor absoluto de una suma de Gauss, con independencia del carácter con el que estemos tratando. Nótese también su relación con la hipótesis de Riemann dentro

de las conjeturas de Weil: si expresamos el número de puntos de una variedad en función de sumas de Gauss podemos esperar que los ceros de la función zeta tengan módulo $q^{1/2}$, tal y como podríamos predecir.

2.2.1. Reciprocidad cuadrática

Uno de los problemas más antiguos en la teoría de números algebraica es el de la resolución de la congruencia

$$x^2 \equiv a \mod p,$$

con p primo.

DEFINICIÓN 2.2.6. — Definimos el símbolo de Legendre como

$$(a/p) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ 1 & \text{si } x^2 \equiv a \mod p \text{ tiene solución}, \\ -1 & \text{en otro caso.} \end{cases}$$

Es claro entonces que el número de soluciones de $x^2 \equiv a \mod p$ es $1 + (a/p)$. Esto está en perfecta sintonía con el teorema 2.1.18, puesto que el símbolo de Legendre es de hecho un carácter de orden 2.

Utilizando propiedades de las sumas de Gauss es posible dar una demostración del que el propio Gauss consideraba *Theorema Aureum*: la ley de reciprocidad cuadrática.

TEOREMA 2.2.7 ***(Ley de reciprocidad cuadrática).*** — *Sean p y q primos distintos, y supongamos que $q > 2$. Entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Demostración. Seguiremos en líneas generales la demostración de [Ste09]. Empezamos definiendo $g_a = g_a((\cdot/p))$ y $g = g_1$, las sumas de Gauss del símbolo de Legendre en $\mathbb{F}_p$. Evidentemente, $g_a = (a/p)g$. Escribimos $p^* = (-1)^{(p-1)/2}p$.

LEMA 2.2.8. — $a^{(q-1)/2} = (a/q) \mod q$.

Demostración. Sea b tal que $b^2 = a$, con $b \in \overline{\mathbb{F}}$. Entonces, que a sea un cuadrado en $\mathbb{F}_q$ es equivalente a que $b^{q-1} = 1$, es decir, $a^{(q-1)/2} = 1$. En caso contrario, $b^{q-1} = a^{(q-1)/2} \neq 1$ implica que $a^{(q-1)/2} = -1$ y que a no es un cuadrado en $\mathbb{F}_q$. □

LEMA 2.2.9. — $g^2 = p^*$.

Demostración. De nuevo evaluamos una suma de dos maneras. Por una parte

$$\sum_{a=0}^{p-1} g_t g_{-t} = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \sum_{a=0}^{p-1} (-1)^{(p-1)/2} \left(\frac{a}{p}\right)^2 g^2 = \\ = (-1)^{(p-1)/2}(p-1)g^2.$$

Por la otra,

$$\sum_{a=0}^{p-1} g_t g_{-t} = \sum_{a=0}^{p-1}\sum_{b=0}^{p-1}\sum_{c=0}^{p-1} \left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\psi(a(b-c)) = \\ = \sum_{b=0}^{p-1}\sum_{c=0}^{p-1} \left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\delta_{b,c}p = \\ = p\sum_{b=0}^{p-1}\left(\frac{b}{p}\right)^2 = (p-1)p.$$

Comparando los dos resultados se obtiene el lema. □

Haciendo $(p^*)^{(q-1)/2} = g^{q-1}$ obtenemos

$$g^q \equiv g\left(\frac{p^*}{q}\right) \mod q.$$

Podemos calcular explícitamente la parte izquierda a partir de la definición de g y obtenemos

$$g^q \equiv \left(\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta^{qt} \equiv g_q \mod q.$$

A partir de las dos ecuaciones anteriores llegamos a

$$g_q \equiv \left(\frac{q}{p}\right)g \equiv \left(\frac{p^*}{q}\right)g \mod q \implies \left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \mod q,$$

porque podemos cancelar g a ambos lados al ser coprimo con q. Por el lema anterior,

$$\left(\frac{p^*}{q}\right) \equiv (-1)^{(p-1)(q-1)/4} p^{(q-1)/2} \equiv (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) \mod q,$$

y como los símbolos de Legendre toman valores en $\{0,1,-1\}$ y $q \geq 3$, si son iguales módulo q serán también iguales en $\mathbb{Z}$. Por lo tanto $(q/p) = (p/q)(-1)^{(p-1)(q-1)/4}$, de donde se deduce el teorema. □

2.3. Sumas de Jacobi

EJEMPLO 2.3.1. — Supongamos que queremos hallar el número de soluciones de

$$x^m + y^n = 0$$

en $\mathbb{F}_q$, con $m, n \mid q-1$. Podemos hallar el número fijando a y b con $a+b=0$ y viendo las soluciones a todas las posibilidades de combinaciones de $x^m = 0$ e $y^n = 0$, es decir, haciendo

$$N(x^m + y^n = 0) = \sum_{a+b=0} N(x^m = a) \cdot N(y^n = b).$$

A partir del teorema 2.1.18 sabemos que $N(x^m = a) = \sum_{i=0}^{m-1} \chi^i(a)$, con χ un carácter de orden m. Si tomamos λ de orden n, se tendrá que

$$N(x^m + y^n = 0) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{a+b=0} \chi^i(a)\lambda^j(b).$$

Nos interesa, por lo tanto, hallar el valor de las sumas de la forma

$$\sum_{a+b=0} \chi(a)\lambda(b).$$

Introducimos para ello el concepto de suma de Jacobi (cf. [BEW98]).

DEFINICIÓN 2.3.2. — Sean $\chi_1, \ldots, \chi_k$ caracteres de $\mathbb{F}_q$. Se define la sumas de Jacobi de los caracteres como

$$J(\chi_1, \ldots, \chi_k) = \sum_{c_1+\cdots+c_k=1} \chi(c_1)\cdots\chi(c_k)$$

y

$$J_0(\chi_1, \ldots, \chi_k) = \sum_{c_1+\cdots+c_k=0} \chi(c_1)\cdots\chi(c_k),$$

con los c_i en $\mathbb{F}_q$.

OBSERVACIÓN 2.3.3. — La suma contiene q^{k-1} términos, porque podemos dar a los $k-1$ primeros c_i los valores que queramos y despejar el último.

Para $k=1$, se tiene que $J(\chi) = \chi(1)$. Con $k=2$, $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$. En general,

$$J(\chi_1, \ldots, \chi_k) = J(\chi_{\sigma(1)}, \ldots, \chi_{\sigma(k)})$$

para cualquier permutación $\sigma \in S_k$. Lo mismo se cumple para la suma J_0.

OBSERVACIÓN 2.3.4. — En las sumas de Gauss veíamos que solo era importante considerar g_0 y g, las demás las podíamos transformar en estas. Aquí, de la misma manera,

$$\sum_{\sum c_i = a} \chi_1(c_1)\cdots\chi_k(c_k) = \sum_{\sum c_i = 1} \chi_1(ac_1)\cdots\chi_k(ac_k) = \\ = (\chi_1\cdots\chi_k)(a)J(\chi_1,\cdots,\chi_k).$$

El cálculo de las sumas de Jacobi no es en general trivial, pero sí es sencillo cuando hay caracteres triviales.

PROPOSICIÓN 2.3.5. —

$$J(\chi_1,\ldots,\chi_k) = \begin{cases} q^{k-1} & si\ \forall\ i : \chi_i = \varepsilon, \\ 0 & si\ \exists\ i \neq j : \chi_i = \varepsilon \neq \chi_j. \end{cases}$$

Demostración. Si todos los caracteres son triviales es claro que

$$J(\varepsilon,\ldots,\varepsilon) = \sum_{\sum c_i = 1} 1 = q^{k-1}.$$

Si solo algunos son triviales, podemos suponer simplemente que $\chi_1 \neq \varepsilon$, y $\chi_k = \varepsilon$. Se tiene

$$J(\chi_1,\ldots,\chi_{k-1},\varepsilon) = \sum_{\sum c_i = 1} \chi_1(c_1)\cdots\chi_{k-1}(c_{k-1}) = \\ = q \sum_{c_i \in \mathbb{F}_q} \chi_1(c_1)\cdots\chi_{k-1}(c_{k-1}) = \\ = q \sum_{c_1 \in \mathbb{F}_q} \chi_1(c_1) \cdots \sum_{c_{k-1} \in \mathbb{F}_q} \chi_{k-1}(c_{k-1}) = 0. \qquad \square$$

Como no podía ser de otra manera, existen relaciones entre las dos sumas.

PROPOSICIÓN 2.3.6. — *Sean $\chi_1,\ldots,\chi_k$ caracteres de $\mathbb{F}_q$. Se cumple que*

$$J_0(\chi_1,\ldots,\chi_k) = \begin{cases} q^{k-1} & si\ \forall\ i : \chi_i = \varepsilon, \\ -(q-1)J(\chi_1,\ldots,\chi_k) & si\ \forall\ i : \chi_i \neq \varepsilon,\ y\ \chi_1\cdots\chi_k = \varepsilon, \\ 0 & en\ otro\ caso. \end{cases}$$

Demostración. Calculamos la suma

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_q}\sum_{c_1+\cdots+c_k=a}\chi(c_1)\cdots\chi(c_k) = \\
&\quad = \sum_{c_1+\cdots+c_k=0}\chi(c_1)\cdots\chi(c_k) + \sum_{a\in\mathbb{F}_q^*}\sum_{c_1+\cdots+c_k=a}\chi(c_1)\cdots\chi(c_k) = \\
&\quad = J_0(\chi_1,\ldots,\chi_k) + J(\chi_1,\ldots,\chi_k)\sum_{a\in\mathbb{F}_q^*}\chi_1\cdots\chi_k(a) = \\
&\quad = \begin{cases} J(\chi_1,\ldots,\chi_k) + (q-1)J(\chi_1,\ldots,\chi_k) & \text{si } \chi_1\cdots\chi_k = \varepsilon, \\ J(\chi_1,\ldots,\chi_k) & \text{si no.} \end{cases}
\end{aligned}$$

Y por otra parte,

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_q}\sum_{c_1+\cdots+c_k=a}\chi(c_1)\cdots\chi(c_k) = \sum_{c_1}\chi_1(c_1)\cdots\sum_{c_k}\chi_k(c_k) = \\
&\qquad = \begin{cases} q^k & \text{si } \forall\, i : \chi_i = \varepsilon, \\ 0 & \text{si no.} \end{cases}
\end{aligned}$$

Por lo tanto,

- si todos los caracteres son triviales,

$$\begin{aligned}
J_0(\chi_1,\ldots,\chi_k) + (q-1)J(\chi_1,\ldots,\chi_k) = q^k \implies \\
\implies J_0(\chi_1,\ldots,\chi_k) = q^k + (1-q)q^{k-1} = q^{k-1};
\end{aligned}$$

- si todos son no triviales pero su producto sí,

$$\begin{aligned}
J_0(\chi_1,\ldots,\chi_k) + (q-1)J(\chi_1,\ldots,\chi_k) = 0 \implies \\
\implies J_0(\chi_1,\ldots,\chi_k) = -(q-1)J(\chi_1,\ldots,\chi_k);
\end{aligned}$$

- y si se da cualquier otra circunstancia,

$$J_0(\chi_1,\ldots,\chi_k) = 0.$$

□

Veamos ahora otras propiedades interesantes de las sumas de Jacobi: las *fórmulas de reducción*, que nos permiten pasar de una suma en k caracteres a otra con $k-1$.

PROPOSICIÓN 2.3.7. — *Si $\chi_1,\ldots,\chi_k$ son caracteres no triviales y $\chi_1\cdots\chi_k = \varepsilon$, entonces*

$$J_0(\chi_1,\ldots,\chi_k) = \chi_k(-1)(q-1)J(\chi_1,\ldots,\chi_{k-1}).$$

Demostración. A partir de la definición de J_0,

$$\begin{aligned}
J_0(\chi_1,\dots,\chi_k) &= \sum_{\sum c_i=0} \chi_1(c_1)\cdots\chi_k(c_k) = \\
&= \sum_{c_k\in\mathbb{F}_q^*}\left(\sum_{\sum c_i=-c_k}\chi_1(c_1)\cdots\chi_{k-1}(c_{k-1})\right)\chi_k(c_k) = \\
&= \sum_{c_k\in\mathbb{F}_q^*}(\chi_1\cdots\chi_{k-1})(-c_k)J(\chi_1,\dots,\chi_{k-1})\chi_k(c_k) = \\
&= \chi_k^{-1}(-1)J(\chi_1,\dots,\chi_{k-1})\sum_{c_k\in\mathbb{F}_q^*}(\chi_1\cdots\chi_k)(c_k) = \\
&= \chi_k(-1)J(\chi_1,\dots,\chi_{k-1})(q-1).
\end{aligned}$$

□

COROLARIO 2.3.8. — *En las condiciones anteriores, con $\chi_i\neq\varepsilon$ pero $\chi_1\cdots\chi_k=\varepsilon$,*

$$J(\chi_1,\dots,\chi_k) = -\chi_k(-1)J(\chi_1,\dots,\chi_{k-1}).$$

Demostración. Basta utilizar las dos proposiciones anteriores, y se tendrá que

$$\chi_k(-1)(q-1)J(\chi_1,\dots,\chi_{k-1}) = -(q-1)J(\chi_1,\dots,\chi_k),$$

de donde se deduce el resultado. □

PROPOSICIÓN 2.3.9. — *Si $\chi_1,\dots,\chi_k$ son caracteres no triviales, entonces*

$$J(\chi_1,\dots,\chi_k) = \begin{cases} -qJ(\chi_1,\dots,\chi_{k-1}) & si\ \chi_1\cdots\chi_{k-1}=\varepsilon, \\ J(\chi_1\cdots\chi_{k-1},\chi_k)J(\chi_1,\dots,\chi_{k-1}) & si\ \chi_1\cdots\chi_{k-1}\neq\varepsilon. \end{cases}$$

Demostración. Calculamos

$$\begin{aligned}
J(\chi_1,\dots,\chi_k) &= \sum_{\sum c_i=1}\chi_1(c_1)\cdots\chi_k(c_k) = \\
&= \sum_{c_k=1}\chi_1(c_1)\cdots\chi_k(c_k) + \sum_{c_k\neq 1}\chi_1(c_1)\cdots\chi_k(c_k) = \\
&= J_0(\chi_1,\dots,\chi_{k-1}) + \sum_{c_k\neq 1}\chi_k(c_k)\sum_{\sum c_i=1-c_k}\chi_1(c_1)\cdots\chi_{k-1}(c_{k-1}) = \\
&= J_0(\chi_1,\dots,\chi_{k-1}) + \sum_{c_k\neq 1}(\chi_1\cdots\chi_{k-1})(1-c_k)\chi_k(c_k)J(\chi_1,\dots,\chi_{k-1}) = \\
&= J_0(\chi_1,\dots,\chi_{k-1}) + J(\chi_1,\dots,\chi_{k-1})\big(J(\chi_1\cdots\chi_{k-1},\chi_k) - (\chi_1\cdots\chi_{k-1})(0)\big).
\end{aligned}$$

Separemos ahora los dos casos posibles.

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

$$\begin{aligned} J(\chi_1, \ldots, \chi_k) &= -(q-1)J(\chi_1, \ldots, \chi_{k-1}) + J(\chi_1, \ldots, \chi_{k-1})(0-1) = \\ &= -qJ(\chi_1, \ldots, \chi_{k-1}). \end{aligned}$$

- En caso contrario, $J_0(\chi_1, \ldots, \chi_{k-1}) = 0$, y como $\chi_1 \cdots \chi_{k-1} \neq \varepsilon$ debe tenerse que $(\chi_1 \cdots \chi_{k-1})(0) = 0$, por lo que

$$J(\chi_1, \ldots, \chi_k) = J(\chi_1, \ldots, \chi_{k-1})J(\chi_1 \cdots \chi_{k-1}, \chi_k). \qquad \square$$

Finalmente, veamos la relación entre las sumas de Gauss y las de Jacobi.

TEOREMA 2.3.10. — *Sean $\chi_1, \ldots, \chi_k$ caracteres no triviales. Entonces*

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

Demostración. Lo haremos por inducción en k. El caso $k = 1$ es trivial. Para $k = 2$, tenemos dos casos posibles.

- Si $\chi_1\chi_2 \neq \varepsilon$, entonces

$$\begin{aligned} g(\chi_1)g(\chi_2) &= \sum_{c_1} \sum_{c_2} \chi_1(c_1)\chi_2(c_2)\psi(c_1 + c_2) = \\ &= \sum_{c} \psi(c) \sum_{c_1 + c_2 = c} \chi(c_1)\chi(c_2) = \\ &= \sum_{c_1 + c_2 = 0} \chi_1(c_1)\chi_2(c_2) + \sum_{c \neq 0} \psi(c) \sum_{c_1} \chi_1(c_1)\psi(c - c_1) = \\ &= \chi_2(-1) \sum_{c_1} \chi_1\chi_2(c_1) + \sum_{c \neq 0} \psi(c) \sum_{c_1} \chi_1(c_1 c)\chi_2(c - c_1 c). \end{aligned}$$

  Como $\chi_1\chi_2$ no es trivial, el sumando de la izquierda se anula. Además, en el sumando de la derecha aparece una suma de Jacobi con $\sum c_i = c$, por lo que normalizando llegamos a

$$g(\chi_1)g(\chi_2) = J(\chi_1, \chi_2) \sum_{c \neq 0} \chi_1\chi_2(c)\psi(c) = J(\chi_1, \chi_2)g(\chi_1\chi_2),$$

  de donde llegamos al resultado.

- Si $\chi_1\chi_2 = \varepsilon$, entonces $\chi_2 = \chi_1^{-1}$ y

$$J(\chi_1, \chi_2) = -\chi_1(-1) = -\frac{g(\chi_1)g(\chi_2)}{q}.$$

Veamos ahora qué sucede con $k \geq 3$. Tenemos tres situaciones posibles:

1. Si $\chi_1 \cdots \chi_{k-1} = \varepsilon$, entonces

$$\begin{aligned} J(\chi_1, \ldots, \chi_k) &= -qJ(\chi_1, \ldots, \chi_{k-1}) = -q\left(-\frac{g(\chi_1)\cdots g(\chi_{k-1})}{q}\right) = \\ &= g(\chi_1)\cdots g(\chi_{k-1})\frac{g(\chi_k)}{g(\chi_k)} = \frac{g(\chi_1)\cdots g(\chi_k)}{g(\chi_1\cdots\chi_k)}. \end{aligned}$$

2. Si $\chi_1 \cdots \chi_{k-1} \neq \varepsilon$ pero $\chi_1 \cdots \chi_k = \varepsilon$, entonces $\chi_1 \cdots \chi_{k-1} = \chi_k^{-1}$ y

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

3. Finalmente, si $\chi_1 \cdots \chi_{k-1} \neq \varepsilon \neq \chi_1 \cdots \chi_k$,

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

□

De la proposición anterior deducimos inmediatamente un corolario que nos permite hallar el valor absoluto de una suma de Jacobi.

COROLARIO 2.3.11. — *Si $\chi, \ldots, \chi_k$ son caracteres no triviales, entonces*

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

2.4. La relación de Hasse–Davenport

En la sección 1 vimos que, mediante la traza y la norma, se pueden relacionar los caracteres en un cuerpo finito con los de sus extensiones. Para el caso de sumas de Gauss es posible también enlazar las sumas asociadas a caracteres del cuerpo base y a caracteres de la extensión, mediante la relación de Hasse–Davenport (cf. [DH35] o [IR90, § 11.4]).

Consideremos como base el cuerpo k con p^r elementos, y sea K una extensión suya de grado s.

TEOREMA 2.4.1 ***(Relación de Hasse–Davenport).*** — *Sea χ un carácter de k, y $\chi' = \chi \circ \mathrm{N}_{K/k}$. Entonces*

$$(-g(\chi))^s = -g(\chi').$$

Demostración. Necesitamos en primer lugar una serie de lemas.

LEMA 2.4.2. — *Sea $\alpha \in K$, $k' = k[\alpha]$, y $f(x) \in k[x]$ el polinomio mínimo de α sobre k. Escribimos*

$$f(x) = x^d - c_1 x^{d-1} + \cdots + (-1)^d c_d.$$

Entonces,

1. $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}})$.
2. $\mathrm{tr}_{K/k}(\alpha) = \dfrac{s}{d} c_1$.
3. $\mathrm{N}_{K/k}(\alpha) = c_d^{s/d}$.

Demostración. Para la primera parte, basta aplicar la proposición 1.1.7: como ϕ lleva raíces en raíces, y los α^{q^i} son diferentes, deben ser entonces las raíces de f.

Para los siguientes apartados nótese que, por las relaciones de Cardano-Vieta, $\mathrm{tr}_{k'/k} = c_1$ y $\mathrm{N}_{k'/k} = c_d$. Por otra parte, como $\alpha \in k'$, sabemos que $\mathrm{tr}_{K/k'} = [K : k']\alpha$ y $\mathrm{N}_{K/k'} = \alpha^{[K:k']}$. Y como

$$s = [K : k] = [K : k'][k' : k] \implies [K : k'] = \frac{s}{d},$$

utilizando la proposición 2.1.14, son inmediatos los puntos 2 y 3. □

Ahora, para un polinomio mónico arbitrario

$$f(x) = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n \in k[x],$$

definimos $\lambda(f) = \psi(c_1)\chi(c_n)$.

LEMA 2.4.3. — $\lambda(fg) = \lambda(f)\lambda(g)$.

Demostración. Como $f(x)g(x) = x^{n+m} - (b_1 + c_1)x^{n+m-1} + \cdots + (-1)^{n+m} b_m c_n$, se tiene que

$$\lambda(fg) = \psi(b_1 + c_1)\chi(b_m c_n) = \psi(b_1)\psi(c_1)\chi(b_m)\chi(c_n) = \lambda(f)\lambda(g). \qquad \square$$

Escribimos ahora $\psi'(a) = \psi \circ \mathrm{tr}_{K/k}(a)$.

LEMA 2.4.4. — *Si $\alpha \in K$ y $f \in k[x]$ es su polinomio mínimo, $\lambda(f)^{s/(\deg f)} = \chi'(\alpha)\psi'(\alpha)$.*

Demostración. Utilizando los apartados 2 y 3 del lema 2.4.2, y que $\psi(a)^k = \psi(k \cdot a)$ y $\chi(a)^k = \chi(a^k)$,

$$\begin{aligned} \lambda(f)^{s/d} &= \psi(c_1)^{s/d}\chi(c_d)^{s/d} = \psi\left(\frac{s}{d}c_1\right)\chi(c_d^{s/d}) = \\ &= \psi \circ \mathrm{tr}_{K/k}(\alpha) \cdot \chi \circ \mathrm{N}_{K/k}(\alpha) = \psi'(\alpha)\chi'(\alpha). \end{aligned} \qquad \square$$

LEMA 2.4.5. — $g(\chi') = \sum \deg f \cdot \lambda(f)^{s/(\deg f)}$, *donde sumamos los polinomios mónicos irreducibles tales que* $\deg f \mid s$.

Demostración. Por el lema anterior, los sumandos de la parte derecha son de la forma

$$\begin{aligned} \deg f \cdot \lambda(f)^{s/d} &= \lambda(f)^{s/d} + \cdots + \lambda(f)^{s/d} = \\ &= \chi'(\alpha_1)\psi'(\alpha_1) + \cdots + \chi'(\alpha_{\deg f})\psi'(\alpha_{\deg f}) = \\ &= \sum_{i=1}^{\deg f} \chi'(\alpha_i)\psi'(\alpha_i), \end{aligned}$$

donde los α_i son las diferentes raíces del polinomio. Por la definición de $g(\chi')$ basta demostrar que los polinomios mínimos de todos los elementos de K tienen grado divisor de s, y que todos los polinomios mónicos irreducibles de grado divisor de s tienen todas sus raíces en K.

Para la primera parte, si α tiene a f como polinomio mínimo, entonces $K \supset F[\alpha] \supset k$, y por la transitividad del grado de las extensiones, $s = [K/k'] \cdot \deg f \implies \deg f \mid s$. Para la segunda, si α es raíz de un polinomio mónico irreducible de grado $d = s/l$, entonces

$$\alpha^{q^s} = \alpha^{q^{dl}} = \Big(\big(\alpha^{\underbrace{q^d}}\big)^{\cdots}\Big)^{q^d} = \alpha,$$

l veces

porque $\alpha^{q^d} = \alpha^{|k[\alpha]|} = \alpha$. $\square$

Llamamos ahora $\mathscr{M}$ al conjunto de polinomios mónicos de $k[x]$, y $\mathscr{M}^*$ a los elementos irreducibles de $\mathscr{M}$. Es claro que cada elemento de $\mathscr{M}$ se descompone de manera única como producto de elementos de $\mathscr{M}^*$.

LEMA 2.4.6. — $\displaystyle\sum_{f\in\mathscr{M}} \lambda(f)\,t^{\deg f} = \prod_{f\in\mathscr{M}^*} \left(1-\lambda(f)\,t^{\deg f}\right)^{-1}$

Demostración.

$$\prod_{f\in\mathscr{M}^*} \left(1-\lambda(f)\,t^{\deg f}\right)^{-1} = \prod_{f\in\mathscr{M}^*} \sum_{i=0}^{\infty} \lambda(f)^i\, t^{i\deg f}.$$

Si escribimos $f\in\mathscr{M}$ como $f = p_1^{e_1}\cdot\cdots\cdot p_k^{e_k}$, con los $p_j\in\mathscr{M}^*$ necesariamente distintos, entonces, aplicando el lema 2.4.3,

$$\lambda(f)\,t^{\deg f} = \lambda\left(p_1^{e_1}\cdot\cdots\cdot p_k^{e_k}\right) t^{e_1\deg p_1+\cdots+e_k\deg p_k} = \prod_{j=1}^{k} \lambda(p_j)^{e_j}\, t^{e_j\deg p_j},$$

por lo tanto todos los términos de la suma a la izquierda en el enunciado aparecen en el producto tomando los sumandos correspondientes a su factorización, y todos los productos de la derecha dan lugar claramente a un polinomio de $\mathscr{M}$, de donde se obtiene la igualdad. □

Analicemos ahora la parte izquierda de la igualdad que acabamos de probar. Agrupando los polinomios de $\mathscr{M}$ en función de su grado obtenemos

$$\sum_{f\in\mathscr{M}} \lambda(f)\,t^{\deg f} = \sum_{d=0}^{\infty} \Big(\sum_{\deg f=d} \lambda(f)\Big) t^d.$$

Tomaremos $\lambda(1)=1$, luego el término $d=0$ es 1. Para $d=1$,

$$\sum_{\deg f=1} \lambda(f) = \sum_{a\in K} \lambda(x-a) = \sum_{a\in k} \chi(a)\psi(a) = g(\chi).$$

Si $d>1$, entonces

$$\sum_{\deg f=d} \lambda(f) = \sum_{c_1,\ldots,c_d\in k} \lambda(x^d - c_1x^{d-1} + \cdots + (-1)^s c_d).$$

Como los coeficientes intermedios $c_2,\ldots,c_{d-1}$ son irrelevantes, basta tener en cuenta en el cálculo de λ los coeficientes c_1 y c_d y multiplicarlo por las q^{d-2} elecciones de

otros coeficientes, obteniendo

$$\sum_{\deg f=d} \lambda(f) = q^{d-2} \sum_{c_1,c_d\in k} \chi(c_d)\psi(c_1) = q^{d-2}\Big(\sum_{c_d\in k} \chi(c_d)\Big)\Big(\sum_{c_1\in k} \psi(c_1)\Big) = 0,$$

porque la suma de los $\psi(c_1)$ se anula. Tenemos entonces que

$$\prod_{f\in\mathscr{M}^*} \big(1-\lambda(f)\,t^{\deg f}\big)^{-1} = \sum_{f\in\mathscr{M}} \lambda(f)\,t^{\deg f} = 1+g(\chi)\,t.$$

Tomando la derivada logarítmica llegamos a

$$\frac{\mathrm{d}}{\mathrm{d}t}\log \prod_{f\in\mathscr{M}^*} \big(1-\lambda(f)\,t^{\deg f}\big)^{-1} = \sum_{f\in\mathscr{M}^*} \deg f \frac{\lambda(f)\,t^{\deg f-1}}{1-\lambda(f)\,t^{\deg f}} = \frac{g(\chi)}{1+g(\chi)\,t}.$$

Si multiplicamos por t y volvemos a expandir $u/(1-u)$ como serie geométrica e invirtiendo el orden de suma con $k\cdot\deg f = n$ obtenemos

$$\begin{aligned}\sum_{f\in\mathscr{M}^*} \deg f\Big(\sum_{k=1}^{\infty} \lambda(f)^k t^{k\deg f}\Big) &= \sum_{n=1}^{\infty}\Big(\sum_{\deg f\mid n} \deg f\cdot\lambda(f)^{n/(\deg f)}\Big)\,t^n = \\ &= \sum_{k=1}^{\infty} (-1)^{k+1} g(\chi)^k t^k,\end{aligned}$$

Basta igualar los coeficientes de t^s a cada lado y utilizar el lema 2.4.5 para llegar a

$$\sum_{\deg f\mid s} \deg f\cdot\lambda(f)^{s/(\deg f)} = g(\chi') = (-1)^{s+1} g(\chi)^s \implies -g(\chi') = (-g(\chi))^s. \qquad \square$$

De la misma manera que al principio del capítulo veíamos como relacionar los caracteres en $\mathbb{F}_q$ con los de $\mathbb{F}_{q^s}$, la relación de Hasse–Davenport nos dice que también puede establecerse una analogía similar con sumas de Gauss.

La generalización para sumas de Jacobi es inmediata.

LEMA 2.4.7. — $(\chi_1\cdots\chi_k)' = \chi_1'\cdots\chi_k'$.

Demostración. Para cualquier $a\in K$,

$$\begin{aligned}(\chi_1\cdots\chi_k)'(a) = (\chi_1\cdots\chi_2)(\mathrm{N}(a)) = \chi_1(\mathrm{N}(a))\cdots\chi_k(\mathrm{N}(a)) = \\ = \chi_1'(a)\cdots\chi_k'(a) = (\chi_1'\cdots\chi_k')(a).\end{aligned} \qquad \square$$

Extendiendo el lema anterior a productos arbitrariamente largos llegamos a

PROPOSICIÓN 2.4.8. — *Sean $\chi_1,\dots,\chi_k$ caracteres en $\mathbb{F}_q$, y sean también $\chi'_1,\dots,\chi'_k$ sus equivalentes en $\mathbb{F}_{q^s}$ a través de $\chi'_i = \chi_i \circ \mathrm{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$. Entonces*

$$J(\chi'_1,\dots,\chi'_k) = (-1)^{(s+1)(k+1)} J(\chi_1,\dots,\chi_k)^s.$$

Demostración. Siguiendo la línea del teorema 2.3.10, tenemos dos opciones:

- Si $\chi_1\cdots\chi_k \neq \varepsilon$,

$$\begin{aligned} J(\chi'_1,\dots,\chi'_k) = \frac{g(\chi'_1)\cdots g(\chi'_k)}{g(\chi'_1\cdots\chi'_k)} = \frac{(-1)^{(s+1)k} g(\chi_1)^s\cdots g(\chi_k)^s}{(-1)^{s+1} g(\chi_1\cdots\chi_k)^s} = \\ = (-1)^{(s+1)(k-1)} \left(\frac{g(\chi_1)\cdots g(\chi_k)}{g(\chi_1\cdots\chi_k)}\right)^s = \\ = (-1)^{(s+1)(k+1)} J(\chi_1,\dots,\chi_k)^s. \end{aligned}$$

- Si $\chi_1\cdots\chi_k = \varepsilon$,

$$\begin{aligned} J(\chi'_1,\dots,\chi'_k) = -\frac{g(\chi'_1)\cdots g(\chi'_k)}{q^s} = -\frac{(-1)^{(s+1)k} g(\chi_1)^s\cdots g(\chi_k)^s}{q^s} = \\ = -(-1)^{(s+1)k}(-1)^s \left(-\frac{g(\chi_1)\cdots g(\chi_k)}{q}\right)^s = \\ = (-1)^{(s+1)(k+1)} J(\chi_1,\dots,\chi_k)^s. \end{aligned}$$

□

3

Hipersuperficies diagonales

> *Don't just read it; fight it! Ask your own question, look for your own examples, dicover your own proofs. Is the hypothesis necessary? Is the converse true? What happens in the classical special case? What about the degenerate cases? Where does the proof use the hypothesis?*
>
> — Paul Halmos

CUANDO EN 1949 Weil introducía sus conjeturas sobre variedades proyectivas (cf. [Wei49]), lo hacía sobre el ejemplo de ciertas hipersuperficies de Fermat, mediante el uso de sumas de Gauss y Jacobi. En este capítulo estudiaremos en general las funciones zeta de hipersuperficies diagonales, que contienen a las hipersuperficies de Fermat, sobre la base de las sumas de Jacobi.

3.1. Definición

Fijemos un cuerpo $\mathbb{F}_q$ a lo largo de todo el capítulo.

DEFINICIÓN 3.1.1. — Sean $a_1, \dots, a_n \in \mathbb{F}_q^*$, $a \in \mathbb{F}_q$ coeficientes en el cuerpo, y $k_1, \dots, k_n \in \mathbb{Z}^+$ enteros positivos. Llamamos *hipersuperficie diagonal* a la variedad en $\mathbb{A}^n(\mathbb{F}_q)$ definida por el polinomio

$$f(x_1, \dots, x_n) = a_1 x_1^{k_1} + a_2 x_2^{k_2} + \cdots + a_n x_n^{k_n} - a.$$

La restricción de que los a_i sean no nulos no es realmente necesaria, ya que reduce al caso de la ecuación con una variable menos, pero por simplificar descartamos esta opción.

EJEMPLO 3.1.2. — La variedad definida en el ejemplo anterior, dada por la ecuación $x^m + y^n = 0$ en $\mathbb{F}_q$, es una hipersuperficie diagonal.

Nuestro primer problema surge del hecho de que estamos analizando variedades proyectivas, y el polinomio f no es homogéneo. La solución, por lo tanto, es homogeneizar el polinomio.

DEFINICIÓN 3.1.3. — Sea $P \in k[x_1, \ldots, x_s]$ un polinomio en s variables. Llamamos homogeneinización de P al polinomio

$$P^*(x_0, \ldots, x_s) = x_0^{\deg P} P\left(\frac{x_1}{x_0}, \ldots, \frac{x_s}{x_0}\right).$$

Evidentemente la homogeneinización de un polinomio devuelve un polinomio homogéneo del mismo grado, ya que consiste únicamente en añadir una variable extra a los monomios que no sean de grado máximo para aumentar su grado.

EJEMPLO 3.1.4. — De nuevo con el mismo ejemplo, si $m > n$, la homogeneización de $P(x, y) = x^m + y^n$ es

$$P^*(x, y, z) = x^m + y^n z^{m-n}.$$

Podemos por lo tanto considerar la variedad generada por la homogeneización de f. Si $\deg f = m$, obtenemos

$$\begin{aligned} f^*(x_1, \ldots, x_n) &= x_0^m f(x_1/x_0, \ldots, x_n/x_0) = \\ &= a_1 x_1^{k_1} x_0^{m-k_1} + a_2 x_2^{k_2} x_0^{m-k_2} + \cdots + a_n x_n^{k_n} x_0^{m-k_n} - a x_0^m. \end{aligned}$$

¿Pero cómo podemos enlazar el número de soluciones afines con las proyectivas? Es claro que todas las soluciones afines son también soluciones proyectivas haciendo $x_0 = 1$. Si por el otro lado hacemos $x_0 = 0$, tendremos varias posibilidades. Por una parte tendremos que hallar el número de puntos de una nueva variedad

$$\left\{ a_{i_0} x_{i_0}^{k_{i_0}} + \cdots + a_{i_l} x_{i_l}^{k_{i_l}} = 0 \right\} \subset \mathbb{P}^l,$$

donde aparecen todas las coordenadas que tenían grado máximo en f (supongamos que son de hecho las que van entre 1 y $l+1$). Llamaremos N^H al número de puntos proyectivos de esta variedad – como quedan $n-l-1$ coordenadas libres, cada punto de la nueva variedad genera q^{n-l-1} en la original.

Por otra parte, si las $l+1$ variables de la nueva hipersuperficie se anulan, nos quedan tantos puntos como el proyectivo de dimensión $n-l-2$, al no haber restricciones

sobre las variables que restan (lo único a tener en cuenta es que el origen no es un punto proyectivo). Tendremos entonces que

$$N^{\mathbb{P}} = N^{\mathbb{A}} + q^{n-l-1}N^H + q^{n-l-2} + \cdots + q + 1.$$

Naturalmente, el problema estará entonces en el cálculo de $N^{\mathbb{A}}$ (del cual deberíamos ser capaces de deducir el valor de N^H).

3.2. Contando puntos afines

Busquemos primero hallar el número de soluciones afines de la ecuación

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} + \cdots + a_n x_n^{k_n} = 0,$$

que llamaremos N. Si escribimos $d_i = \gcd(q-1, k_i)$, se tiene que

$$\begin{aligned} N &= \sum_{c_1+\cdots+c_n=0} N(a_1 x_1^{k_1} = c_1) \cdots N(a_n x_n^{k_n} = c_n) = \\ &= \sum_{c_1+\cdots+c_n=0} N(x_1^{k_1} = a_1^{-1} c_1) \cdots N(x_n^{k_n} = a_n^{-1} c_n). \end{aligned}$$

Expresando ahora los términos del producto como suma de caracteres llegamos a

$$\begin{aligned} N &= \sum_{\sum c_i = 0} \left(\sum_{j_1=0}^{d_1-1} \chi_1^{j_1}(a_1^{-1} c_1) \right) \cdots \left(\sum_{j_n=0}^{d_n-1} \chi_n^{j_n}(a_n^{-1} c_n) \right) = \\ &= \sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) \sum_{\sum c_i = 0} \chi_1^{j_1}(c_1) \cdots \chi_n^{j_n}(c_n). \end{aligned}$$

Tenemos a la izquierda una suma de Jacobi, $J_0(\chi_1^{j_1}, \ldots, \chi_n^{j_n})$. Distinguimos tres casos:

- Si $j_1 = \cdots = j_n = 0$, entonces todos los caracteres son triviales, y podemos simplificar la suma a $J_0(\varepsilon, \ldots, \varepsilon) = q^{n-1}$.
- Si solamente algunos de los j_i son triviales, o ninguno es trivial y su producto tampoco, entonces J_0 se anula.
- En otro caso (es decir, caracteres no triviales con producto trivial), tenemos que

$$J_0(\chi_1^{j_1}, \ldots, \chi_n^{j_n}) = -(q-1) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}).$$

Llegamos por tanto a

$$N = q^{n-1} + (q-1) \sum_{\substack{j_1=1 \\ \chi_1^{j_1}\cdots\chi_n^{j_n}=\varepsilon}}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}).$$

Si tomamos $a \neq 0$, el mismo procedimiento nos hace llegar a

$$\begin{aligned} N &= \sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) \sum_{\sum c_i = a} \chi_1^{j_1}(c_1) \cdots \chi_n^{j_n}(c_n) = \\ &= \sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(a_1^{-1}a) \cdots \chi_n^{j_n}(a_n^{-1}a) \sum_{\sum c_i = 1} \chi_1^{j_1}(c_1) \cdots \chi_n^{j_n}(c_n). \end{aligned}$$

Y por las mismas consideraciones de la suma de Jacobi, simplificamos como

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

3.3. *El caso homogéneo*

Consideremos, de manera más específica, el caso

$$a_0 x_0^m + a_1 x_1^m + a_2 x_2^m + \cdots + a_n x_n^m = 0,$$

conocido también como *hipersuperficies de Fermat*. Es fácil ver que, si $N^{\mathbb{A}}$ es el número de puntos afines, y $N^{\mathbb{P}}$ el número de puntos proyectivos, se cumple la relación

$$N^{\mathbb{A}} = 1 + (q-1)N^{\mathbb{P}},$$

porque cada representante en la variedad proyectiva generará $(q-1)$ múltiplos en la afín, y hay que añadir el origen que no es un punto proyectivo.

OBSERVACIÓN 3.3.1. — El $N^{\mathbb{P}}$ que calculamos ahora coincide de hecho con el N^H de la primera sección, haciendo $n = l$.

OBSERVACIÓN 3.3.2. — La función zeta de una variedad depende únicamente del número de puntos, y el número de puntos de la variedad depende únicamente de $\gcd(m, q-1)$. Para simplificar los cálculos, supondremos que $m \mid q-1$, lo que se traduce en que $\gcd(m, q^s - 1)$ no varía en función de s. Además, se tiene entonces que

la hipersuperficie no contiene puntos singulares: como cada derivada parcial será de la forma

$$\frac{\partial f}{\partial x_i} = m a_i x_i^{m-1} = 0 \implies x_i = 0,$$

se tiene que el único candidato a punto singular es $[0 : \cdots : 0]$, que no es un punto proyectivo. En cualquier caso, si se tuviera que $p \mid m$, utilizando que $x \mapsto x^p$ actúa como la identidad en X se tiene que el número de puntos de la variedad es el mismo que tomando como exponentes m/p (y, en general, m/p^r, con el mayor r posible), luego podemos *atajar* el problema.

A partir de los resultados de la sección anterior se tendrá entonces que

$$(q-1)\overline{N} = q^n - 1 + (q-1) \sum_{\substack{j_0=1 \\ \chi_1^{j_1}\cdots\chi_n^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} \chi_1^{j_0}(a_0^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_0^{j_0}, \ldots, \chi_n^{j_n}) \implies$$

$$\overline{N} = 1 + q + \cdots + q^{n-1} + \sum_{\substack{j_0=1 \\ \chi_1^{j_1}\cdots\chi_n^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} \chi_0^{j_0}(a_0^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_0^{j_0}, \ldots, \chi_n^{j_n}).$$

Veamos ahora qué forma tiene la función zeta. En un cuerpo $\mathbb{F}_{q^s} \supset \mathbb{F}_q$, con los mismos cálculos llegamos a

$$\overline{N}_s = 1 + (q^s) + \cdots + (q^s)^{n-1} + \\ + \sum_{\substack{j_0=1 \\ \chi_1^{j_1}\cdots\chi_n^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} (\chi_0')^{j_0}(a_0^{-1}) \cdots (\chi_n')^{j_n}(a_n^{-1}) J((\chi_0')^{j_0}, \ldots, (\chi_n')^{j_n}),$$

y gracias a la relación de Hasse–Davenport simplificamos como

$$\overline{N}_s = 1 + (q^s) + \cdots + (q^s)^{n-1} - \\ - (-1)^{sn} \sum_{\substack{j_0=1 \\ \chi_1^{j_1}\cdots\chi_n^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} \left(\chi_0^{j_0}(a_0^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_0^{j_0}, \ldots, \chi_n^{j_n}) \right)^s = \\ = 1 + q^s + \cdots + (q^{n-1})^s - \\ - \sum_{\substack{j_0=1 \\ \chi_1^{j_1}\cdots\chi_n^{j_n}=\varepsilon}}^{m-1} \cdots \sum_{j_n=1}^{m-1} \left((-1)^n \chi_0^{j_0}(a_0^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_0^{j_0}, \ldots, \chi_n^{j_n}) \right)^s.$$

Llamamos α_i a cada uno de los valores posibles de la suma. Nos podemos entonces preguntar, ¿cuántos sumandos hay, es decir, cuantos valores de α_i habrá?

PROPOSICIÓN 3.3.3. — *El número de sumandos es*

$$S(n,m) = ((m-1)^{n+1} - (-1)^{n+1}(m-1))/m.$$

Demostración. Tenemos que buscar $j_1, \ldots, j_n$ tales que $1 \leq j_i < m$ y

$$j_1 + \cdots + j_n \equiv 0 \mod m.$$

Lo haremos por inducción sobre n. Sea $S(k,m)$ el número de sumandos en la hipersuperficie con variables hasta x_k. Es claro que $S(0,m) = 0$, y $S(1,m) = m-1$. Para un k arbitrario, tenemos que se debe cumplir la congruencia

$$0 \not\equiv -j_k \equiv j_0 + \cdots + j_{k-1} \mod m,$$

porque $j_k \neq 0$, luego el número de opciones es todas las combinaciones de j_0 hasta j_{k-1} menos las que sumen cero, que son de hecho $S(k,m)$. Por lo tanto

$$\begin{aligned} S(k,m) = (m-1)^k - S_{k-1} = (m-1)^k - \frac{(m-1)^k - (-1)^k(m-1)}{m} = \\ = \frac{m(m-1)^k - (m-1)^k - (-1)^{k+1}(m-1)}{m} = \\ = \frac{(m-1)^{k+1} - (-1)^{k+1}(m-1)}{m}. \end{aligned}$$

□

Podemos escribir

$$Z(u) = \frac{R(u)^{(-1)^n}}{(1-u)(1-qu)\cdots(1-q^{n-1}u)}$$

con $R(u) = \prod(1-\alpha_i u)$ un polinomio de grado $S(n,m)$. Veamos que en efecto se verifican las conjeturas de Weil.

1. *Racionalidad:* $Z(u)$ es evidentemente una función racional en u. Como los coeficientes se obtienen a partir de sumas y productos de caracteres, y los valores de los caracteres son necesariamente raíces de la unidad, aprovechando que los enteros algebraicos forman un anillo obtenemos que los coeficientes de $Z(u)$ son en efecto enteros algebraicos.

2. *Ecuación funcional:* tenemos que probar en primer lugar que $z \mapsto q^{n-1}/z$ manda raíces de R en raíces de R. Basta ver que si α_i es raíz, entonces q^{n-1}/α_i también. Como
$$\alpha_i \overline{\alpha_i} = |\alpha_i|^2 = q^{n-1},$$
será suficiente con ver que $\overline{\alpha_i}$ es también una de las raíces.

LEMA 3.3.4. — *Si* $\chi_1 \cdots \chi_k = \varepsilon$, *entonces* $\overline{\chi_1} \cdots \overline{\chi_k} = \varepsilon$.

Demostración. Basta ver que
$$\overline{\chi_1} \cdots \overline{\chi_k}(a) = \overline{\chi_1 \cdots \chi_k}(a) = \overline{(\chi_1 \cdots \chi_k)(a)} = 1$$
para cualquier $a \in \mathbb{F}_q$. □

LEMA 3.3.5. — $J(\overline{\chi_1}, \ldots, \overline{\chi_k}) = \overline{J(\chi_1, \ldots, \chi_k)}$.

Demostración.
$$J(\overline{\chi_1}, \ldots, \overline{\chi_k}) = \sum_{\sum c_i = 1} \overline{\chi_1}(c_1) \cdots \overline{\chi_k}(c_k) = \sum_{\sum c_i = 1} \overline{\chi_1(c_1) \cdots \chi_k(c_k)} =$$
$$= \overline{\sum_{\sum c_i = 1} \chi_1(c_1) \cdots \chi_k(c_k)} = \overline{J(\chi_1, \ldots, \chi_k)}.$$ □

Supongamos que $\alpha_i = (-1)^n \chi_0^{j_0}(a_0^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_0^{j_0}, \ldots, \chi_n^{j_n})$ para unos determinados $j_0, \ldots, j_n$. Entonces
$$\chi_0^{m-j_0} \cdots \chi_n^{m-j_n} = \overline{\chi_0^{j_0}} \cdots \overline{\chi_n^{j_n}} = \varepsilon,$$
por lo que podemos expresar el conjugado de α_i de la forma
$$\overline{\alpha_i} = (-1)^n \chi_0^{m-j_0}(a_0^{-1}) \cdots \chi_n^{m-j_n}(a_n^{-1}) J(\chi_0^{m-j_0}, \ldots, \chi_n^{m-j_n}),$$
o lo que es lo mismo, $\overline{\alpha_i}$ se corresponde con algún otro α_j. Vemos entonces que
$$Z\left(\frac{1}{q^{n-1}u}\right) = \frac{R\left(\frac{1}{q^{n-1}u}\right)^{(-1)^n}}{(1-1/u)\cdots(1-1/(q^{n-1}u))}$$
$$= (-1)^{n-1} q^{(n-1)n/2} u^{n-1} \frac{R\left(\frac{1}{q^{n-1}u}\right)^{(-1)^n}}{(1-u)\cdots(1-q^{n-1}u)}.$$

Analizando mejor el término de R, llegamos a

$$\begin{aligned} R\left(\frac{1}{q^{n-1}u}\right)^{(-1)^n} &= u^{(-1)^{n-1}S(n,m)} \prod_{S(n,m)} \left(u - \frac{\alpha_i}{q^{n-1}}\right) = \\ &= (-1)^{S(n,m)} u^{(-1)^{n-1}S(n,m)} \prod_{S(n,m)} \left(u - \frac{1}{\overline{\alpha_i}}\right) = \\ &= (-1)^{S(n,m)} u^{(-1)^{n-1}S(n,m)} \prod_{S(n,m)} \alpha_i \prod_{S(n,m)} \left(\overline{\alpha_i} u - 1\right) = \\ &= (-1)^{S(n,m)} u^{(-1)^{n-1}S(n,m)} q^{S(n,m)(n-1)/2} R(u), \end{aligned}$$

porque en el producto aparecen cada α_i con su conjugado, y su producto da q^{n-1}. Juntando los resultados obtenemos

$$Z\left(\frac{1}{q^{n-1}u}\right) = \pm q^{(n-1)(n+(-1)^{n-1}S(n,m))/2} u^{n+(-1)^{n-1}S(n,m)} Z(u),$$

que es en efecto la ecuación funcional buscada.

3. Hipótesis de Riemann: tenemos ya escrita Z de la forma pedida. Se cumple que $P_1 = 1 - u$ y $P_{2\dim X} = 1 - q^{\dim X} u$, ya que en este caso se tiene que $\dim X = \dim \mathbb{P}^n(\mathbb{F}_q) - 1 = n - 1$. Con respecto a la hipótesis de Riemann, el denominador cumple lo esperado. Por otra parte, en el numerador,

$$|\alpha_i| = \left|(-1)^n \chi_0^{j_0}(a_0^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_0^{j_0}, \ldots, \chi_n^{j_n})\right| = q^{(n-1)/2},$$

es decir, podemos identificar $R(u)$ como parte de P_{n-1}.

4. *Números de Betti:* los números de Betti de la variedad en $\mathbb{C}^{n+1}$ son

$$B_i = \begin{cases} 0 & \text{si } 0 \le i \le 2(n-1),\ i \ne n-1 \text{ impar}, \\ 1 & \text{si } 0 \le i \le 2(n-1),\ i \ne n-1 \text{ par}, \\ S(n,m) & \text{si } i = n-1 \text{ impar}, \\ 1 + S(n,m) & \text{si } i = n-1 \text{ par}, \end{cases}$$

(véase [GY95, § 2]), lo cual se corresponde con los grados de los polinomios de $Z(u)$. Se tiene entonces que $E = n + (-1)^{n-1} S_n$.

Por lo tanto, tal y como cabía esperar, la función zeta de la hipersuperficie dada por

$$a_0 x_0^m + a_1 x_1^m + a_2 x_2^m + \cdots + a_n x_n^m = 0.$$

cumple en efecto todas las conjeturas de Weil.

OBSERVACIÓN 3.3.6. — Dado el polinomio

$$f(x_1,\dots,x_n) = a_1x_1^m + a_2x_2^m + \cdots + a_nx_n^m - a,$$

con $a \neq 0$, se tiene que su homogeinización, que define una hipersuperficie en $\mathbb{P}^n(\mathbb{F}_q)$, es de la forma que acabamos de analizar. Si, por el contrario, tuviéramos

$$f(x_1,\dots,x_n) = a_1x_1^m + a_2x_2^m + \cdots + a_nx_n^m,$$

se tiene entonces que f define una hipersuperficie en $\mathbb{P}^{n-1}(\mathbb{F}_q)$. En ambos casos, la función zeta de la hipersuperficie correspondiente cumple todas las conjeturas de Weil.

OBSERVACIÓN 3.3.7. — La fórmula obtenida para los números de Betti B_i es válida para cualquier hipersuperficie lisa en $\mathbb{C}^{n+1}$ de grado m.

3.4. *El caso general*

Supongamos ahora que partimos de una variedad no homogénea, es decir, que debemos homogeneizar un polinomio para llegar a $X = \mathcal{V}(f^*)$. Uno podría pensar, visto lo anterior, que el generalizar supone una gran complicación, pero lo cierto es que vamos a ver cómo la mayoría de hipersuperficies con las que trabajaremos son de hecho singulares, luego no podemos esperar de ellas que cumplan las conjeturas de Weil.

Veamos una serie de lemas para hallar qué hipersuperficies son singulares.

LEMA 3.4.1. — *Sea X la variedad proyectiva generada por un determinado polinomio $f^* \in k[x_0,\dots,x_n]$. Si*

$$\text{máx}\, k_i - \text{mín}\, k_i \geq 2,$$

entonces X contiene al menos un punto singular.

Demostración. Nos basta suponer que $k_1 - k_n \geq 2$. Tenemos entonces que f^* se escribe como

$$f^* = a_1x_1^{k_1} + a_2x_2^{k_2}x_0^{k_1-k_2} + \cdots + a_nx_n^{k_n}x_0^{k_1-k_n} - ax_0^{k_1},$$

y por lo tanto $P = [0 : \cdots : 0 : 1] \in X$. Además, calculando las derivadas parciales

llegamos a

$$\begin{aligned}
\frac{\partial f^*}{\partial x_0}(P) &= x_0\left(\cdots + (a_n(k_1-k_n))x_n^{k_n}x_0^{k_1-k_n-2} - k_1 a x_0^{k_1-2}\right) = 0\\
\frac{\partial f^*}{\partial x_1}(P) &= k_1 a_1 x_1^{k_1-1} = 0\\
&\vdots\\
\frac{\partial f^*}{\partial x_{n-1}}(P) &= k_{n-1}a_{n-1}x_{n-1}^{k_{n-1}-1}x_0^{k_1-k_{n-1}} = 0\\
\frac{\partial f^*}{\partial x_n}(P) &= k_n a_n x_n^{k_n-1}x_0^{k_1-k_n} = 0.
\end{aligned}$$

es decir, P es un punto singular de X. □

Nótese que, en el lema, utilizamos la hipótesis para poder sacar factor común y escribir $x_0^{k_1-k_n-2}$ asegurándonos de que el grado de x_0 no es negativo. El caso $k_n = k_1 - 1$ no será, por desgracia, tan sencillo.

LEMA 3.4.2. — *En las condiciones anteriores, si $k = k_{n-1} = k_n = k_1 - 1$, X es singular.*

Demostración. Tomaremos el punto $P = [0 : \cdots : 0 : y_{n-1} : y_n]$, aunque no diremos de momento quiénes son y_{n-1} e y_n. El mismo cálculo que hicimos antes nos confirma que P está en X, y que al menos las derivadas con respecto a $x_1, \ldots, x_n$ se anulan. Veamos qué ocurre con respecto a x_0. Operando obtenemos

$$\frac{\partial f^*}{\partial x_0} = a_{n-1}x_{n-1}^k + a_n x_n^k,$$

que es una hipersuperficie de Fermat. Por la sección anterior, sabemos que la ecuación debe tener soluciones (si no su función zeta sería constante e igual a 1, algo que sabemos que no sucede). Por lo tanto, tomando y_{n-1}, y_n soluciones de la ecuación (quizás en $\mathbb{F}_{q^s}$, pero no nos importaría), obtenemos que $P \in X$ es un punto singular. □

Hemos eliminado ya bastantes casos, reduciendo el estudio a la ecuación

$$a_1 x_1^k + \cdots + a_{n-1}x_{n-1}^k + a_n x_n^{k-1} = 0.$$

Todavía podemos afinar algo más.

LEMA 3.4.3. — *Para una variedad X definida por la ecuación anterior, se tiene que X será singular si $k \geq 3$.*

Demostración. Basta ver que, si tuviéramos $k \geq 3$, el punto $P = [1 : 0 : \cdots : 0] \in X$ es singular. Las única derivada para las cuales esto no es trivial son x_n (que se cumple porque $k-1 \geq 2$, luego x_n aparece en el término de la derivada) y x_0 (que solamente aparece en el último término, luego se anula por se $x_n = 0$). □

Nótese que el caso $k = 1$ se reduce a una hipersuperficie de Fermat al homogeneizar, caso que ya hemos visto. Por lo tanto, nos queda un último obstáculo por superar.

PROPOSICIÓN 3.4.4. — *Si X viene dada por la ecuación*

$$a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 + a_n x_n,$$

definida en $\mathbb{F}_q$ con $2 \nmid q$, entonces X define una variedad no singular.

Demostración. Supongamos que $P = [y_0, y_1, \ldots, y_n] \in X$ es un punto singular. Entonces, obligando a que se anulen las derivadas, obtenemos $y_1, \ldots, y_{n-1} = 0$. En el último término, la derivada con respecto a x_0 obliga a tener $x_n = 0$, mientras que la derivada con respecto a x_n fuerza que $x_0 = 0$. Por lo tanto $P = [0 : \cdots : 0]$, que no es un punto de X por no ser un punto proyectivo. □

Toca entonces calcular el número de puntos de la variedad

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_{n-1} x_{n-1}^2 + a_n x_n x_0.$$

Si $x_0 = 1$, la variedad resultante será isomorfa a $\mathbb{A}^{n-1}$, haciendo

$$x_n = \frac{1}{a_n}\left(a_1 x_1^2 + a_2 x_2^2 + \cdots + a_{n-1} x_{n-1}^2\right) \quad \forall (x_1, \ldots, x_{n-1}) \in \mathbb{A}^{n-1}.$$

Si $x_0 = 0$, nos queda la hipersuperficie de Fermat

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_{n-1} x_{n-1}^2,$$

que tiene $q^{n-3} + \cdots + q + 1 + \sum \alpha_i$ soluciones (donde la suma recorre los productos de caracteres y sumas de Jacobi correspondientes), por las q opciones disponibles para x_n, más el punto $[0 : \cdots : 0 : 1]$. Entonces

$$\begin{aligned} N_s &= \left(q^{n-1}\right)^s + q^s\left(\left(q^{n-3}\right)^s + \cdots + q^s + 1 + \sum \alpha_i^s\right) + 1 = \\ &= \left(q^{n-1}\right)^s + \left(q^{n-2}\right)^s + \cdots + q^s + 1 + \sum (q\alpha_i)^s = \\ &= \left(q^{n-1}\right)^s + \left(q^{n-2}\right)^s + \cdots + q^s + 1 + \sum \beta_i^s, \end{aligned}$$

con $|\beta_i|^2 = q^{n-1}$. Se tiene entonces que la función zeta será

$$Z(u) = \frac{\left(\prod(1-\beta_i u)\right)^{(-1)^n}}{(1-u)(1-qu)\cdots(1-q^{n-1}u)}.$$

La comprobación de que la función $Z(u)$ satisface las conjeturas de Weil es completamente análoga a lo visto en la sección anterior: los denominadores *se comportan bien*, y el numerador también por cumplir por los cálculos realizados para hipersuperficies de Fermat (con la excepción de que hemos pasado de α_i a β_i, que corrige el módulo para que se adecúe a lo esperado y se cumpla que $|\beta_i| = q^{(n-1)/2}$).

Aunque hemos visto que la mayoría de hipersuperficies diagonales no son lisas (y por lo tanto no tienen por qué cumplir las conjeturas de Weil), merece la pena observar que sus funciones zeta (que están perfectamente definidas a pesar de ser variedades singulares) cumplen propiedades similares a las esperadas. Recordemos que en la primera sección vimos que para la hipersuperficie X dada por

$$f(x_1,\ldots,x_n) = a_1x_1^{k_1} + a_2x_2^{k_2} + \cdots + a_nx_n^{k_n} - a.$$

podemos escribir

$$N_s^{\mathbb{P}} = N_s^{\mathbb{A}} + \left(q^{n-l-1}\right)^s N_s^H + \left(q^{n-l-2}\right)^s + \cdots + q^s + 1.$$

Si, recordando que H es una hipersuperficie de Fermat, escribimos su número de puntos como

$$N_s^H = q^{(l-1)s} + q^{(l-2)s} + \cdots + 1 + \sum \alpha_i^s,$$

simplificaremos la ecuación anterior llegando a

$$\begin{aligned} N_s^{\mathbb{P}} &= N_s^{\mathbb{A}} + \left(q^{n-l-1}\right)^s \left(q^{(l-1)s} + q^{(l-2)s} + \cdots + 1 + \sum \alpha_i^s\right) + \left(q^{n-l-2}\right)^s + \cdots + q^s + 1 = \\ &= N_s^{\mathbb{A}} + \sum \left(q^{n-l-1}\alpha_i\right)^s + \left(q^{n-2}\right)^s + \cdots + q^s + 1 = \\ &= N_s^{\mathbb{A}} + \sum \beta_i^s + \left(q^{n-2}\right)^s + \cdots + q^s + 1. \end{aligned}$$

Definimos $R_H(u) = \prod 1 - \beta_i u$, y llegamos a

$$Z(X,u) = \frac{R_H(u)^{(-1)^n}}{(1-u)(1-qu)\cdots(1-q^{n-2}u)} Z(X^{\mathbb{A}},u).$$

Falta entonces calcular $N_s^{\mathbb{A}}$. Si $a \neq 0$ (es decir, si el polinomio tiene término indepen-

diente), habíamos calculado que

$$N^{\mathbb{A}} = q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}a) \cdots \chi_n^{j_n}(a_n^{-1}a) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}),$$

por lo que mediante la relación de Hasse–Davenport obtenemos

$$N_s^{\mathbb{A}} = \left(q^{n-1}\right)^s + \sum \left((-1)^{n+1}\gamma_i\right)^s,$$

y por lo tanto

$$Z(X^{\mathbb{A}}, u) = \frac{R_{\mathbb{A}}(u)^{(-1)^{n+1}}}{1 - q^{n-1}u},$$

con $R_{\mathbb{A}}(u) = \prod\left(1 - \gamma_i u\right)$, de donde deducimos que

$$Z(X, u) = \frac{R_{\mathbb{A}}(u)^{(-1)^{n+1}} R_H(u)^{(-1)^n}}{(1-u)(1-qu)\cdots(1-q^{n-1}u)}.$$

Podemos destacar ciertas propiedades de la función zeta:

- Se trata de una función racional con coeficientes enteros.
- Podemos escribirla como productos y cocientes de polinomios alternados, tales que $P_0 = 1 - u$ y $P_{\dim X} = 1 - q^{n-1}u$.
- Además, todas las raíces de los polinomios cumplen que su módulo es una potencia entera de $q^{1/2}$. Para las de los denominadores de manera trivial, y para el numerador,

$$|\beta_i| = |q^{n-l-1}\alpha_i| = q^{n-l-1}|\alpha_i| = (q^{1/2})^{2n-l-3},$$

$$|\gamma_i| = \begin{cases} (q^{1/2})^{n-1} & \text{para el producto de } \chi_i \text{ no trivial,} \\ (q^{1/2})^{n-2} & \text{en otro caso.} \end{cases}$$

El estudio de $a \neq 0$ es idéntico, cambiando únicamente $R_{\mathbb{A}}$, por lo que lo omitimos señalando simplemente que cumple las mismas propiedades.

A partir de todo el estudio anterior, podemos ver que a pesar de tratarse de superficies con puntos singulares sus funciones zeta presentan ciertas características similares a las predichas por Weil. Finalmente, enunciamos el siguiente

TEOREMA 3.4.5. — *La función zeta de una hipersuperficie diagonal no singular cualquiera satisface las conjeturas de Weil.*

4

Curvas

Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.

— Godfrey Harold Hardy

PASAMOS AHORA DE hipersuperficies en espacios de dimensión arbitraria a curvas proyectivas, que para nosotros serán variedades proyectivas de dimensión 1 sobre $\mathbb{P}^2$. Para calcular la función zeta utilizaremos la teoría de divisores, así como ciertas herramientas más avanzadas de geometría algebraica.

Con el objetivo de tratar el tema de la manera más introductoria posible, evitaremos ser generales y trataremos únicamente con las herramientas que nos resulten imprescindibles, sin preocuparnos por los casos más generales (por ejemplo, divisores generados por subvariedades de codimensión 1).

4.1. Divisores y formas tangentes

Al comienzo del trabajo, antes incluso de introducir la función zeta, mencionábamos los *divisores primos* $\mathfrak{D}$, que definíamos simplemente como la *órbita* de un punto bajo la acción del automorfismo de Frobenius φ. Veamos ahora una noción algo más general.

DEFINICIÓN 4.1.1. — Sea X una curva. Un *divisor* D sobre X es una suma formal

$$D = \sum_{P \in X} D(P)P,$$

donde únicamente para una cantidad finita de puntos se tiene que $D(P) \neq 0$. Se define el grado del divisor D como

$$\deg D = \sum_{P \in X} D(P).$$

En cierto sentido, pasamos de considerar un conjunto de puntos a una suma formal de los puntos (con coeficientes enteros). Esto presenta algunas ventajas.

OBSERVACIÓN 4.1.2. — Podemos ver el conjunto de divisores sobre una curva como el $\mathbb{Z}$–módulo libre generado por los puntos $P \in X$. Podemos por lo tanto considerar

$$D_1 + D_2 = \sum_{P \in X} \big(D_1(P) + D_2(P)\big) P.$$

También podemos definir

$$D \geq 0 \Longleftrightarrow D(P) \geq 0 \quad \forall P \in X,$$

y de manera natural considerar las comparaciones entre divisores

$$D_1 \geq D_2 \Longleftrightarrow D_1 - D_2 \geq 0.$$

Veamos entonces qué es el análogo de $\mathfrak{D}$ en nuestra nueva definición de divisores.

DEFINICIÓN 4.1.3. — Decimos que un divisor es primo si

$$D = P_1 + P_2 + \cdots + P_d,$$

y se tiene que $\varphi(P_i) = P_{i+1}$.

A partir de la definición anterior, es evidente que el grado de un divisor primo es $\deg D = d$. Si $\mathscr{P}$ es el conjunto de todos los divisores primos, definimos $\mathrm{Div}(X) = \mathbb{Z}^{\mathscr{P}}$, el $\mathbb{Z}$-módulo libre generado por los divisores primos, y de manera análoga $\mathrm{Div}(X)^+ = \mathbb{N}^{\mathscr{P}}$ (esto ya no es un módulo, porque $\mathbb{N}$ solamente es un semianillo).

Podemos ahora asociar determinados divisores a las funciones sobre la curva.

DEFINICIÓN 4.1.4. — Dada una función racional $f \in K(X)$, definimos su divisor como

$$\mathrm{div}(f) = \sum_{P \in X} v_P(f) P,$$

donde $v_P(f)$ denota el residuo de f en P. En divisor de la forma $D = \mathrm{div}(f)$ se denomina *divisor principal*, o en algunas ocasiones *divisor de polos y ceros de* f.

Es decir, pasamos de una suma *arbitraria* de puntos a una basada en funciones de $K(X)$. Los divisores de funciones racionales nos permiten establecer la siguiente relación de equivalencia.

DEFINICIÓN 4.1.5. — Sean $D_1, D_2 \in \mathrm{Div}(X)$. Decimos que

$$D_1 \sim D_2 \iff D_1 - D_2 = \mathrm{div}(f), \quad f \in K(X).$$

Llamamos *grupo de Picard* de X al cociente

$$\mathrm{Div}(X)/_{\sim} = \mathrm{Pic}(X).$$

Es decir, las clases de equivalencia que forman el grupo de Picard son los conjuntos de divisores tales que la diferencia de dos de ellos es un divisor principal. Sigamos ahora el estudio de los divisores con el comportamiento del grado de un divisor.

PROPOSICIÓN 4.1.6. — *La aplicación* $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ *es sobreyectiva.*

Demostración. Supondremos como cierta la desigualdad de Hasse–Weil (que aparece como el teorema 4.4.1), para cuya demostración ni esta proposición ni nada que derivemos de ella es necesario. La desigualdad dice que

$$N_r = q^r + \mathcal{O}\left(q^{r/2}\right).$$

En concreto, para valores grandes de r sabemos que siempre podremos hallar solución. Sean p_1, p_2 primos suficientemente grandes. Como $N_{p_1} \geq 1$, se tendrá que existe al menos un divisor D_1 de grado p_1 (y por el mismo argumento, D_2 de grado p_2). Pero entonces

$$\alpha p_1 + \beta p_2 = 1 \implies \deg D = \deg\left(\alpha D_1 + \beta D_2\right) = 1 \implies \deg(nD) = n \quad \forall n \in \mathbb{Z}. \qquad \square$$

Llamamos ahora $\mathrm{Div}^n(X) = \deg^{-1}(n)$, y lo mismo para $\mathrm{Div}^n(X)^+$ y $\mathrm{Pic}^n(X)$. Tenemos el siguiente

COROLARIO 4.1.7. — $\mathrm{Div}(X)/_{\mathrm{Div}^0(X)} \cong \mathbb{Z}$.

Demostración. Basta aplicar el primer teorema de isomorfía. $\square$

La consecuencia inmediata de este corolario es el siguiente

COROLARIO 4.1.8. — *El isomorfismo anterior induce* $\mathrm{Div}^n(X) \cong \mathrm{Div}^0(X)$, *y este a su vez induce* $\mathrm{Pic}^n(X) \cong \mathrm{Pic}^0(X)$.

Demostración. Tomamos $D_n \in \mathrm{Div}^n(X)$ arbitrario pero fijo. Entonces, la aplicación

$$\begin{array}{rccc} \mu & : & \mathrm{Div}^n(X) & \longrightarrow & \mathrm{Div}^0(X) \\ & & D & \longmapsto & D - D_n \end{array}$$

es de manera trivial un isomorfismo, y al cocientar por los divisores principales induce un isomorfismo $\mu' : \mathrm{Pic}^n(X) \to \mathrm{Pic}^0(X)$. □

Cambiamos ahora de tema e introducimos muy brevemente el concepto de 1-formas.

DEFINICIÓN 4.1.9. — Una 1-forma racional ω es un elemento de $\Omega^1_{K(X)}$, es decir, una función de la forma $f\,\mathrm{d}g$ con $f, g \in K(X)$.

Uno podría pensar en ω como una función que sale del espacio tangente. Es posible demostrar que, localmente (en el entorno de un punto P), cualquier forma se puede escribirse como $g\,\mathrm{d}t$, y en esas condiciones definimos $v_P(\omega) = v_P(g)$.

DEFINICIÓN 4.1.10. — Definimos el divisor de ω como

$$\sum_{P \in X} v_P(\omega) P.$$

Si $\omega \neq 0$, se dice que es un *divisor canónico*.

Ha llegado la hora de ver para qué sirve toda la maquinaria que hemos estado desarrollando.

DEFINICIÓN 4.1.11. — Para cualquier $D \in \mathrm{Div}(X)$, definimos los espacios vectoriales

$$H_0(X, D) = \left\{ f \in K(X)^\times \mid \mathrm{div}(f) + D \geq 0 \right\} \cup \{0\},$$
$$H_0(X, \Omega^1(-D)) = \left\{ 0 \neq \omega \in \Omega^1_{K(X)} \mid \mathrm{div}(\omega) - D \geq 0 \right\} \cup \{0\}.$$

Definimos el *género* de X como $g = \dim H_0(X, \Omega^1)$.

TEOREMA 4.1.12 *(Riemann–Roch).* — *Se tiene que*

$$\dim H^0(X, D) + \dim H^0(X, \Omega^1(-D)) = \deg(D) + 1 - g.$$

No demostraremos este teorema, aunque veremos una consecuencia importante.

LEMA 4.1.13. — *Sea $\omega_0 \neq 0$ una forma de tal manera que* $\mathrm{div}(\omega_0)$ *sea un divisor canónico. Entonces la aplicación $f \mapsto f \cdot \omega_0$ establece un isomorfismo*

$$H^0(X, \Omega^1(-D)) \to H^0(X, \mathrm{div}(\omega_0) - D).$$

Demostración.

$$\begin{aligned} f\cdot\omega_0 \in H^0(X,\Omega^1(-D)) &\iff \operatorname{div}(f\cdot\omega_0)-D\geq 0\\ &\iff \operatorname{div}(f)+\big(\operatorname{div}(\omega_0)-D\big)\geq 0\\ &\iff f\in H^0(X,\operatorname{div}(\omega_0)-D). \end{aligned}$$ □

DEFINICIÓN 4.1.14. — Llamamos $h_0(D)$ a la dimensión de $H^0(X,D)$ como espacio vectorial.

COROLARIO 4.1.15. — $h_0(D)+h_0(\operatorname{div}(\omega_0)-D)=\deg(D)+1-g$.

Hemos acumulado ya suficientes herramientas como para ser capaces de tratar la función zeta de X. Nótese que el tratamiento que hemos hecho de la teoría de divisores ha sido muy elemental: un estudio más general pasa por considerar *variedades de codimensión 1* en lugar de puntos, y estudiar la dualidad de Serre para demostrar el teorema de Riemann–Roch tal y como lo hemos enunciado aquí (con H^0 y no con H^1). Algunas referencias para un análisis más exhaustivo son [Sha94, § II] o [Mil09, § 12].

4.2. Función zeta de una curva

Veamos ahora cómo expresar la función zeta de una curva en función de sus divisores, de manera similar a cómo trabajamos en la proposición 1.2.7. Comenzamos definiendo

$$d_n=\left|\operatorname{Div}^n(X)^+\right|.$$

PROPOSICIÓN 4.2.1. — $Z(u)=\displaystyle\sum_{n=0}^{\infty} d_n u^n$.

Demostración. Recordemos que, por lo que vimos en el capítulo 1, podemos escribir

$$Z(u)=\prod_{D\in P}\frac{1}{1-t^{\deg D}}.$$

Trabajando ahora con los divisores de X llegamos a

$$\prod_{D\in P}\frac{1}{1-t^{\deg D}}=\prod_{D\in P}\sum_{n=0}^{\infty}t^{n\deg P}=\sum_{D\in\operatorname{Div}(X)^+}t^{\deg D}=\sum_{n=0}^{\infty}d_n t^n.$$ □

Vemos por tanto que el cálculo de Z se reduce al de d_n. Veremos cómo hallar este número a través de una serie de lemas.

LEMA 4.2.2. — *Sea $D \in \mathrm{Div}(X)^+$, y $\overline{D}$ su proyección en $\mathrm{Pic}(X)$. Entonces podemos establecer una biyección*

$$\begin{array}{rccc} \psi & : & H_0(X,D)\setminus\{0\}/\mathbb{F}_q^\times & \longrightarrow & \pi^{-1}(\overline{D}) \\ & & \overline{f} & \longmapsto & \mathrm{div}(f)+D. \end{array}$$

Demostración. En primer lugar, vemos que

$$f \in H_0(X,D) \implies \mathrm{div}(f)+D \geq 0 \implies \psi(\overline{f}) \in \mathrm{Div}(X)^+,$$

y la aplicación está bien definida. Para probar la inyectividad, observamos que dados $0 \neq f_1, f_2 \in H_0(X,D)$, se tiene que

$$\mathrm{div}(f_1)+D = \mathrm{div}(f_2)+D \implies \mathrm{div}(f_1) = \mathrm{div}(f_2) \implies f_1 = \lambda f_2,\ \lambda \in \mathbb{F}_q^\times \implies \overline{f_1} = \overline{f_2}.$$

Y para probar la sobreyectividad, es evidente que

$$D' \in \pi^{-1}(\overline{D}) \implies \overline{D} = \overline{D'} \implies D' = D + \mathrm{div}(f) \implies D' = \psi(\overline{f}). \qquad \square$$

Este lema tiene una serie de consecuencias inmediatas.

LEMA 4.2.3. — $d_n = \displaystyle\sum_{D \in \mathrm{Pic}^n(X)} \frac{q^{h_0(D)}-1}{q-1}$.

Demostración. Basta reescribir d_n como

$$\left|\mathrm{Div}^n(X)^+\right| = \sum_{D\in\mathrm{Pic}^n(X)} \left|\pi^{-1}(D)\right| = \sum_{D\in\mathrm{Pic}^n(X)} \frac{\left|H_0(X,D)\setminus\{0\}\right|}{q-1} = \sum_{D\in\mathrm{Pic}^n(X)} \frac{q^{h_0(D)}-1}{q-1}. \qquad \square$$

LEMA 4.2.4. — *Para $n \geq 2g-1$ se tiene que $d_n = \left|\mathrm{Pic}^0(X)\right| \frac{q^{n-(g-1)}-1}{q-1}$.*

Demostración. Aplicando el resultado anterior, teniendo en cuenta que $h_0(D) = n+1-g$ si $\deg D = n \geq 2g-2$, y recordando que $\mathrm{Pic}^n(X) \cong \mathrm{Pic}^0(X)$, obtenemos inmediatamente el resultado. $\square$

Estamos ya en condiciones de calcular $Z(u)$.

TEOREMA 4.2.5. — *Podemos escribir la función zeta de X como*

$$Z(u) = \frac{P_1(u)}{(1-u)(1-qu)}, \quad P_1 \in \mathbb{Z}[u]_{\leq 2g}.$$

Demostración. Utilizamos que

$$Z(u) = \sum_{n=0}^{\infty} d_n u^n,$$

y dividimos la suma para d_n menor o mayor que $2g-2$, con lo que resulta

$$Z(u) = \sum_{n=0}^{2g-2} d_n u^n + \left|\mathrm{Pic}^0(X)\right| \sum_{n=2g-1}^{\infty} \frac{q^{n-(g-1)}-1}{q-1} u^n.$$

Si analizamos la segunda suma, vemos que

$$\begin{aligned}
\sum_{n=2g-1}^{\infty} \frac{q^{n-(g-1)}-1}{q-1} u^n &= \frac{u^{2g-1}}{q-1} \sum_{n=2g-1}^{\infty} \left(q^{n-(g-1)}-1\right) u^{n-2g+1} = \\
&= \frac{u^{2g-1}}{q-1} \left(\sum_{n=1}^{\infty} \left(q^{n+g}-1\right) u^n \right) = \\
&= \frac{u^{2g-1}}{q-1} \left(\sum_{n=1}^{\infty} q^g (qu)^n - \sum_{n=1}^{\infty} u^n \right) = \\
&= \frac{u^{2g-1}}{q-1} \left(\frac{q^g}{1-qu} - \frac{1}{1-u} \right) = \frac{f(u)}{(1-u)(1-qu)},
\end{aligned}$$

con f un polinomio que cumple $\deg f \leq 2g$. Entonces podemos escribir

$$Z(u) = \frac{(1-u)(1-qu)\sum_{n=0}^{2g-2} d_n u^n + \left|\mathrm{Pic}^0(X)\right| f(u)}{(1-u)(1-qu)} = \frac{P_1(u)}{(1-u)(1-qu)},$$

tal y como queríamos, con un $P_1(u)$ que cumple $\deg P_1 \leq 2g$. □

4.3. *La ecuación funcional*

Probemos ahora que la función zeta de una curva satisface la ecuación funcional prevista por las conjeturas de Weil. Para ello, explotaremos el hecho de que la dualidad de Serre establece una simetría $n \mapsto 2(g-1)-n$ útil para manipular d_n, y utilizaremos el teorema de Riemann–Roch para hallar una relación explícita entre $Z(u)$ y $Z(1/qu)$.

A partir de ahora viviremos en el $\mathbb{Q}[u,u^{-1}]$–módulo

$$M=\left\{\sum_{n\in\mathbb{Z}} a_n u^n \mid a_n\in\mathbb{Q}\right\},$$

que uno podría entender como las *series de Laurent* con coeficientes racionales. Necesitaremos en primer lugar un lema.

LEMA 4.3.1. — *Para todo* $0\le n\le 2g$ *se tiene que*

$$d_n - q^{n-(g-1)}d_{2(g-1)-n}=\frac{q^{n-(g-1)}-1}{q-1}\left|\mathrm{Pic}^0(X)\right|.$$

Demostración. Tomemos un divisor $D\in\mathrm{Div}^n(X)$ cualquiera. Se tiene que

$$\left|\pi^{-1}(\overline{D})\right|=\frac{q^{h_0(D)}-1}{q-1},$$

y consideremos el divisor $\mathrm{div}(\omega)-D$. Para un ω arbitrario pero fijo esta involución induce una biyección

$$\mathrm{Div}^n(X)\longrightarrow \mathrm{Div}^{2(g-1)-n}(X),$$

que a su vez establece otra

$$\mathrm{Pic}^n(X)\longrightarrow \mathrm{Pic}^{2(g-1)-n}(X).$$

Además, por la dualidad de Serre podemos relacionar D y $\mathrm{div}(\omega)-D$ como

$$h^0(D)-h^0(\mathrm{div}(\omega)-D)=n+1-g,$$

por lo que operando calculamos

$$\left|\pi^{-1}(\overline{\mathrm{div}(\omega)-D})\right|=\frac{q^{h_0(\mathrm{div}(\omega)-D)}-1}{q-1}=\frac{q^{h_0(D)-(n+1-g)}-1}{q-1}.$$

Entonces se tendrá que

$$\left|\pi^{-1}(\overline{D})\right|-q^{n+1-g}\left|\pi^{-1}(\overline{\mathrm{div}(\omega)-D})\right|=\frac{q^{n-(g-1)}-1}{q-1}.$$

Si sumamos para todas las clases, tenemos que

$$\sum_{\overline{D}\in\mathrm{Pic}^n(X)}\left|\pi^{-1}(\overline{D})\right|=\left|\{D\in\mathrm{Div}^n(X)^+\}\right|=d_n,$$

y como sumar en $\mathrm{Pic}^n(X)$ es equivalente a sumar en $\mathrm{Pic}^{2(g-1)-n}$, se cumple que

$$d_n - q^{n-(g-1)} d_{2(g-1)-n} = \frac{q^{n-(g-1)}-1}{q-1} \left|\mathrm{Pic}^0(X)\right|. \qquad \square$$

Estamos ya en condiciones de demostrar la ecuación funcional que cumple $Z(u)$.

TEOREMA 4.3.2. — *La función zeta satisface la ecuación funcional, es decir,*

$$Z\left(1/qu\right) = \pm q^{E/2} u^E Z(u),$$

recordando que una curva tiene dimensión 1.

Demostración. Tomando que $d_n = 0$ para $n < 0$, se tiene que $Z(u) \in M$ y

$$Z\left(\frac{1}{qu}\right) = \sum_{n\in\mathbb{Z}} d_n \left(qu\right)^{-n} = \sum_{n\in\mathbb{Z}} d_{-n} q^n u^n.$$

Deducimos entonces que

$$q^{g-1}u^{2g-2} Z\left(\frac{1}{qu}\right) = q^{g-1}u^{2g-2} \sum_{n\in\mathbb{Z}} d_{-n} q^n u^n = \sum_{n\in\mathbb{Z}} d_{2g-2-n} q^{n+1-g} u^n,$$

y restándolo a $Z(u)$ llegamos a

$$Z(u) - q^{g-1}u^{2g-2} Z(u) = \sum_{n\in\mathbb{Z}} \left(d_n - d_{2g-2-n} q^{n+1-g}\right) u^n,$$

que podemos escribir por el lema anterior como

$$Z(u) - q^{g-1}u^{2g-2} Z\left(\frac{1}{qu}\right) = \frac{\left|\mathrm{Pic}^0(X)\right|}{q-1} \sum_{n\in\mathbb{Z}} \left(q^{n+1-g} - 1\right) u^n.$$

Analicemos la suma del término a la derecha. Expandimos y multiplicamos por $1 - qu$, y llegamos a que en el primer sumando se tiene

$$(1-qu)\left(q^{1-g}\right) \sum_{n\in\mathbb{Z}} q^n u^n = \left(q^{1-g}\right)\left(\sum_{n\in\mathbb{Z}} q^n u^n - \sum_{n\in\mathbb{Z}} q^{n+1} u^{n+1}\right) = 0.$$

Si multiplicamos también por $1 - u$ quedará en el segundo sumando

$$(1-u) \sum_{n\in\mathbb{Z}} u^n = \sum_{n\in\mathbb{Z}} u^n - \sum_{n\in\mathbb{Z}} u^{n+1} = 0.$$

Entonces se tiene que

$$(1-u)(1-qu)\left(Z(u)-q^{g-1}u^{2g-2}Z\left(\frac{1}{qu}\right)\right)=0.$$

Reescribimos lo anterior para llegar a

$$(1-u)(1-qu)Z(u)=(1-u)(1-qu)\left(q^{g-1}u^{2g-2}Z\left(\frac{1}{qu}\right)\right).$$

Una primera observación es darse cuenta de que la parte izquierda está en $\mathbb{Q}[[u]]$, mientras que la derecha está en $u^{2g-2}\mathbb{Q}[[u^{-1}]]$, luego debe cumplirse que estén ambas mitades en $\mathbb{Q}[u]_{\leq 2g}$. Por lo tanto

$$Z(u)=\frac{P_1(u)}{(1-u)(1-qu)},$$

con $P_1(u)$ un polinomio de coeficientes racionales de grado a lo más $2g$. Como nuestro objetivo es relacionar $Z(u)$ y $Z(1/qu)$, y sabemos que en 1 y en q^{-1} tiene polos ambas, podemos asumir que $u\neq 1,q^{-1}$, y obtenemos

$$Z\left(\frac{1}{qu}\right)=q^{1-g}u^{2-2g}Z(u),$$

tal y como cabría esperar si recordemos que la característica de Euler de una curva de género g es exactamente $E=2-2g$. □

Veamos ahora algunas consecuencias particulares de la ecuación funcional, que nos permitirán arrojar luz sobre la función zeta, que escribimos como

$$Z(u)=\frac{P_1(u)}{(1-u)(1-qu)}=\frac{P_1(u)}{P_0(u)P_2(u)}$$

COROLARIO 4.3.3. — $\deg P_1=2g$.

Demostración. Particularizando la ecuación funcional para $P(u)$ es fácil ver que

$$P_1(u)=q^g u^{2g}P_1\left(\frac{1}{qu}\right),$$

y como sabemos que P es un polinomio de grado menor o igual que $2g$, podemos

escribirlo como

$$P_1(u) = p_0 + p_1 u + \cdots + p_{2g} u^{2g},$$

y sustituyendo en la ecuación funcional llegamos a

$$p_{2g-n} = q^{g-n} p_n.$$

Como sabemos que $Z(0) = 1$ (basta ver la definición con la exponencial) se tendrá que $P_1(0) = p_0 = 1$, y por lo tanto $p_{2g} = q^g$, es decir, P_1 es un polinomio de grado exactamente $2g$. □

COROLARIO 4.3.4. — *Los grados de los $P_i(u)$ en la función zeta coinciden con los números de Betti B_i de la curva.*

Demostración. En efecto, los números de Betti asociados a una curva proyectiva son $B_0 = 1$, $B_1 = 2g$, $B_2 = 1$, de donde se deduce también que $E = 2 - 2g$. □

Recopilando todos los resultados probados en esta sección, tenemos que la función zeta de una curva cumple *casi todas* las conjeturas de Weil. Nos falta únicamente una: el análogo de la hipótesis de Riemann.

4.4. Desigualdad de Hasse–Weil

Para hallar la norma de las raíces de $P_1(u)$, veremos primero la desigualdad de Hasse–Weil, que acota N_s, y la utilizaremos para *controlar* el valor de la suma de los inversos de las raíces. Hecho esto, explotaremos la simetría de la ecuación funcional para ver que podemos *encajar* las raíces en una serie de desigualdades para llegar al valor deseado. Escribiremos

$$P_i(u) = \prod_{i=1}^{2g} (1 - \alpha_i u).$$

TEOREMA 4.4.1. — *Dada una curva proyectiva no singular X de género g definida sobre un cuerpo $\mathbb{F}_q$, se tiene que*

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

El orden para probar esta desigualdad suele ser el contrario (partiendo de la hipótesis de Riemann), aunque es posible demostrarla considerando únicamente el número de intersección de varias subvariedades de la diagonal $\Delta = X \times X$ (cf. [EHT16, § 14]). Por simplicidad (y por compacidad) omitimos la demostración.

OBSERVACIÓN 4.4.2. — Esta desigualdad es la generalización de la *desigualdad de Hasse* para curvas elípticas (con género $g = 1$), conjeturada por Artin en [Art24] y demostrada por Hasse (cf. [Has36]) en 1936. Lejos de ser un mero lema auxiliar, la desigualdad de Hasse–Weil juega un papel importante en áreas tan poco esperadas como la teoría de códigos (cf. [Mor91]).

Nótese que, si trabajamos en un cuerpo base $\mathbb{F}_q$, para hallar N_s basta aplicar el teorema directamente en $\mathbb{F}_{q^s}$ para obtener

$$\left|N_s - (q+1)\right| \leq 2gq^{s/2}.$$

TEOREMA 4.4.3. — *En las condiciones anteriores, se tiene que* $|\alpha_i| = q^{1/2}$.

Demostración. Por la expresión de la función zeta sabemos que

$$N_s = q^s + 1 - \sum_{i=1}^{2g} \alpha_i^s.$$

Entonces se tiene que

$$\left|N_s - (q^s+1)\right| = \left|\sum_{i=1}^{2g} \alpha_i^s\right| \leq 2gq^{s/2}.$$

Definimos

$$\xi(t) = \sum_{i=1}^{2g}\sum_{m=1}^{\infty} \alpha_i^m t^m = \sum_{i=1}^{2g} \frac{\alpha_i t}{1-\alpha_i t}.$$

Resulta entonces que $\xi(t)$ tiene polos en cada uno de los $1/\alpha_i$, pero por otra parte

$$\left|\xi(t)\right| \leq \sum_{m=1}^{\infty} \left|\sum_{i=1}^{2g} \alpha_i^s\right| |t|^m \leq 2g \sum_{m=1}^{\infty} \left(q^{1/2}|t|\right)^m = \frac{2gq^{1/2}|t|}{1-q^{1/2}|t|}$$

para $|t| < q^{-1/2}$. Entonces, como vemos que ξ no tiene ceros en $B(0, q^{-1/2})$, deducimos

$$\frac{1}{|\alpha_i|} \geq q^{-1/2} \implies |\alpha_i| \leq q^{1/2}.$$

Si se cumple la ecuación funcional, debe tenerse que

$$Z\left(\frac{1}{qu}\right) = q^{1-g}u^{2-2g}Z(u) \implies 0 = Z(\alpha_i^{-1}) = Z\left(\frac{\alpha_i}{q}\right).$$

Para que la función Z a la derecha se anule, necesariamente sucederá que α_i/q será otra raíz, es decir,

$$\frac{\alpha_i}{q} = \alpha_j^{-1} \implies \alpha_i\alpha_j = q \implies q^{1/2} \leq \frac{q}{|\alpha_j|} = |\alpha_i| \leq q^{1/2} \implies |\alpha_i| = q^{1/2}. \qquad \square$$

OBSERVACIÓN 4.4.4. — En esta sección hemos partido de la desigualdad de Hasse–Weil para calcular la norma de los α_i, pero es posible recorrer el camino en la otra dirección, haciendo

$$\left|N-(q+1)\right| = \left|\alpha_1+\cdots+\alpha_{2g}\right| \leq |\alpha_1|+\cdots+|\alpha_{2g}| = 2gq^{1/2}.$$

Hemos visto entonces cómo describir la función zeta en función de los divisores de la curva (que no es más que otra manera de contar puntos). Juntando los resultados de las secciones anteriores, podemos finalizar el capítulo con el siguiente teorema, cuya demostración acabamos de terminar.

TEOREMA 4.4.5. — *La función zeta de una curva proyectiva sin puntos singulares satisface las conjeturas de Weil.*

Bibliografía

[Apo76] Tom M. APOSTOL. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[Art24] Emil ARTIN. «Quadratische Körper im Gebiete der höheren Kongruenzen. II». En: *Math. Z.* 19.1 (1924) (vid. págs. 6, 72).

[BEW98] Bruce C. BERNDT, Ronald J. EVANS y Kenneth S. WILLIAMS. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998 (vid. pág. 36).

[BS89] Joel V. BRAWLEY y George E. SCHNIBBEN. *Infinite algebraic extensions of finite fields*. Vol. 95. Contemporary Mathematics. American Mathematical Society, Providence, RI, 1989.

[Del74] Pierre DELIGNE. «La conjecture de Weil. I». En: *Inst. Hautes Études Sci. Publ. Math.* 43 (1974) (vid. pág. 8).

[DF04] David S. DUMMIT y Richard M. FOOTE. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[DH35] Harold DAVENPORT y Helmut HASSE. «Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen». En: *J. Reine Angew. Math.* 172 (1935) (vid. pág. 42).

[Dir99] Peter G. L. DIRICHLET. *Lectures on number theory*. Vol. 16. History of Mathematics. American Mathematical Society, Providence, RI; London Mathematical Society, London, 1999 (vid. pág. 5).

[Dwo60] Bernard DWORK. «On the rationality of the zeta function of an algebraic variety». En: *Amer. J. Math.* 82 (1960) (vid. pág. 7).

[EHT16] Bas EDIXHOVEN, David HOLMES y Lenny TAELMAN. *Algebraic Goemoetry*. Ago. de 2016 (vid. pág. 71).

[Gro88] Alexander GROTHENDIECK. *Récoltes et Semailles. Réflexions et témoignage sur un passé de mathématicien*. 1988 (vid. pág. 8).

[Gro95] Alexander GROTHENDIECK. «Formule de Lefschetz et rationalité des fonctions *L*». En: *Séminaire Bourbaki, Vol. 9*. Soc. Math. France, Paris, 1995 (vid. pág. 8).

[GY95] Fernando Q. GOUVÊA y Noriko YUI. *Arithmetic of diagonal hypersurfaces over finite fields*. Vol. 209. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1995 (vid. pág. 54).

[Har77] Robin HARTSHORNE. *Algebraic geometry*. Vol. 52. Graduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1977 (vid. págs. 8, 11).

[Has36] Helmut HASSE. «Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung». En: *J. Reine Angew. Math.* 175 (1936) (vid. pág. 72).

[IK04] Henryk IWANIEC y Emmanuel KOWALSKI. *Analytic number theory*. Vol. 53. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 2004.

[IR90] Kenneth IRELAND y Michael ROSEN. *A classical introduction to modern number theory*. Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York, 1990 (vid. págs. 33, 42).

[Kob84] Neal KOBLITZ. *p-adic numbers, p-adic analysis, and zeta-functions*. Second. Vol. 58. Graduate Texts in Mathematics. Springer-Verlag, New York, 1984 (vid. pág. 7).

[Mil09] James S. MILNE. *Algebraic Number Theory (v3.02)*. 2009 (vid. pág. 65).

[Mil16] James S. MILNE. «The Riemann hypothesis over finite fields from Weil to the present day». En: *The legacy of Bernhard Riemann after one hundred and fifty years. Vol. II*. Vol. 35. Adv. Lect. Math. (ALM). Int. Press, Somerville, MA, 2016 (vid. pág. 8).

[Mor91] Carlos MORENO. *Algebraic curves over finite fields*. Vol. 97. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1991 (vid. pág. 72).

[Neu99] Jürgen NEUKIRCH. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999 (vid. págs. 5, 18).

[Oor14] Frans OORT. «The Weil conjectures». En: *Nieuw Arch. Wiskd. (5)* 15.3 (2014) (vid. pág. 8).

[Roq02] Peter ROQUETTE. «The Riemann hypothesis in characteristic p, its origin and development. Part 1. The formation of the zeta-functions of Artin and of F. K. Schmidt». En: *Mitt. Math. Ges. Hamburg* 21.2 (2002) (vid. pág. 6).

[Roq04] Peter ROQUETTE. «The Riemann hypothesis in characteristic p, its origin and development. Part 2. The first steps by Davenport and Hasse». En: *Mitt. Math. Ges. Hamburg* 23.2 (2004) (vid. pág. 6).

[Roq06] Peter ROQUETTE. «The Riemann hypothesis in characteristic p, its origin and development. Part 3. The elliptic case». En: *Mitt. Math. Ges. Hamburg* 25 (2006) (vid. pág. 6).

[Roq12] Peter ROQUETTE. «The Riemann hypothesis in characteristic p, its origin and development. Part 4. Davenport-Hasse fields». En: *Mitt. Math. Ges. Hamburg* 32 (2012) (vid. pág. 6).

[Sha94] Igor R. SHAFAREVICH. *Basic algebraic geometry. 1*. Second. Springer-Verlag, Berlin, 1994 (vid. pág. 65).

[Ste09] William STEIN. *Elementary number theory: primes, congruences, and secrets*. Undergraduate Texts in Mathematics. Springer, New York, 2009 (vid. pág. 34).

[Wei48] André WEIL. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948 (vid. pág. 6).

[Wei49] André WEIL. «Numbers of solutions of equations in finite fields». En: *Bull. Amer. Math. Soc.* 55 (1949) (vid. págs. 7, 15, 47).