UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

LAS CONJETURAS DE WEIL PARA HIPERSUPERFICIES DE FERMAT

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A

JESUS ROGELIO PEREZ BUENDIA

DIRECTOR DE TESIS: DR. ENRIQUE JAVIER ELIZONDO HUERTA

2000

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis:
Las Conjeturas de Weil para Hipersuperficies de Fermat

realizado por Jesús Rogelio Pérez Buendía

con número de cuenta 9219476-4 , pasante de la carrera de Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio

Atentamente

Director de Tesis Propietario	Dr. Enrique Javier Elizondo Huerta.	Javier Elizondo
Propietario	Dr. Herbert Kanarek Blando.	H Kanarek
Propietario	Dr. Rodolfo San Agustín Chi.	
Suplente	Dr. Héctor Sánchez Morgado.	F Sánchez M
Suplente	M. en C. Emigdio Martínez Ojeda.	

Consejo Departamental de Matemáticas

Mat. Cesar Guevara Bravo.

Las Conjeturas de Weil para Hipersupeficies de Fermat

Jesús Rogelio Pérez Buendía
UNAM

A Yuki:

Porque esta tesis representa
alcanzar la meta del camino
que juntos recorrimos.

Porque indudablemente
aquí hay mucho de ti.

A mi madre, hermanos y hermanas:

Porque *simplemente* sin ustedes
esto no hubiera sido posible.

AGRADECIMIENTOS

Quiero agradecer a todas las personas que de alguna manera han influido para que este trabajo se vea ahora concluido. Para comenzar quiero agradecer al Dr. Enrique Javier Elizondo Huerta por todo el apoyo que me ha brindado, gracias al cual he podido lograr varias de mis metas tales como ingresar al instituto, iniciar el Posgrado, conseguir becas, asistir a eventos de matemáticas, el presente trabajo, entre otros. También le agradezco a los cuates Mito, Paulino, Andrés y a mi hermano Eduardo que sin tenerlo que hacer, se tomaron la molestia de darle una buena revisada a mi tesis gracias a la cual corregí varios de mis errores ortográficos, matemáticos y de LaTeX. Así mismo, le agradezco a los sinodales Dr. Javier Elizondo Huerta, Dr. Herbert Kanarek Blando, Dr. Rodolfo San Agustín Chi, Dr. Héctor Sánchez Morgado y M en C. Emigdio Martínez Ojeda por sus correcciones y ambles sugerencias para mejorar la tesis. A Yuki Navarro quien innegablemente me ayudó en todo lo que pudo (y hasta en lo que no pudo), porque durante el tiempo de la carrera su compañia fue, sin dudarlo, una de las mejores cosas que me han pasado en la vida. A los cuates del cubículo, del instituto y de la facultad por soportar mis chistes malos y por crear un ambiente agradable de estudio (y también de no estudio). Al Instituto de Matemáticas por permitirme un espacio en él (y todo lo que esto conlleva) para poder realizar mis estudios de la mejor manera. A la Facultad de Ciencias por enseñarme mucho de lo poco que sé. A Javier, a Herbert y a todas las personas que me ayudaron a darle buen término a los problemas burocráticos en los que me vi envuelto recientemente.

Especialmente agradezco a mi madre Ana María Buendía y a mis hermanos: Ana Rosa, Fidel, Sergio, Leticia, Lilia, Arturo, Raúl, Javier, Estela, Ana María, Rubén, Ana Luz y Eduardo; porque cada uno, y de manera distinta, ha influido no sólo en este trabajo, sino en en todas mis actividades. Porque han sido más que hermanos. Porque esta tesis también es suya.

Índice General

INTRODUCCIÓN

The story on "Weil Conjectures" is a marvelous example of mathematical imagination and one of the most striking instances exhibiting the fundamental unity of mathematics. The essential ideas which led to their proof are due to six men: E. Artin, F. K. Schmidt, H, Hasse, A. Weil, Grothendieck, and P. Deligne, over a period of fifty years (1923 - 1973).

J.A. Dieudonné

Estudiar el número de soluciones de una ecuación polinomial $p(x_1, x_2, \ldots, x_n) = 0$ es un problema que ha mantenido a muchos matemáticos ocupados desde hace ya mucho tiempo. Como muestra tenemos los trabajos de Gauss acerca del número de soluciones de las congruencias

$$ax^3 - by^3 \equiv 1 \,(\mathrm{mod}\, p) \qquad ax^4 - by^4 \equiv 1 \,(\mathrm{mod}\, p)$$
$$y^2 \equiv ax^4 - b \,(\mathrm{mod}\, p)$$

donde p es un número primo. O bien, su famoso teorema de la reciprocidad cuadrática que nos sirve para determinar cuándo la ecuación $x^2 - a = 0$ tiene solución en un campo finito con p elementos. También podemos considerar el teorema de Fermat que asegura que el número de soluciones enteras no triviales de la ecuación $x^n + y^n = z^n$ es cero para n mayor o igual a tres.

Encontrar el número de soluciones a ecuaciones polinomiales ha dado pie al desarrollo de nuevas teorías y al establecimiento de puentes entre algunas áreas de la matemática tales como Teoría de Números y la Geometría Algebraica. Un ejemplo de esto son las "Conjeturas de Weil".

En 1949 A. Weil publicó un artículo titulado "Number of solutions of equations in finite fields" [Wei49] en el que da unas conjeturas acerca de una serie de potencias asociada a una variedad algebraica definida sobre un campo finito. Dichas conjeturas relacionan propiedades topológicas de las variedades con propiedades aritméticas y algebraicas de éstas. Entre otras cosas motiva el estudio de nuevas teorías de cohomología.

Después del trabajo de varios matemáticos, en 1960 Dwork publicó un artículo titulado "On the Rationality of the Zeta Function of an Algebraic Variety" [Dwo60] en el que muestra, con toda generalidad, que la función zeta es una función racional y que cumple con la ecuación funcional. Sin embargo, deja pendiente la demostración de que se cumple el análogo con la hipótesis de Riemann. Una de las cosas que hacen que esta analogía sea de gran importancia es que nos permite dar una estimación para los números N_s de puntos $\mathbb{F}_{q^s}$-racionales de la variedad. No fue sino hasta 1973 que P. Deligne, utilizando matemáticas del más alto nivel, demuestra la validez de la analogía con la hipótesis de Riemann dando por concluida la demostración completa de las llamadas "Conjeturas de Weil".

El objetivo central de esta tesis es presentar la validez de las conjeturas de Weil para el caso que Weil estudió en su artículo, es decir, para las hipersuperficies de Fermat que son las dadas por polinomios de la forma

$$a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l$$

con $a_0a_1\cdots a_n \neq 0$. Es importante mencionar que, en su artículo, Weil sólo muestra que la función zeta asociada a las hipersuperficies de Fermat es racional, dejando pendiente la verificación de las otras conjeturas. Así, gran parte de mi trabajo consistió en construir una demostración "original" del resto de las conjeturas, aunque apegada a las ideas expuestas por Weil, Ireland y Lornecini [Wei49], [IR90] y [Lor96]. También quiero dejar claro que en el presente trabajo no me involucro con la demostración general de las conjeturas ni con el punto de vista cohomológico de éstas, ya que escapa de los objetivos del presente. Cabe mencionar que se cambió la notación presentada en [Wei49] a la que actualmente se utiliza.[1]

Concretamente, en el primer capítulo presento un repaso general de la teoría de campos finitos haciendo hincapié en su existencia y unicidad. Así por ejemplo, muestro que para cada entero positivo n y cada número primo p existe un campo finito con p elementos; también,

[1] Se usa la notación presentada en los libros [AP95], [Ste94] y [IR90] entre otros. En estos libros también se puede encontrar más información al respecto.

que dado un campo finito $\mathbb{F}_q$ con q elementos, toda extensión algebraica es de Galois, que si es finita de grado m, entonces es isomorfa al campo de descomposición del polinomio $x^{q^m} - x$ sobre $\mathbb{F}_q$. En este capítulo estudio, también, a los grupos de Galois definidos sobre campos finitos, muestro que el grupo de Galois de una extensión finita es un grupo cíclico generado por el automorfismo de Frobenius de la extensión. Finalmente estudio cómo son los espacios afín y proyectivo, incluyendo algunas de sus subvariedades algebraicas, y doy una caracterización de sus puntos racionales como puntos fijos de potencias del q-automorfismo de Frobenius.

En el segundo capítulo presento la herramienta clave de la tesis: estudio la estructura de los grupos de caracteres definidos sobre un campo finito, así como un tipo especial de sumas exponenciales, llamadas sumas de Gauss. Estas sumas nos permiten dar una fórmula para los números N_s que nos posibilita mostrar la validez de las conjeturas para hipersuperficies de Fermat, gracias a la relación de Hasse-Davenport que cumplen las sumas de Gauss. Así, en este capítulo el objetivo central es demostrar la relación de Hasse-Davenport.

Para el tercer capítulo, me adentro ya en el estudio del número de soluciones en un campo finito que tienen las ecuaciones polinomiales de la forma

$$a_0 x_0^{l_0} + a_1 x_1^{l_1} + \cdots + a_n x_n^{l_n} = 0, \tag{0.1}$$

por lo que comienzo estudiando un caso bien conocido de la teoría de los números clásica: la ecuación $x^l - a = 0$, que para $l = 2$ no es otra cosa que estudiar cuándo a es residuo cuadrático. De hecho, se da una fórmula para calcular el número de soluciones de $x^l - a = 0$ en un campo finito, que resulta análoga a la fórmula $1 + (a/p)$ del número de soluciones de la congruencia $x^2 \equiv a (\mathrm{mod}\, p)$, con p primo y (a/p) el símbolo de Jacobi estudiada en la teoría de la reciprocidad cuadrática. Lo anterior, aunado al estudio de las sumas de Jacobi y a la relación de éstas con las sumas de Gauss, es fundamental en la obtención de una fórmula para el caso general; es decir, el número de soluciones de la ecuación 0.1. En realidad, en este capítulo no se estudia, tal cual, el número de soluciones de las ecuaciones de la forma 0.1, sino, su equivalente geométrico, es decir, se estudia el número de puntos racionales dados por las hipersuperficies determinadas por los polinomios de la forma $a_0 x_0^{l_0} + a_1 x_1^{l_1} + \cdots + a_n x_n^{l_n}$.

Finalmente, en el último capítulo establezco la validez de las conjeturas de Weil para hipersuperficies de Fermat, para lo que defino una clase especial de conjuntos y morfismos entre éstos: los conjuntos Δ_s y los morfismos derivación. Mismos que están relacionados con

caracteres y sumas de Gauss. Además estudio la acción de subgrupos del grupo de Galois de la cerradura algebraica del campo finito sobe los Δ_s y presento una serie de resultados que nos llevan a la demostración de las conjeturas.

Capítulo 1

CAMPOS FINITOS

En este capítulo estudiaremos las propiedades generales de los campos finitos, mostraremos que existen campos finitos diferentes de los $\mathbb{Z}/p\mathbb{Z}$ y demostraremos que todos los campos finitos son extensiones de Galois de cualquiera de sus subcampos, en particular de su campo primo. También estudiaremos a los grupos de Galois asociados a estos campos así como a los espacios afín y proyectivo definidos sobre éstos.

Los resultados presentados en este capítulo serán de gran utilidad durante todo este trabajo y se presupone que el lector esta familiarizado con la teoría general de campos.

1.1 Propiedades generales de campos finitos

En esta primera sección estudiaremos el número de elementos de un campo finito $\mathbb{F}$ y algunas propiedades estructurales. Mostraremos que este número es necesariamente de la forma p^n con p primo y $n \in \mathbb{N}$. También mostraremos que $\mathbb{F}^*$ es un grupo cíclico, lo que nos ayudará a mostrar que cualquier extensión finita de $\mathbb{F}$ es simple. Finalmente veremos que todo campo finito es perfecto.

Denotaremos por $\mathbb{F}_p$ al campo $\mathbb{Z}/p\mathbb{Z}$ con p primo. Si $\mathbb{K}$ es un subcampo de $\mathbb{F}_p$, entonces $\mathbb{K}$ debe contener al 0 y al 1 de $\mathbb{F}_p$, y por lo tanto debe contener a todo $\mathbb{F}_p$; es decir, $\mathbb{Z}/p\mathbb{Z}$ no tiene subcampos propios. Esto nos lleva a la siguiente definición

Definición 1.1.1. Un campo que no contiene subcampos propios es llamado *campo primo*.

Ejemplo 1.1.2. $\mathbb{F}_p$ y $\mathbb{Q}$ (el campo de los números racionales) son campos primos

Definición 1.1.3. Diremos que la *característica* del campo finito $\mathbb{F}$ es p, si éste tiene como subcampo primo a $\mathbb{Z}/p\mathbb{Z}$.

Nota 1.1.4. La característica de un campo finito siempre es un número primo. Más aún, si un campo tiene característica p, entonces éste tiene como subcampo primo a $\mathbb{Z}/p\mathbb{Z}$ salvo isomorfismo.

Notación 1.1.5. Si $\mathbb{E}$ es una extensión de $\mathbb{F}$, tenemos que $\mathbb{E}$ es un $\mathbb{F}$-espacio vectorial. Denotaremos por el símbolo $[\mathbb{E} : \mathbb{F}]$ a la dimensión de $\mathbb{E}$ como $\mathbb{F}$-espacio vectorial.

Lema 1.1.6. *Sea $\mathbb{K}$ un campo finito que contiene a un subcampo $\mathbb{F}$, con q elementos. Entonces $\mathbb{K}$ tiene q^m elementos, donde $[\mathbb{K} : \mathbb{F}] = m$.*

Demostración. $\mathbb{K}$ es un $\mathbb{F}$-espacio vectorial de dimensión finita, ya que $\mathbb{K}$ es finito. Sea $m = [\mathbb{K} : \mathbb{F}]$ y $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base de $\mathbb{K}$. Cada elemento $\beta \in \mathbb{K}$, se puede escribir de forma única como combinación lineal de los elementos de la base, es decir:

$$\beta = a_1\alpha_1 + \cdots + a_m\alpha_m$$

donde $a_i \in \mathbb{K}$. Como cada a_i puede tomar q valores, y cada expresión de la forma anterior está en $\mathbb{K}$, concluimos que $\mathbb{K}$ debe tener exactamente q^m elementos. □

Consideremos ahora a $\mathbb{F}_q$ como una extensión de su campo primo. Haciendo una adaptación al teorema anterior y tomando en cuenta que el campo primo de $\mathbb{F}_q$ tiene p elementos (donde p es la característica de $\mathbb{F}_q$), tenemos un nuevo e importante teorema.

Teorema 1.1.7. Sea $\mathbb{F}$ un campo finito. Entonces $\mathbb{F}$ tiene p^m elementos, donde m es igual a la dimensión de $\mathbb{F}$ sobre su campo primo, y p es la característica de $\mathbb{F}$.

Ahora mostraremos que $\mathbb{F}^*$ es cíclico, para esto usaremos la fórmula de inversión de Möbius que presentaremos a continuación, sin embargo, la demostración de ésta la omitiremos (véase [LN94]).

Definición 1.1.8 (Función de Möbius). Sea $\mu : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ el mapeo definido por $\mu(1) = 1$, $\mu(n) = 0$ si $p^2|n$ para algún primo p y $\mu(p_1p_2\cdots p_r) = (-1)^r$ donde $p_1, p_2, \ldots, p_r$ son primos distintos.

Ejemplo 1.1.9. $\mu(5) = -1$, $\mu(25) = 0$ y $\mu(15) = (-1)^2 = 1$.

Teorema 1.1.10 (Fórmula de Inversión de Möbius). Sea $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ una función con valores complejos. Si $F(n) := \sum_{d|n} f(d)$, entonces

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right),$$

donde las sumas son sobre los enteros positivos que son divisores de n.

Esta fórmula, además de ayudarnos a demostrar que $\mathbb{F}^*$ es cíclico, nos sirve, entre otras cosas, para calcular el valor de la función de Euler, lo que también nos será de gran utilidad.

Aplicación 1.1.11. Sea ϕ la función de Euler, i.e., $\phi(1) = 1$, para $n > 1$ $\phi(n)$ es igual al número de enteros positivos menores que n, que son primos relativos con n. Demos una fórmula para calcular $\phi(n)$. Es fácil ver que $n = \sum_{d|n} \phi(d)$, entonces si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, usando la fórmula de inversión de Möbius, tenemos que:

$$\begin{aligned} \phi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} \\ &= n - \sum_{i} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} + \cdots \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \end{aligned} \tag{1.1}$$

Así, por ejemplo, 10 tiene $10(1 - 1/2)(1 - 1/5) = 4$ números menores y primos relativos con él

Teorema 1.1.12. Sea $\mathbb{F}^*$ el grupo de las unidades de un campo finito $\mathbb{F}$ Entonces $\mathbb{F}^*$ es cíclico

Demostración. Sea $|\mathbb{F}^*| = m$. Denotemos por $\psi(d)$ al número de elementos en $\mathbb{F}^*$ de orden d. Tenemos que $m = \sum_{d|m} \psi(d)$, usando la fórmula de inversión de Möbius y la ecuación 1.1, nos queda:

$$\psi(m) = \sum_{d|n} \mu(d) \frac{m}{d} = \phi(m).$$

Como $\varphi(m) = 1$ si y sólo si $m = 1$ (que es el caso trivial), tenemos que $\phi(m)$, y por lo tanto $\psi(m)$, es mayor que 1 para $m > 1$, lo que significa que $\mathbb{F}^*$ tiene cuando menos un elemento de orden m, y entonces $\mathbb{F}^*$ es cíclico. □

Corolario 1.1.13. *Cualquier extensión finita de un campo finito $\mathbb{F}$ es simple.*

Demostración. Sea $\mathbb{E}$ una extensión finita de $\mathbb{F}$, entonces si $[\mathbb{E} : \mathbb{F}] = s$, tenemos que $\mathbb{E}$ tiene $|\mathbb{F}|^s$ elementos, de donde $\mathbb{E}$ es un campo finito. Por el teorema anterior, existe un elemento $\gamma \in \mathbb{E}^*$ que genera a $\mathbb{E}^*$, entonces $\mathbb{E} = \mathbb{F}(\gamma)$. □

Definición 1.1.14. Sea $\mathbb{F}_q$ un campo finito con q elementos. Una extensión $\mathbb{K}$ de $\mathbb{F}_q$ es un campo de descomposición del polinomio $f(x) \in \mathbb{F}_q[x]$ sobre $\mathbb{F}_q$, si todas las raíces de $f(x)$ están en $\mathbb{K}$ y no existe subcampo de $\mathbb{K}$ que contenga a $\mathbb{F}_q$ con esta propiedad.

Ahora presentaremos unos resultados de la teoría general de campos de descomposición cuyas demostraciones las podemos encontrar en el libro de [Mor96].

Teorema 1.1.15 (Existencia de campos de descomposición). Sea $\mathbb{F}$ un campo. Si $f(x) \in \mathbb{F}[x]$ es un polinomio de grado positivo, entonces existe un campo de descomposición para $f(x)$ sobre $\mathbb{F}$.

Teorema 1.1.16 (Unicidad de campos de descomposición). Cualesquiera dos campos de descomposición de un polinomio $f(x) \in \mathbb{F}[x]$ sobre el campo $\mathbb{F}$ son isomorfos con un isomorfismo que deja fijos a los elementos de $\mathbb{F}$ y actúa como permutación en las raíces de $f(x)$.

Definición 1.1.17. Sea $\mathbb{E}$ una extensión algebraica del campo finito $\mathbb{F}$. *Un polinomio irreducible* $p(x) \in \mathbb{F}[x]$ es *separable* si no tiene raíces múltiples en su campo de descomposición. Un polinomio $g(x) \in \mathbb{F}[x]$ es *separable* si cada factor irreducible de $g(x)$ es separable. Un *elemento* $\alpha \in \mathbb{E}$ es *separable* si su polinomio mínimo sobre $\mathbb{F}$ es separable. $\mathbb{E}$ es *separable* si todo elemento en $\mathbb{E}$ es separable.

La proposición que presentamos a continuación, es un resultado de la teoría general de campos. Podemos encontrar una demostración de este hecho en [Mor96].

Proposición 1.1.18. *Un polinomio $f(x)$ no tiene raíces múltiples si y sólo si $f(x)$ y su derivada $f'(x)$ son primos relativos.*

Corolario 1.1.19. *Un polinomio irreducible $p(x)$ es separable si y sólo si $p'(x) \neq 0$.*

Definición 1.1.20. Un campo $\mathbb{F}$ es perfecto, si toda extensión algebraica de $\mathbb{F}$, es separable.

Ahora nuestro objetivo es mostrar que todo campo finito $\mathbb{F}$ es perfecto, para esto, basta mostrar que todo polinomio irreducible en $\mathbb{F}[x]$ es separable.

Proposición 1.1.21. *Sea $\mathbb{F}$ un campo finito de característica p. Entonces:*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad y \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

para todo entero positivo n.

Demostración. Haremos inducción sobre n y usaremos el hecho, fácil de demostrar, de que p divide al coeficiente binomial $\binom{p}{i}$ para $1 \leq i < p$, lo que implica que $\binom{p}{i} = 0$ en $\mathbb{F}$ para $1 \leq i < p$.

$$\begin{aligned}(a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^{p-i}b^i \\ &= a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}b^i \\ &= a^p + b^p.\end{aligned}$$

por lo que el caso $n = 1$ esta completo. Supongamos que el resultado es verdadero para $n-1$, entonces:

$$\begin{aligned}(a+b)^{p^n} &= (a+b)^{p^{n-1}p} \\ &= [(a+b)^{p^{n-1}}]^p \\ &= (a^{p^{n-1}} + b^{p^{n-1}})^p \\ &\overset{\text{caso } n=1}{=} a^{p^n} + b^{p^n}.\end{aligned}$$

Para demostrar $(a-b)^{p^n} = a^{p^n} - b^{p^n}$, notemos que.

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}$$

y el resultado es inmediato. □

Corolario 1.1.22. *Sea $\mathbb{F}$ un campo finito con q^n elementos. Entonces:*

$$(a+b)^{q^j} = a^{q^j} + b^{q^j} \quad y \quad (a-b)^{q^j} = a^{q^j} - b^{q^j}$$

para todo entero positivo j.

La demostración es inmediata ya que q es una potencia de un número primo p, donde p es la característica de $\mathbb{F}$.

Proposición 1.1.23. *Sea $\mathbb{F}$ un campo finito con q elementos, entonces $a^q = a$ para todo $a \in \mathbb{F}$.*

Demostración. Todo elemento $a \in \mathbb{F}^*$ satisface que $a^{q-1} = 1$ ya que $\mathbb{F}^*$ es un grupo de orden $q-1$, por lo tanto, $a^q = a$ para todo $a \in \mathbb{F}$. □

Corolario 1.1.24. *Sea $\mathbb{F}$ un campo finito con q elementos, entonces $a^{q^n} = a$ para todo $a \in \mathbb{F}$ y todo entero positivo n.*

Lema 1.1.25. *Sea $\mathbb{F}$ un campo finito de característica p, y sea $f(x) \in \mathbb{F}[x]$, un polinomio irreducible. Si $f(x)$ es un polinomio no separable (inseparable), entonces existe un entero positivo d tal que $f(x) = h(x^{p^d})$ donde $h(x)$ es separable.*

Demostración. Si $f(x) = a_0 + a_1x + \cdots + a_nx^n$ no es separable, por el corolario 1.1.19, sabemos que $f'(x) = 0$, esto significa que $p|ia_i$, lo que implica que $p|i$ para las i's tales que $a_i \neq 0$, por lo tanto, $f(x) = h(x^p)$. Si $h(x)$ es separable, hemos terminado, de lo contrario podemos aplicar el mismo argumento para $h(x)$ y obtener el resultado deseado en un número finito de pasos. □

Teorema 1.1.26. Todo polinomio irreducible sobre un campo finito es separable, por lo tanto, todo campo finito es perfecto.

Demostración. Sea $\mathbb{F}$ un campo finito de característica p, entonces el campo primo de $\mathbb{F}$ es $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Si $[\mathbb{F} : \mathbb{F}_p] = n$, entonces $\mathbb{F}$ tiene $p^n = q$ elementos. Como todo elemento $a \in \mathbb{F}$ satisface $a^q = a$ (proposición 1.1.23), tenemos que $a = b^p$ con $b = a^{p^{n-1}}$, así vemos que todo elemento en $\mathbb{F}$ es una potencia de p.

Supongamos que $f(x)$ es un polinomio inseparable en $\mathbb{F}[x]$. Por la proposición 1.1.25, $f(x) = h(x^p)$, por lo que:

$$\begin{aligned} f(x) &= a_0 + a_1x^p + \cdots + a_nx^{p^n} \\ &= b_0^p + b_1^px^p + \cdots + b_n^px^{np} \\ &= (b_0 + b_1x + \cdots + a_nx^n)^p \quad \text{usando la proposición 1.1.21.} \end{aligned}$$

Por lo tanto $f(x)$ no es irreducible y, por lo tanto, todo campo finito es perfecto. □

1.2 Campos finitos como Campos de descomposición

En esta sección veremos que todo campo finito es el campo de descomposición de un polinomio sobre su campo primo. Con esto, usando la unicidad de los campos de descomposición, veremos que sólo hay un único campo finito con q elementos (salvo isomorfismo), lo que nos permitirá hablar del campo finito con q elementos.

Así mismo, dado un polinomio sobre un campo primo, nos podemos preguntar sobre el campo de descomposición de este polinomio. La existencia de este campo de descomposición nos garantizará la existencia de los campos finitos Más aún, mostraremos que existe siempre un campo finito con p^n elementos para todo primo p y para todo entero positivo n.

Lo que mostraremos en seguida es que todo campo finito es el campo de descomposición de un polinomio de la forma $x^{p^n} - x \in \mathbb{F}_p[x]$ para algún primo p y un entero positivo n.

Recordemos que si $\mathbb{F}_{p^s}$ es un campo finito con p^s elementos, entonces este tiene característica p y por lo tanto, tiene como subcampo primo a $\mathbb{F}_p$.

Lema 1.2.1. *Sea $f(x)$ el polinomio $x^{q^n} - x \in \mathbb{F}_q[x]$ donde $\mathbb{F}_q$ es un campo finito con q elementos. Entonces $f(x)$ no tiene raíces múltiples en su campo de descomposición, i.e., es separable.*

Demostración Supongamos que $\mathbb{F}_q$ tiene característica p, entonces p divide a q y por lo tanto $q = 0$ en $\mathbb{F}_q$. Como $f'(x) = q^n x^{q^n-1} - 1 = -1 \neq 0$ en $\mathbb{F}_q[x]$, tenemos que el máximo común divisor de $f(x)$ y $f'(x)$ es 1. Usando la proposición 1.1.18 vemos que $f(x)$ es separable. □

Teorema 1.2.2. Sea $\mathbb{F}_{q^n}$ un campo finito con q^n elementos. Entonces $\mathbb{F}_{q^n}$ es un campo de descomposición del polinomio $x^{q^n} - x \in \mathbb{F}_q[x]$ (este campo es único salvo isomorfismos).

Demostración. Por la proposición 1.1.23, $a^{q^n} = a$ para toda $a \in \mathbb{F}_{q^n}$, se tiene que toda $a \in \mathbb{F}_{q^n}$ es raíz del polinomio $x^{q^n} - x$. Como este polinomio tiene exactamente q^n raíces distintas (recordemos que es separable) y $\mathbb{F}_{q^n}$ tiene q^n elementos, vemos que $\mathbb{F}_{q^n}$ es, en efecto, un campo de descomposición de este polinomio (único salvo isomorfismo). □

Corolario 1.2.3. *Cualesquiera dos campos finitos con el mismo número de elementos son isomorfos*

Demostración. Sean $\mathbb{F}$ y $\mathbb{K}$ dos campos finitos con q elementos. Como $q = p^n$ para algún primo p y algún entero positivo n, tenemos que ambos campos tienen al mismo subcampo primo

$\mathbb{F}_p$. Por el teorema anterior cada uno de los campos $\mathbb{F}$ y $\mathbb{K}$ son un campo de descomposición del polinomio $x^q - x \in \mathbb{F}_p[x]$. Del teorema 1.1.16 se sigue que $\mathbb{F} \cong \mathbb{K}$. □

Los resultados anteriores nos permiten mostrar la existencia y unicidad de los campos finitos, lo que nos permitirá hablar del "campo finito" con q elementos.

Teorema 1.2.4 (Existencia y unicidad de campos finitos). Sea q una potencia de un primo. Supongamos que existe un campo finito $\mathbb{F}_q$, con q elementos, entonces para cada entero positivo n existe un campo finito con q^n elementos que contiene como subcampo a $\mathbb{F}_q$. Este campo es único salvo isomorfismos.

Demostración. Sea $\mathbb{K}$ un campo de descomposición del polinomio $f(x) = x^{q^n} - x \in \mathbb{F}_q[x]$. Por la saparabilidad de este polinomio, hay q^n elementos distintos en $\mathbb{K}$ que son raíces de $f(x)$. Sea $S = \{y \in \mathbb{K} : y^{q^n} = y\}$. Este conjunto contiene a todas las raíces de $f(x)$ y solamente a éstas ya que todo $a \in S$ satisface que $a^{q^n} - a = 0$, por lo que $|S| = q^n$.

Afirmamos que S es un subcampo de $\mathbb{K}$. En efecto, el 1 y 0 están en S; si tomamos $a, b \in S$, por la proposición 1.1.21, $(a-b)^{q^n} = a^{q^n} - b^{q^n} = a - b$ y $(ab^{-1})^{q^n} = a^{q^n}(b^{-1})^{q^n} = a^{q^n}(b^{q^n})^{-1}) = ab^{-1}$ tenemos que $a - b$ y ab^{-1} están en S, por lo que S es un subcampo de $\mathbb{K}$.

Como S es un subcampo de $\mathbb{K}$ formado por las raíces de $f(x)$, tenemos que $f(x)$ se descompone en S y por lo tanto $S = \mathbb{K}$. Tenemos que S es un campo finito con q^n elementos y es el campo de descomposición de $f(x)$. Por los teoremas 1.1.15, 1.1.16 y el corolario 1.2.3 este campo existe y es único (salvo isomorfismo). □

De este resultado se sigue el siguiente teorema.

Teorema 1.2.5. Sea $\mathbb{F}_p$ el campo finito con p elementos. Para cada entero positivo n existe un único campo con p^n elementos tal que tiene a $\mathbb{F}_p$ como subcampo.

Corolario 1.2.6. *Para cada potencia de un primo q, y para cada entero positivo n, existe un campo con q^n elementos.*

1.3 Los subcampos de un campo finito

Teorema 1.3.1. Sean $\mathbb{F}$, $\mathbb{K}$ y $\mathbb{E}$ campos finitos tales que $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$. Entonces $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$.

Demostración. Supongamos que $\mathbb{F}$ tiene q elementos. Como consecuencia del lema 1.1.6 tenemos que $\mathbb{E}$ tiene $q^{[\mathbb{E}:\mathbb{F}]}$ elementos y $\mathbb{K}$ tiene $t = q^{[\mathbb{K}:\mathbb{F}]}$ elementos; así mismo $\mathbb{E}$ tiene $t^{[\mathbb{E}:\mathbb{K}]}$ elementos. Por lo tanto:

$$q^{[\mathbb{E}:\mathbb{F}]} = t^{[\mathbb{E}:\mathbb{K}]} = (q^{[\mathbb{K}:\mathbb{F}]})^{[\mathbb{E}:\mathbb{K}]} = q^{[\mathbb{K}:\mathbb{F}][\mathbb{E}:\mathbb{K}]}$$

y entonces $[\mathbb{E}:\mathbb{F}] = [\mathbb{E}:\mathbb{K}][\mathbb{K}:\mathbb{F}]$. □

Lema 1.3.2. *Sea $\mathbb{F}$ un campo. Entonces $x^l - 1$ divide a $x^m - 1$ en $\mathbb{F}[x]$ si, y sólo si, l divide a m.*

Demostración. Sea $m = lq + r$ con $0 \leq r < l$ Entonces

$$\frac{x^m - 1}{x^l - 1} = x^r \frac{x^{ql} - 1}{x^l - 1} + \frac{x^r - 1}{x^l - 1}$$

como $(x^{ql} - 1)/(x^l - 1) = (x^l)^{q-1} + (x^l)^{q-2} + \cdots + x^l + 1 = f(x) \in \mathbb{F}[x]$, tenemos que $\frac{x^m-1}{x^l-1} = x^r f(x) + \frac{x^r-1}{x^l-1}$. por lo que $x^l - 1$ divide a $x^m - 1$ si y sólo si $(x^m - 1)/(x^l - 1)$ es un polinomio; si y sólo si

$$\frac{x^r - 1}{x^l - 1} = \frac{x^m - 1}{x^l - 1} - x^r f(x)$$

es un polinomio; si y sólo si $r = 0$ ya que $r < l$. □

Lema 1.3.3. *Si a es un entero positivo, entonces $a^l - 1$ divide a $a^m - 1$ si, y sólo si, l divide a m*

Si $a = 1$ el resultado es trivial. Si $a \neq 1$, la demostración es inmediata al substituir x por a en la demostración al lema anterior.

Teorema 1.3.4. Sea $\mathbb{K}$ una extensión finita del campo finito $\mathbb{F}_q$ tal que $[\mathbb{K}:\mathbb{F}] = n$. Entonces para cada divisor positivo m de n existe un único (salvo isomorfismo) subcampo de $\mathbb{K}$ que contiene a $\mathbb{F}_q$ con q^m elementos. Conversamente, cada subcampo de $\mathbb{K}$ que contiene a $\mathbb{F}_q$ tiene q^m elementos para algún divisor positivo m de n.

Demostración Como $[\mathbb{K} \cdot \mathbb{F}_q] = n$ entonces $\mathbb{K}$ tiene q^n elementos Sea m un divisor de n, por el lema 1.3.3 sabemos que $q^m - 1$ divide a $q^n - 1$ y por el lema 1.3.2 tenemos que $x^{q^m-1} - 1$ divide a $x^{q^n-1} - 1$, por lo que toda raíz de $x^{q^m-1} - 1$ es raíz de $x^{q^n-1} - 1$ y por lo tanto, toda raíz de $x^{q^m} - x$ es raíz de $x^{q^n} - x$. Sabemos que $\mathbb{K}$ es el campo de descomposición del

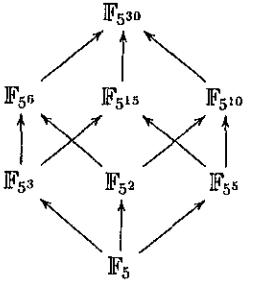
polinomio $x^{q^n} - x$ así que $\mathbb{K}$ debe contener como subcampo al campo $\mathbb{F}$ de descomposición de $x^{q^m} - x$ sobre $\mathbb{F}_q$. Por la saparabilidad de este polinomio, $\mathbb{F}$ debe tener exactamente q^m elementos. En virtud del corolario 1.2.3, $\mathbb{F} \cong \mathbb{F}_{q^m}$.

Conversamente, si $\mathbb{F}$ es un subcampo de $\mathbb{K}$ que contiene a $\mathbb{F}_q$, entonces $\mathbb{F}$ tiene q^m elementos donde $m = [\mathbb{F} : \mathbb{F}_q]$ (lema 1.1.6), como por el teorema 1.3.1 $[\mathbb{F} : \mathbb{F}_q]$ divide a $[\mathbb{K} : \mathbb{F}_q] = n$, el resultado se sigue. □

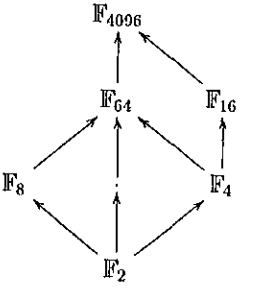
Observación 1.3.5. De la demostración al teorema anterior podemos concluir que el único subcampo de $\mathbb{F}_{q^n}$ que contiene a $\mathbb{F}_q$ de orden q^m para algún divisor m de n, está dado por las raíces del polinomio $x^{q^m} - x \in \mathbb{F}_q[x]$.

Corolario 1.3.6. *Sea $\mathbb{K}$ un campo con p^n elementos donde p es la característica de $\mathbb{K}$ y n un entero positivo. Entonces para cada divisor positivo m de n existe un único subcampo (salvo isomorfismo) de $\mathbb{K}$ con p^m elementos.*

Ejemplo 1.3.7. Tenemos que los subcampos del campo finito $\mathbb{F}_{5^{30}}$ los podemos encontrar determinando los divisores de 30. Así tenemos el siguiente diagrama:



Ejemplo 1.3.8. Ahora consideremos el campo finito $\mathbb{F}_{4096}$, i.e., este campo tiene 4096 elementos. Como $4096 = 2^{12}$, tenemos el siguiente diagrama:



Terminaremos esta sección con unos resultados que nos serán de gran utilidad para demostrar la racionalidad de la función zeta y que tienen que ver con las ideas expuestas aquí

Lema 1.3.9. *Sean s, μ, q, enteros positivos. El máximo común divisor entre $q^s - 1$ y $q^\mu - 1$ es un número de la misma forma, i e., $(q^s - 1, q^\mu - 1) = q^\nu - 1$ para algún entero $1 \leq \nu \leq \mu$.*

Demostración. Supongamos sin perdida de generalidad que $s \geq \mu$. Si μ divide a s entonces $q^\mu - 1$ divide a $q^s - 1$ (lema 1.3.3) y, por lo tanto, $(q^s - 1, q^\mu - 1) = q^\mu - 1$. Si μ no divide a s, entonces existen enteros positivos l, r tales que $s = l\mu + r$ con $1 \leq r < \mu$ y así

$$q^s - 1 = q^r(q^{l\mu} - 1) + q^r - 1 \text{ y } 0 \leq q^r - 1 < q^{l\mu} - 1,$$

sabemos también que $(q^{l\mu}-1)/(q^\mu-1)$ es un polinomio, por lo que si $t(x) = q^r(q^{l\mu}-1)/(q^\mu-1)$, tenemos:

$$q^s - 1 = t(x)(q^\mu - 1) + q^r - 1,$$

usando el algoritmo de Euclides para encontrar el máximo común divisor y el argumento anterior repetido en cada paso, tenemos que existe $\nu \geq 1$ tal que $(q^s - 1, q^\mu - 1) = q^\nu - 1$. □

1.4 Polinomios irreducibles y teoría de Galois sobre campos finitos

En esta sección veremos algunas propiedades de los polinomios irreducibles y su conexión con las extensiones algebraicas de un campo finito dado, también estudiaremos el grupo de Galois de estas extensiones. Mostraremos que toda extensión finita de un campo finito es una extensión de Galois y que el grupo de Galois de dicha extensión es un grupo cíclico generado por el automorfismo de Frobenius.

Lema 1.4.1. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre el campo finito $\mathbb{F}_q$ y sea α raíz de f en alguna extensión de $\mathbb{F}_q$. Entonces para un polinomio $h \in \mathbb{F}_q[x]$ tenemos que $h(\alpha) = 0$ si y sólo si f divide a h en $\mathbb{F}_q[x]$*

La demostración de este lema es de rutina y se puede encontrar, por ejemplo, en [Mor96] o bien, en [LN94]

Lema 1.4.2. *Sea $f \in \mathbb{F}_q[x]$ irreducible sobre $\mathbb{F}_q$ de grado m, entonces $f(x)$ divide a $x^{q^n} - x$ si, y sólo si, m divide a n.*

Demostración. Supongamos que $f(x)$ divide a $x^{q^n} - x$ y sea α una raíz de $f(x)$ en alguna extensión de $\mathbb{F}_q$, entonces $\alpha^{q^n} = \alpha$ por lo que $\alpha \in \mathbb{F}_{q^n}$ (teorema 1.2.2) y $\mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$. Como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg f = m$ y el grado de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ es n, usamos el teorema 1.3.1 para concluir que m divide a n.

Ahora supongamos que m divide a n, como $\mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^m}$ y $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg f = m$ entonces $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ y por lo tanto α es raíz de $x^{q^m} - x$, pero como $m|n$, $x^{q^m} - x$ divide a $x^{q^n} - x$ por lo que α también es raíz de $x^{q^n} - x$. Usando el lema anterior tenemos que f divide a $x^{q^n} - x$. □

Teorema 1.4.3. Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible de grado m. Entonces f tiene una raíz α en $\mathbb{F}_{q^m}$. Más aún, todas las raíces de f están dadas por los elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.

Demostración. Si α es una raíz de f en su campo de descomposición sobre $\mathbb{F}_q$, entonces $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg f = m$ por lo que

$$\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}, \tag{1.2}$$

y en particular $\alpha \in \mathbb{F}_{q^m}$. Ahora mostraremos que si β es un raíz de f, entonces también lo es β^q. Pongamos $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ donde las a_i's están en $\mathbb{F}_q$. Usando la propiedad de que $a^q = a$ para todo $a \in \mathbb{F}_q$ y el corolario 1.1.22 tenemos:

$$\begin{aligned} f(\beta^q) &= a_m\beta^{qm} + a_{m-1}\beta^{q(m-1)} + \cdots + a_0 \\ &= a_m^q\beta^{qm} + a_{m-1}^q\beta^{q(m-1)} + \cdots + a_0^q \\ &= (a_m\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0)^q \\ &= f(\beta)^q = 0, \end{aligned}$$

con lo que los elementos $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$ son raíces de f. Ahora demostraremos que estos elementos son distintos, con lo que demostraremos, de hecho, que estos elementos son precisamente las raíces de f. Supongamos que $\alpha^{q^j} = \alpha^{q^k}$ para algunos enteros $0 \leq j < k \leq m-1$, elevando esta igualdad a la potencia q^{m-k} tenemos:

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$$

por lo que, usando los lemas anteriores, concluimos que $f(x)$ divide a $x^{q^{m-k+j}} - x$ y por lo tanto m tiene que dividir a $m-k+j$ lo que es un absurdo ya que $0 < m-k+j < m$. □

Corolario 1.4.4. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible de grado m. Entonces el campo de descomposición de f sobre $\mathbb{F}_q$ es $\mathbb{F}_{q^m}$.*

Demostración Por el teorema anterior sabemos que el campo de descomposición de f es el campo $\mathbb{F}(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$, pero tenemos las siguientes igualdades:

$$\mathbb{F}(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}(\alpha) = \mathbb{F}_{q^m}.$$

La ultima igualdad se sigue de la ecuación 1.2 en la demostración al teorema anterior. □

Corolario 1.4.5. *Cualesquiera dos polinomios irreducibles en $\mathbb{F}_q$ del mismo grado tienen campos de descomposición isomorfos.*

Recordemos que el grupo de Galois $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ de una extensión $\mathbb{K}$ de $\mathbb{F}$ se define como el grupo de los automorfismos de $\mathbb{K}$ que dejan fijo a cada elemento de $\mathbb{F}$, i.e., $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) := \{\sigma \in \mathrm{Aut}(\mathbb{K}) : \sigma(a) = a \text{ para todo } a \in \mathbb{F}\}$.

Definición 1.4.6. Una extensión $\mathbb{K}$ de $\mathbb{F}$ es *normal* sobre $\mathbb{F}$, si $\mathbb{K}$ es el campo de descomposición de un conjunto de polinomios en $\mathbb{F}[x]$.

Definición 1.4.7. Una extensión $\mathbb{K}$ de $\mathbb{F}$ es una *extensión de Galois* si ésta es normal y separable.

Teorema 1.4.8. Una extensión finita $\mathbb{K}$ de $\mathbb{F}$ es una extensión de Galois si y sólo si se cumple que $|\mathrm{Gal}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$.

La demostración de este teorema se puede encontrar en [Mor96].

Lo que mostraremos en seguida es que todo campo finito es una extensión de Galois sobre su campo primo, más aún, veremos que toda extensión finita de un campo finito es una extensión de Galois, o bien, que $\mathbb{F}_{q^m}$ es una extensión de Galois del campo finito $\mathbb{F}_q$ para todo entero positivo m.

Lema 1.4.9. *Sea $\mathbb{F}_{q^m}$ la extensión de grado m del campo finito $\mathbb{F}_q$. Entonces $\mathbb{F}_{q^m}$ es una extensión normal de $\mathbb{F}_q$.*

La demostración de este lema es una consecuencia del teorema 1.2.2.

Lema 1.4.10. *La extensión $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ es separable.*

Este lema es consecuencia inmediata del teorema 1.1.26.

Como consecuencia inmediata de los lemas anteriores, tenemos el siguiente e importante teorema.

Teorema 1.4.11. La extensión $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ es de Galois.

Como consecuencia de este teorema y del teorema 1.4.8 sabemos que el grupo de Galois de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ tiene exactamente m elementos, sin embargo, es posible decir aún más, podemos dar explícitamente los elementos de este grupo.

Sea $\sigma_j : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$ el mapeo definido por $\sigma_j(\alpha) = \alpha^{q^j}$ donde $0 \leq j \leq m-1$. Afirmamos que σ_j es un automorfismo de $\mathbb{F}_{q^m}$ que deja fijos a los elementos de $\mathbb{F}_q$. En efecto, si $a \in \mathbb{F}_q$ entonces por el corolario 1.1.24 tenemos que $\sigma_j(a) = a$. Tomemos α, β dos elementos en $\mathbb{F}_{q^m}$, obviamente $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ y, por el corolario 1.1.22, tenemos que:

$$\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta),$$

además $\sigma_j(\alpha) = 0$ si y sólo si $\alpha = 0$ por lo que σ_j es inyectivo y como $\mathbb{F}_{q^m}$ es finito también es suprayectivo, por lo que σ_j es un automorfismo.

Definición 1.4.12. Al automorfismo de $\mathbb{F}_{q^m}$ definido por $\sigma(\alpha) = \alpha^q$ lo llamamos *automorfismo de Frobenius* del campo $\mathbb{F}_{q^m}$.

Teorema 1.4.13. El grupo de Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ es un grupo cíclico de orden m generado por el automorfismo de Frobenius de $\mathbb{F}_{q^m}$.

Demostración. Lo que haremos es demostrar que los automorfismos σ_j, definidos arriba, son todos distintos para $0 \leq j \leq m-1$, de aquí se sigue que estos son todos los elementos del grupo de *Galois* ya que son exactamente m, y como $\sigma_j = \sigma^j$ con σ el automorfismo de Frobenius, vemos que esto es lo único que necesitamos demostrar.

Supongamos pues que $\sigma_j = \sigma_k$ para $0 \leq j, k \leq m-1$. Sea $\alpha \in \mathbb{F}_{q^m}$ un generador de $\mathbb{F}^*_{q^m}$ (recordemos que $\mathbb{F}^*_{q^m}$ es un grupo cíclico), entonces $\alpha^{q^k} \neq \alpha^{q^j}$ de donde $\sigma_j(\alpha) \neq \sigma_k(\alpha)$ lo que es una contradicción. Así,

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{\sigma_j : 0 \leq j \leq m-1\} = < \sigma > .$$

□

Proposición 1.4.14. *Sea $p(x) \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado m. Supongamos que α es una raíz de este polinomio en algún campo de extensión. Entonces el conjunto de las raíces de $p(x)$ en su campo de descomposición $\mathbb{F}_{q^m}$ es precisamente la órbita de α bajo la acción del grupo de Galois $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Es decir, el conjunto $\{\sigma(\alpha) : \sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)\}$ es precisamente el conjunto de raíces de $p(x)$.*

Demostración. Recordemos que el teorema 1.4.3 nos garantiza que las raíces de p son los elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$, y por la forma que tienen los automorfismos del grupo de Galois de $\mathbb{F}_{q^m}$, el resultado es inmediato. □

Definición 1.4.15. *Sea $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^m}$. Llamamos conjugados de α con respecto a $\mathbb{F}_q$, a los elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Ejemplo 1.4.16. Sea $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ entonces f es irreducible sobre $\mathbb{F}_2$ ya que no tiene raíces en $\mathbb{F}_2$. Sea α una raíz de f en alguna extensión de $\mathbb{F}_2$, entonces $\alpha^2 + \alpha + 1 = 0$ y $\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$. Así, podemos considerar a los elementos de $\mathbb{F}_4$ como

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} = \{0, 1, \alpha, \alpha + 1\}$$

ya que $\alpha^2 = \alpha + 1$. Además tenemos que $\mathbb{F}_4^*$ es un grupo cíclico de orden 3 generado por α.

Ejemplo 1.4.17. Consideremos al campo finito con dos elementos $\mathbb{F}_2$, y tomemos una raíz α del polinomio irreducible $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ (este polinomio es irreducible ya que no tiene raíces en $\mathbb{F}_2$, lo que es fácil comprobar haciendo las evaluaciones), entonces $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$ y el campo $\mathbb{F}_2(\alpha) \cong \mathbb{F}_8$ es el campo de descomposición del polinomio $f(x)$ sobre $\mathbb{F}_2$ tal como lo muestra el corolario 1.4 4, por lo tanto, las raíces de $f(x)$ son $\alpha, \alpha^2, \alpha^4$. Como $f(\alpha) = 0$, entonces $\alpha^3 = \alpha^2 + 1$ y así $\alpha^4 = \alpha^2 + \alpha + 1$ por lo que, en términos de la base $\{1, \alpha, \alpha^2\}$ de $\mathbb{F}_8$ como $\mathbb{F}_2$ espacio vectorial, las raíces de $f(x)$ son α, α^2 y $\alpha^2 + \alpha + 1$.

Ejemplo 1.4.18. Sea $\alpha \in \mathbb{F}_{16}$ una raíz del polinomio $x^4 + x + 1 \in \mathbb{F}_2$, entonces los conjugados de α con respecto a $\mathbb{F}_2$ son $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ y $\alpha^8 = \alpha^2 + 1$. Los conjugados de α con respecto a $\mathbb{F}_4$ son α y α^4.

Observación 1.4.19. Si $\alpha \in \mathbb{F}_{q^m}$ y el polinomio mínimo de α sobre $\mathbb{F}_q$ tiene grado d, entonces d divide a m y dentro de los conjugados de α cada raíz de su polinomio mínimo aparece m/d veces.

Para terminar esta sección daremos una fórmula para contar el número de polinomios mónicos irreducibles sobre un campo finito, lo que nos ayudará a mostrar la existencia de polinomios irreducibles de cualquier grado. Esto es de mucho interés ya que entonces bastará encontrar un polinomio irreducible $p(x) \in \mathbb{F}_p[x]$ sobre $\mathbb{F}_p$ de grado n, para construir el campo finito $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/ < p(x) >$.

Empecemos por dar algunos resultados útiles.

Teorema 1.4.20. Para cada campo finito $\mathbb{F}_q$ y cada entero positivo n, el polinomio $x^{q^n} - x$ se factoriza como el producto de todos los polinomios mónicos irreducibles sobre $\mathbb{F}_q$ cuyo grado es un divisor de n.

Demostración. De acuerdo con el lema 1.4.2 los polinomios mónicos irreducibles que aparecen en la factorización de $g(x) = x^{q^n} - x$ son precisamente aquellos tales que su grado divide a n y sólo estos. Como $g'(x) = -1$, $g(x)$ no tiene raíces múltiples en su campo de descomposición sobre $\mathbb{F}_q$, por lo que cada polinomio mónico irreducible cuyo grado divide a n aparece sólo una vez en la factorización de $g(x)$, así $g(x)$ es precisamente el producto de todos los polinomios mónicos irreducibles, cuyo grado es un divisor de n. □

Corolario 1.4.21. *Si $N_q(d)$ denota el número de polinomios mónicos irreducibles en $\mathbb{F}_q[x]$ de grado d, entonces*

$$q^n = \sum_{d|n} dN_q(d) \text{ para todo } n \in \mathbb{N}, \tag{1.3}$$

donde la suma es sobre todos los divisores positivos de n.

Demostración. Denotemos por $F_q(d)$ al producto de todos los polinomios mónicos irreducibles sobre $\mathbb{F}_q$ de grado d. Por el teorema anterior sabemos que:

$$x^{q^n} - x = \prod_{d|n} F_q(d).$$

Comparando los grados en la identidad anterior, nos queda que $q^n = \sum_{d|n} dN_q(d)$ donde la suma es sobre todos los divisores positivos de n. □

Teorema 1.4.22. El número $N_q(n)$ de polinomios mónicos irreducibles de grado n está dado por la fórmula

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

donde $\mu(m)$ es la función de Möbius definida en la página 6.

Demostración. La ecuación 1.3 nos dice que $q^n = \sum_{d|n} dN_q(d)$, aplicando la fórmula de inversión de Möbius (teorema 1.1.10) tenemos lo deseado. □

Corolario 1.4.23. *Para cada entero positivo n existe un polinomio irreducible de grado n sobre el campo finito $\mathbb{F}_q$.*

Demostración. Tomando en cuenta que $\mu(1) = 1$ y que $\mu(d) \geq -1$ y usando el teorema anterior, tenemos la siguiente estimación para el número $N_q(n)$.

$$N_q(n) \geq \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \cdots - q) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right) > 0.$$

□

Ejemplo 1.4.24. Calculemos el número de polinomios mónicos irreducibles de grado 4 sobre $\mathbb{F}_2$. Usando el teorema anterior tenemos que:

$$\begin{aligned} N_2(4) &= \frac{1}{4}(\mu(1)2^4 + \mu(2)2^2 + \mu(4)2) \\ &= \frac{1}{4}(16 - 4) = 3 \end{aligned}$$

De manera análoga, tenemos que el número de polinomios mónicos irreducibles de grado 2 sobre $\mathbb{F}_2$ está dado por

$$N_2(2) = \frac{1}{2}(\mu(1)2^2 + \mu(2)2) = \frac{1}{2}(4 - 2) = 1,$$

por lo que tenemos que el único polinomio mónico irreducible de grado dos sobre $\mathbb{F}_2$ es $f = x^2 + x + 1$ (ver ejemplo 1.4.16 página 19).

Ejemplo 1.4.25. Si p y q son dos números primos distintos, entonces:

$$N_p(q) = q^{-1}(\mu(1)p^q + \mu(q)p) = q^{-1}(p^q - p)$$

1.5 La cerradura algebraica de un campo finito

Recordemos que un campo $\mathbb{K}$ es algebraicamente cerrado si no existen extensiones algebraicas de $\mathbb{K}$ diferentes de ella misma; y que una extensión algebraica $\mathbb{K}$ de $\mathbb{F}$ es una cerradura

algebraica de $\mathbb{F}$, si $\mathbb{K}$ es algebraicamente cerrado. Además recordemos que dado cualquier campo $\mathbb{F}$, siempre existe una cerradura algebraica y cualesquiera dos cerraduras algebraicas de $\mathbb{F}$ son isomorfas. Tenemos las siguientes equivalencias para un campo $\mathbb{K}$:

1. $\mathbb{K}$ es algebraicamente cerrado.
2. No hay extensiones finitas de $\mathbb{K}$ diferentes de ella misma.
3. Si $\mathbb{E}$ es una extensión de $\mathbb{K}$, entonces $\mathbb{K} = \{a \in \mathbb{E} : a \text{ es algebraico sobre } \mathbb{K}\}$.
4. Cada $f(x) \in \mathbb{K}[x]$ se descompone en $\mathbb{K}$.
5. Cada $f(x) \in \mathbb{K}[x]$ tiene una raíz en $\mathbb{K}$.
6. Cada polinomio irreducible sobre $\mathbb{K}$ tiene grado 1.

Para una demostración de estos hechos ver [Mor96, p. 30–37].

Sea $\mathbb{F}_q$ un campo finito con q elementos, queremos dar algunas propiedades de las cerraduras algebraicas de $\mathbb{F}_q$ y de los grupos de Galois de éstas sobre $\mathbb{F}_q$.

Definición 1.5.1. Sea N una cerradura algebraica de $\mathbb{F}_q$. Al automorfismo $\sigma \in \mathrm{Gal}(N/\mathbb{F}_q)$ tal que $\sigma(a) = a^q$ lo llamamos el *q-automorfismo de Frobenius.*

Teorema 1.5.2. Sea N una cerradura algebraica de $\mathbb{F}_q$. Para cada entero positivo n, existe un único subcampo de N de orden q^n. Si $\mathbb{K}$ y L son subcampos de N de ordenes q^n y q^m respectivamente, entonces $\mathbb{K} \subset \mathrm{L}$ si y sólo si $m|n$. Cuando esto ocurre L es una extensión de Galois de $\mathbb{K}$ con grupo de Galois generado por σ^n (σ es el q-automorfismo de Frobenius).

Demostración. Sea n un entero positivo. El conjunto de raíces en N del polinomio $x^{q^n} - x \in \mathbb{F}_q[x]$ tiene exactamente q^n elementos y es un campo. Entonces existe un subcampo de N de orden q^n. Como cualesquiera dos campos de orden q^n son el campo de descomposición de $x^{q^n} - x$ sobre $\mathbb{F}_q$, y como cualquier subcampo de N consiste exactamente de las raíces de $x^{q^n} - x$, tenemos que sólo existe un subcampo de N de orden q^n.

Sean $\mathbb{K}$ y L subcampos de N, de ordenes q^m y q^n respectivamente. Supongamos que $\mathbb{K} \subset \mathrm{L}$. Entonces:

$$n = [\mathrm{L} : \mathbb{F}_q] = [\mathrm{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}_q] = [\mathrm{L} : \mathbb{K}]m,$$

por lo que m divide a n. Ahora supongamos que $m|n$. Cada elemento de $\mathbb{K}$ satisface $a^{q^n} - a = 0$. Como $m|n$, también satisface $a^{q^n} - a = 0$, por lo que $\mathbb{K} \subset \mathrm{L}$. Cuando esto pasa, L es una extensión de Galois de $\mathbb{K}$ y $\mathrm{Gal}(\mathrm{L}/\mathbb{K}) =< \sigma^{|\mathbb{K}|} >$. □

Observación 1.5.3. Con este teorema vemos que si fijamos a una cerradura algebraica de $\mathbb{F}_q$, entonces sus subcampos finitos de orden q^n quedan totalmente determinados. Por esta razón, si fijamos a una cerradura algebraica, a la que denotaremos por $\overline{\mathbb{F}}_q$, podemos escribir a las extensiones finitas de $\mathbb{F}_q$ como $\mathbb{F}_{q^m} \subset \overline{\mathbb{F}}_q$ donde $m = [\mathbb{F}_{q^m} : \mathbb{F}_q] = |\mathbb{F}_{q^m}|$. Notemos también que con esta notación $\overline{\mathbb{F}}_q = \bigcup_{m\in\mathbb{N}} \mathbb{F}_{q^m}$. Si σ es el q-automorfismo de Frobenius, entonces $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) =< \sigma|_{\mathbb{F}_{q^m}} >$ y si $m|n$ $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^m}) =< \sigma^m|_{\mathbb{F}_{q^m}} >$.

1.6 Espacios sobre campos finitos

Sea $\mathbb{F}_q$ un campo finito con q elementos y fijemos una cerradura algebraica $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Definición 1.6.1. El *n-espacio afín* sobre $\mathbb{F}_q$ lo definimos como el conjunto

$$\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}}_q) = \{P = (x_1, x_2, \ldots, x_n) : x_i \in \overline{\mathbb{F}}_q\}$$

Análogamente, definimos el conjunto de puntos $\mathbb{F}_{q^m}$-racionales de $\mathbb{A}^n$ como el conjunto

$$\mathbb{A}^n(\mathbb{F}_{q^m}) = \{P = (x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_{q^m}\},$$

donde $\mathbb{F}_{q^m}$ es el único subcampo de $\overline{\mathbb{F}}_q$ de orden q^m.

Notemos que el grupo $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ actúa en $\mathbb{A}^n$ de la siguiente manera:

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \times \mathbb{A}^n &\longrightarrow \mathbb{A}^n \\ (\phi, P) &\longmapsto \phi P, \end{aligned} \tag{1.4}$$

donde $\phi P = (\phi(x_1), \phi(x_2), \ldots, \phi(x_n))$ Entonces podemos caracterizar al conjunto de puntos $\mathbb{F}_{q^m}$-racionales como.

$$\mathbb{A}^n(\mathbb{F}_{q^m}) = \{P \in \mathbb{A}^n \ . \ \phi P = P \text{ para todo } \phi \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^m}) \subset \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\}.$$

Sea $\overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n]$ el anillo de polinomios en n variables sobre $\overline{\mathbb{F}}_q$ y sea I un ideal de $\overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n]$.

Definición 1.6.2. Una *variedad (afín)* es un subconjunto de $\mathbb{A}^n$ de la forma:

$$V_I := \{P \in \mathbb{A}^n : f(P) = 0 \text{ para todo } f \in I\}.$$

Si V es una variedad, el *ideal de* V es el conjunto:

$$I(V) := \{f \in \overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n] : f(p) = 0 \text{ para todo } p \in V\}.$$

Una variedad V se dice que está *definida sobre* $\mathbb{F}_{q^m}$ si existen generadores de $I(V)$ en $\mathbb{F}_{q^m}[x_1, x_2, \ldots, x_n]$. Si V es definida sobre $\mathbb{F}_{q^m}$ definimos el conjunto $V(\mathbb{F}_{q^m})$ de puntos $\mathbb{F}_{q^m}$*-racionales* de V como

$$V(\mathbb{F}_{q^m}) := V \bigcap \mathbb{A}^n(\mathbb{F}_{q^m}).$$

Observación 1.6.3. Si V está definida sobre $\mathbb{F}_q$, entonces está definida sobre $\mathbb{F}_{q^m}$ para todo m natural y, por lo tanto, podemos hablar de los puntos $\mathbb{F}_{q^m}$ racionales de V para todo m.

Proposición 1.6.4. *Sea I un ideal de $\overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n]$ y V una variedad . Entonces*

$V_{I(V)} = V$

$I(V_I) = \sqrt{(I)}$. *Donde* $\sqrt{(I)} := \{f \in \overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n] : f^k \in I$ *para algún* $m \in \mathbb{N}\}$.

Demostración. Ver [Har77, p. 3] □

Definición 1.6.5. Si el ideal de una variedad V se puede generar por un polinomio, i.e., $I(V) =< f >$ para algún $f \in \overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n]$, entonces a V la llamamos *hipersuperficie* (afín) y la denotamos por $H_f(\overline{\mathbb{F}}_q)$. Si $H_f(\overline{\mathbb{F}}_q)$ está definida sobre $\mathbb{F}_{q^m}$, entonces denotamos por $H_f(\mathbb{F}_{q^m})$ al conjunto de puntos $\mathbb{F}_{q^m}$-racionales de $H_f(\overline{\mathbb{F}}_q)$.

La acción 1.4 nos define una acción por restricción de $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ sobre V, ya que si $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ entonces $f(\phi P) = \phi f(P)$ para todo $P \in \mathbb{A}^n$ y todo $\phi \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, por lo que si $P \in V$ también $\phi P \in V$.

Ejemplo 1.6.6. Sea $\mathbb{F}_4$ el campo finito con 4 elementos. Entonces $\mathbb{A}^n(\overline{\mathbb{F}}_4)$ tiene 4^n puntos $\mathbb{F}_4$-racionales, i.e., $|\mathbb{A}^n(\mathbb{F}_4)| = 4^n$. Más aún, $|A^n(\mathbb{F}_{4^s})| = 4^{sn}$. En forma general tenemos que $|\mathbb{A}^n(F_{q^s})| = q^{ns}$.

Definición 1.6.7. Decimos que el punto $P \in H_f(\overline{\mathbb{F}}_q)$ es *singular*, si P es un cero común de las derivadas parciales de f. Es decir, si

$$\partial f/\partial x_1(P) = 0,\ \partial f/\partial x_2(P) = 0, \ldots,\ \partial f/\partial x_n(P) = 0.$$

Decimos que que $H_f(\overline{\mathbb{F}}_q)$ es *no singular* si no tiene puntos singulares.

Definición 1.6.8. El *n-espacio proyectivo* sobre $\mathbb{F}_q$, denotado por $\mathbb{P}^n = \mathbb{P}^n(\overline{\mathbb{F}}_q)$, lo definimos como el conjunto de todas las clases de equivalencia de las $n+1$-tuplas $(x_0, x_1, \ldots, x_n) \in \mathbb{A}^{n+1} - \{(0,0,\ldots,0)\}$ bajo la relación de equivalencia dada por

$$(x_0, x_1, \ldots, x_n) \sim (\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$$

para todo $\lambda \in \overline{\mathbb{F}}_q^*$. Si denotamos por $[x_0, \ldots, x_n]$ a la clase de equivalencia de $(x_0, \ldots, x_n)$, entonces

$$\mathbb{P}^n = \{[x_0, x_1, \ldots, x_n] : (x_0, x_1, \ldots, x_n) \in \mathbb{A}^{n+1} - (0,0,\ldots,0)\}.$$

El conjunto de puntos $\mathbb{F}_{q^m}$-racionales (proyectivos) de $\mathbb{P}^n$ lo definimos como el conjunto de todos los elementos $[x_0, x_1, \ldots, x_n] \in \mathbb{P}^n$ tales que existe $\lambda \in \overline{\mathbb{F}}_q^*$ con la propiedad de que $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) \in \mathbb{A}^{n+1}(\mathbb{F}_{q^m})$

Observación 1.6.9. Si definimos $\mathbb{P}^n(\mathbb{F}_{q^m})$ como el conjunto de clases de equivalencia de los elementos $(x_0, x_1, \ldots, x_n) \in \mathbb{A}^{n+1}(\mathbb{F}_{q^m}) - \{(0,0,\ldots,0)\}$ bajo la relación de equivalencia dada por $(x_0, x_1, \ldots, x_n) \sim (\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ para todo $\lambda \in \mathbb{F}_{q^m}^*$ entonces hay, claramente, una biyección entre $\mathbb{P}^n(\mathbb{F}_{q^m})$ y los puntos $\mathbb{F}_{q^m}$-racionales (proyectivos) de $\mathbb{P}^n$. Por lo que, para nuestros fines, no causa ambigüedad si denotamos por $\mathbb{P}^n(\mathbb{F}_{q^m})$ al conjunto de puntos $\mathbb{F}_{q^m}$-racionales (proyectivos) de $\mathbb{P}^n$.

Sea $f \in \overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n]$ un polinomio homogéneo, entonces tiene sentido preguntarse cuándo $f(P) = 0$ para algún $P \in \mathbb{P}^n$ A cada ideal homogéneo I de $\overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n]$ le asociamos un subconjunto de $\mathbb{P}^n$ de la siguiente manera:

$$\overline{V}_I := \{P \in \mathbb{P}^n : f(P) = 0 \text{ para todo} f \in I\}.$$

Definición 1.6.10. Una *variedad algebraica (proyectiva)* es un conjunto de la forma $\overline{V}_I$ con I un ideal homogéneo de $\overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n]$. Si $\overline{V}$ es una variedad algebraica (proyectiva), definimos el ideal (homogéneo) de $\overline{V}$, como

$$I(\overline{V}) .=< \{f \in \overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n] \,.\, f \text{ es homogeneo y } f(P) = 0 \text{ para todo } P \in \overline{V}\} > .$$

Si el ideal de $\overline{V}$ se puede generar con polinomios en $\mathbb{F}_{q^m}[x_0, x_1, \ldots, x_n]$, decimos que $\overline{V}$ *esta definida sobre* $\mathbb{F}_{q^m}$. Si $\overline{V}$ está definida sobre $\mathbb{F}_{q^m}$, definimos al conjunto de puntos $\mathbb{F}_{q^m}$-racionales de $\overline{V}$ como

$$\overline{V}(\mathbb{F}_{q^m}) = \overline{V} \bigcap \mathbb{P}^n(\mathbb{F}_{q^m}).$$

Proposición 1.6.11. *Sea I un ideal homogéneo de $\overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n]$ y $\overline{V}$ una variedad (proyectiva). Entonces*

$\overline{V}_{I(\overline{V})} = \overline{V}$

$I(\overline{V}_I) = \sqrt{(I)}$. *Donde* $\sqrt{(I)} := \{f \in \overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n] : f^k \in I \text{ para algún } m \in \mathbb{N}\}$.

Demostración. Ver [Har77, p. 8–11]. □

Definición 1.6.12. Si $\overline{V}$ es una variedad (proyectiva) e $I(\overline{V})$ esta generado por un polinomio homogéneo, entonces decimos que $\overline{V}$ es una hipersuperficie proyectiva y la denotaremos por $\overline{H}_f(\overline{\mathbb{F}}_q)$. Si $\overline{H}_f(\overline{\mathbb{F}}_q)$ está definida sobre $\mathbb{F}_{q^m}$ entonces denotamos por $\overline{H}_f(\mathbb{F}_{q^m})$ al conjunto de puntos $\mathbb{F}_{q^m}$-racionales de $\overline{H}_f(\overline{\mathbb{F}}_q)$.

Ejemplo 1.6.13. Si $\overline{N} = |\mathbb{P}^n(\mathbb{F}_{q^m})|$ y $N = |\mathbb{A}^{n+1}(\mathbb{F}_{q^m})|$ entonces $\overline{N} = q^{(n+1)m} - 1/q^m - 1 = N - 1/q^m - 1$. Más aún, si f es un polinomio homogéneo con coeficientes en $\mathbb{F}_q$ y $N_m(f) = |H_f(\mathbb{F}_{q^m})|$, entonces el número $\overline{N}_m(f) := |\overline{H}_f(\mathbb{F}_{q^m})|$ esta dado por:

$$\overline{N}_m(f) = N_m(f) - 1/q^m - 1,$$

para todo $m \in \mathbb{N}$.

Definición 1.6.14. A las hipersuperficies proyectivas dadas por polinomios de la forma $a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l$ donde cada $a_i \in \mathbb{F}_q$, $\prod a_i \neq 0$ y $l \in \mathbb{N}$, las llamamos *hipersuperficies de Fermat* sobre $\mathbb{F}_q$.

Como en el caso afín, tenemos que el grupo de Galois $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ actúa en $\mathbb{P}^n$ de la siguiente manera: para cada $P = [x_0, x_1, \ldots, x_n] \in \mathbb{P}^n$ y cada $\phi \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ definimos $\phi P := [\phi(x_0), \phi(x_1), \ldots, \phi(x_n)]$. La acción esta bien definida ya que si $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ es otro representante de P entonces

$$(\phi(\lambda x_0), \phi(\lambda x_1), \ldots, \phi(\lambda x_n)) = \phi(\lambda)(\phi(x_0), \phi(x_1), \ldots, \phi(x_n))$$

y como $\phi(\lambda) \in \overline{\mathbb{F}}_q$ tenemos que $(\phi(\lambda x_0), \phi(\lambda x_1), \ldots, \phi(\lambda x_n))$ también es un representante de ϕP

De manera análoga con el caso afín, esta acción induce una acción, por restricción, en cualquier variedad $\overline{V}$, ya que para todo polinomio homogéneo f, se tiene que $\phi(f(P)) = f(\phi(P))$.

Definición 1.6.15. Decimos que el punto $P \in \overline{H}_f(\overline{\mathbb{F}}_q)$ es *singular*, si P es un cero común de las derivadas parciales de f. Es decir, si

$$\partial f/\partial x_0(P) = 0,\ \partial f/\partial x_1(P) = 0, \ldots,\ \partial f/\partial x_n(P) = 0.$$

Decimos que que $\overline{H}_f(\overline{\mathbb{F}}_q)$ es *no singular* si no tiene puntos singulares.

Observación 1.6.16. Como $\partial f/\partial x_i(P) = a_i l p_i^{l-1}$ donde $P = [p_0, p_1, \cdots, p_n]$ y $f = a_0 x_0^l + a_1 x_1^l + \cdots + a_n x_n^l$ tenemos que que una hipersuperficie de Fermat tiene un punto singular solamente si la característica de $\mathbb{F}_q$ divide a l.

Ejemplo **1.6.17.** *Sea* $f = x_0^3 + x_1^3 + x_2^3 \in \mathbb{F}^2[x_0, x_1, x_2]$, *entonces este polinomio determina* una hipersuperficie de Fermat sobre $\mathbb{F}_2$ cuyos puntos $\mathbb{F}_2$-racionales son

$$[0,1,1],\ \ [1,0,1] \ \text{ y el } \ [1,1,0].$$

Si tomamos a $\mathbb{F}_4$ como en el ejemplo 1.4.16 entonces los puntos $\mathbb{F}_4$-racionales de esta hipersuperficie son.

$$\begin{array}{lll} [0,1,1] & [1,0,1] & [1,1,0] \\ [\alpha,0,1] & [\alpha,1,0] & [0,\alpha,1] \\ [\alpha^2,0,1] & [\alpha^2,1,0] & [0,\alpha^2,1] \end{array}$$

Si ahora consideramos a f *como un polinomio sobre* $\mathbb{F}_4$, *entonces* f *me determina una* hipersuperficie de Fermat sobre $\mathbb{F}_4$ cuyos puntos $\mathbb{F}_4$-racionales coinciden con los puntos $\mathbb{F}_4$-racionales de la hipersuperficie definida sobre $\mathbb{F}_2$. De hecho, los puntos $\mathbb{F}_{4^s}$-racionales de la hipersuperficie determinada por f sobre $\mathbb{F}_4$, siempre coinciden con los puntos $\mathbb{F}_{2^{2s}}$-racionales de la hipersuperficie definida sobre $\mathbb{F}_2$.

Capítulo 2

RELACIÓN HASSE-DAVENPORT

El principal objetivo en este capítulo es mostrar una relación probada por Hasse y Davenport existente entre las "sumas de Gauss" asociadas a ciertos campos finitos. Esta relación es una pieza fundamental en la demostración de la racionalidad de la función zeta que es uno de los fines de esta tesis. Para lograr esto es necesario conocer a los grupos de caracteres asociados a los campos finitos y sus propiedades, es por esto que las primeras secciones las dedicaremos a este fin

2.1 Traza y norma de un elemento sobre un campo finito

En esta sección tomaremos a $\mathbb{F}$ como el campo finito con q elementos, i.e. $\mathbb{F} = \mathbb{F}_q$ y a $\mathbb{F}_s = \mathbb{F}_{q^s}$, como la extensión finita de $\mathbb{F}$ de grado s.

2.1.1 La traza

Definición 2.1.1. Sea $\alpha \in \mathbb{F}_s$. La *traza de α sobre* $\mathbb{F}$, la cual es denotada por $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)$, es definida como

$$Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) := \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{s-1}}.$$

Si $\mathbb{F}$ es el campo primo de $\mathbb{F}_s$, entonces $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ es llamada la *traza absoluta* de α, y es denotada simplemente por $Tr_{\mathbb{F}_s}(\alpha)$.

Observación 2.1.2. La $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ es la suma de los conjugados de α con respecto a $\mathbb{F}$.

Antes de demostrar cualquier proposición de la traza, daremos una descripción diferente de ésta.

Sea $f(x) \in \mathbb{F}[x]$ el polinomio mínimo de α sobre $\mathbb{F}$ tal que $\deg(f(x)) := d = [\mathbb{F}(\alpha) : \mathbb{F}]$. Como $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}_s$ y $[\mathbb{F}_s : \mathbb{F}] = s$, usando el teorema 1.3.1, tenemos que d divide a s.

Definición 2.1.3. Al polinomio $g(x) = f(x)^{s/d} \in \mathbb{F}[x]$ lo llamamos *polinomio característico* de α sobre $\mathbb{F}$.

Proposición 2.1.4. *Sea $g(x)$ el polinomio característico de α sobre $\mathbb{F}$. Si $g(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_0$, entonces $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) = -a_{s-1}$.*

Demostración. Por el teorema 1.4.3, las raíces de $f(x)$ son: $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, de donde $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}})$ y, por lo tanto, $g(x) = (x-\alpha)^{s/d}(x-\alpha^q)^{s/d}\cdots(x-\alpha^{q^{d-1}})^{s/d}$. Por lo que cada raíz de $f(x)$ es raíz de $g(x)$ s/d veces. Por la observación 1.4.19, las raíces de $g(x)$ son precisamente los conjugados de α. Entones:

$$g(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{s-1}}). \tag{2.1}$$

Haciendo la multiplicación y comparando los coeficientes, tenemos que:

$$Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{s-1}} = -a_{s-1}.$$

□

Corolario 2.1.5. $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) \in \mathbb{F}$ *para toda* $\alpha \in \mathbb{F}_s$

Demostración. Como $g(x) \in \mathbb{F}[x]$, entonces $-a_{s-1} \in \mathbb{F}$ y, por la proposición anterior, $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) = -a_{s-1}$. □

Ahora demostraremos que la traza es, en realidad, un funcional lineal de $\mathbb{F}_s$ como $\mathbb{F}$-espacio vectorial.

Teorema 2.1.6. Sean $\mathbb{F} = \mathbb{F}_q$ y $\mathbb{F}_s = \mathbb{F}_{q^s}$, considerados como $\mathbb{F}$-espacios vectoriales. La función $Tr_{\mathbb{F}_s/\mathbb{F}} : \mathbb{F}_s \longrightarrow \mathbb{F}$ cumple con las siguientes propiedades:

i) $Tr_{\mathbb{F}_s/\mathbb{F}}$ es una transformación lineal de $\mathbb{F}_s$ sobre $\mathbb{F}$.

ii) $Tr_{\mathbb{F}_s/\mathbb{F}}(a) = sa$ para todo $a \in \mathbb{F}$.

iii) $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha^q) = Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ para todo $\alpha \in \mathbb{F}_s$.

Demostración. Tomemos $\alpha, \beta \in \mathbb{F}_s$ y $c \in \mathbb{F}$.

i) Veamos que es una transformación lineal.

a) Demostraremos que la traza abre sumas. Usando la proposición 1.1.22

$$\begin{aligned} Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha+\beta) &= (\alpha+\beta)+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{s-1}} \\ &= (\alpha+\beta)+(\alpha^q+\beta^q)+\cdots+(\alpha^{q^{s-1}}+\beta^{q^{s-1}}) \\ &= (\alpha+\alpha^q+\cdots+\alpha^{q^{s-1}})+(\beta+\beta^q+\cdots+\beta^{q^{s-1}}) \\ &= Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)+Tr_{\mathbb{F}_s/\mathbb{F}}(\beta). \end{aligned}$$

b) Demostraremos que la traza saca escalares Como $c \in \mathbb{F}$, $c^{q^k} = c$ para todo $k \in \mathbb{N}$ (proposición 1.1.23 y su corolario 1.1.24 en la página 10).

$$\begin{aligned} Tr_{\mathbb{F}_s/\mathbb{F}}(c\alpha) &= c\alpha+(c\alpha)^q+\cdots+(c\alpha)^{q^{s-1}} \\ &= c\alpha+c^q\alpha^q+\cdots+c^{q^{s-1}}\alpha^{q^{s-1}} \\ &= c\alpha+c\alpha^q+\cdots+c\alpha^{q^{s-1}} \\ &= c(\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{s-1}}) \\ &= cTr_{\mathbb{F}_s/\mathbb{F}}(\alpha). \end{aligned}$$

Por lo tanto, $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ es una transformación lineal Para ver que es suprayectiva, *primero veamos que existe* $\beta \in \mathbb{F}_s$ tal que $Tr_{\mathbb{F}_s/\mathbb{F}}(\beta) \neq 0$. Para esto, notemos que $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) = 0$ si y sólo si α es raíz del polinomio $x+x^q+x^{q^2}+\cdots+x^{q^{s-1}}$. Como este polinomio es de grado q^{s-1}, tiene a los más q^{s-1} raíces; pero $\mathbb{F}_s$ tiene q^s elementos, de donde existe $\beta \in \mathbb{F}_s$ tal que β no es raíz de este polinomio y por lo tanto $Tr_{\mathbb{F}_s/\mathbb{F}}(\beta) \neq 0$. Hagamos $Tr_{\mathbb{F}_s/\mathbb{F}}(\beta) = b$ y tomemos $a \in \mathbb{F}$. Observemos que:

$$Tr_{\mathbb{F}_s/\mathbb{F}}((a/b)\beta) = (a/b)Tr_{\mathbb{F}_s/\mathbb{F}}(\beta) = (a/b)b = a$$

de donde $Tr_{\mathbb{F}_s/\mathbb{F}}$ es suprayectiva.

ii) $Tr_{\mathbb{F}_s/\mathbb{F}}(a) = aTr_{\mathbb{F}_s/\mathbb{F}}(1)$ y claramente $Tr_{\mathbb{F}_s/\mathbb{F}}(1) = s$, por lo que $Tr_{\mathbb{F}_s/\mathbb{F}}(a) = sa$

iii) Por la proposición 1.1.23, $\alpha^{q^s} = \alpha$, de aquí que

$$\begin{aligned} Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha^{q^s} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{s-1}} + \alpha \\ &= Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha). \end{aligned}$$

□

Si ahora consideramos a $\mathbb{E}$ una extensión finita de $\mathbb{F}_s$, i.e., $\mathbb{F} \subset \mathbb{F}_s \subset \mathbb{E}$, tiene sentido preguntarnos por la relación que guardan las diferentes trazas: $Tr_{\mathbb{F}_s/\mathbb{F}}$, $Tr_{\mathbb{E}/\mathbb{F}}$, $Tr_{\mathbb{E}/\mathbb{F}_s}$. El siguiente teorema, de gran utilidad para este trabajo, nos dice cuál es esta relación.

Teorema 2.1.7 (Relación de Transitividad). Sea $\mathbb{F}$ un campo finito, $\mathbb{K}$ una extensión finita de $\mathbb{F}$, y $\mathbb{E}$, una extensión finita de $\mathbb{K}$. Si $\alpha \in \mathbb{E}$, entonces:

$$Tr_{\mathbb{E}/\mathbb{F}}(\alpha) = Tr_{\mathbb{K}/\mathbb{F}}(Tr_{\mathbb{E}/\mathbb{K}}(\alpha)).$$

Demostración. Supongamos que $\mathbb{F} = \mathbb{F}_q$, que $[\mathbb{E} : \mathbb{K}] = m$ y $[\mathbb{K} : \mathbb{F}] = n$. Entonces, por teorema 1.3.1, $[\mathbb{E} : \mathbb{F}] = mn$. Ahora:

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{F}}(Tr_{\mathbb{E}/\mathbb{K}}(\alpha)) &= \sum_{i=0}^{n-1} Tr_{\mathbb{E}/\mathbb{K}}(\alpha)^{q^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} \alpha^{q^{nj}} \right)^{q^i} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha^{q^{nj+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = Tr_{\mathbb{E}/\mathbb{F}}(\alpha). \end{aligned}$$

Hemos utilizado que si $0 \leq j \leq m-1$ y $0 \leq i \leq n-1$, entonces $0 \leq k = nj+i \leq mn-1$. □

Finalmente daremos una caracterización más de la traza, pero ahora en términos de su polinomio mínimo. Esta caracterización nos ayudará a ver que $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ es la traza de una transformación lineal.

Observación 2.1.8. Sea $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{F}[x]$ el polinomio mínimo de $\alpha \in \mathbb{F}_s$, entonces sabemos que $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}})$ por lo que, si consideramos a los campos $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}_s$, entonces $[\mathbb{F}_s : \mathbb{F}(\alpha)] = s/d$ y $Tr_{\mathbb{F}(\alpha)/\mathbb{F}} = \alpha + \alpha^q + \cdots + \alpha^{q^{d-1}} = -a_1$.

Como $\alpha \in \mathbb{F}(\alpha)$, entonces $Tr_{\mathbb{F}_s/\mathbb{F}(\alpha)}(\alpha) = (s/d)\alpha$ (ver teorema 2.1.6) y, por lo tanto:

$$\begin{aligned} Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) &= Tr_{\mathbb{F}(\alpha)/\mathbb{F}}(Tr_{\mathbb{F}_s/\mathbb{F}(\alpha)}(\alpha)) \\ &= Tr_{\mathbb{F}(\alpha)/\mathbb{F}}\left(\frac{s}{d}\alpha\right) \\ &= (s/d)Tr_{\mathbb{F}(\alpha)/\mathbb{F}}(\alpha) \\ &= -(s/d)a_1. \end{aligned}$$

Que es justo lo que queríamos mostrar.

Ejemplo 2.1.9. Tomemos $\alpha \in \mathbb{F}_4$ donde α es como en el ejemplo 1.4.16 página 19, entonces

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} = \{0, 1, \alpha, \alpha + 1\}.$$

Calculemos los valores de la traza absoluta de $\mathbb{F}_4$.

$$\begin{aligned} Tr_{\mathbb{F}_4}(0) &= 0 \\ Tr_{\mathbb{F}_4}(1) &= 1 + 1^2 = 0 \\ Tr_{\mathbb{F}_4}(\alpha) &= \alpha + \alpha^2 = \alpha + (\alpha + 1) = 1 \\ Tr_{\mathbb{F}_4}(\alpha^2) &= Tr_{\mathbb{F}_4}(\alpha) = 1 \text{ teorema 2.1.6 parte } \textit{iii)}. \end{aligned}$$

2.1.2 La norma

Definición 2.1.10. Sea $\alpha \in \mathbb{F}_s$. La *norma* $N_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ *de* α *sobre* $\mathbb{F}$ la definimos como

$$N_{\mathbb{F}_s/\mathbb{F}}(\alpha) := \alpha\alpha^q\alpha^{q^2}\cdots\alpha^{q^{s-1}} = \alpha^{(q^s-1)/(q-1)}$$

i e , $N_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ es el producto de los conjugados de α

Proposición 2.1.11. *Sea* $g(x)$ *el polinomio característico de* α *sobre* $\mathbb{F}$. *Si* $g(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_0$, *entonces* $N_{\mathbb{F}_s/\mathbb{F}}(\alpha) = (-1)^s a_0$

Demostración. Como en la demostración de la proposición 2.1.4, tenemos la ecuación 2.1

$$g(x) = (x - \alpha)(x - \alpha^q)\cdots(x - \alpha^{q^{s-1}}).$$

Haciendo la multiplicación y comparando nos queda

$$N_{\mathbb{F}_s/\mathbb{F}}(\alpha) = (-1)^s a_0.$$

□

Corolario 2.1.12. $N_{\mathbb{F}_s/\mathbb{F}}(\alpha) \in \mathbb{F}$, *para toda* $\alpha \in \mathbb{F}_s$.

Demostración. Por la proposición anterior, $N_{\mathbb{F}_s/\mathbb{F}}(\alpha) = (-1)^s a_0 \in \mathbb{F}$, ya que $g(x) \in \mathbb{F}[x]$. □

Teorema 2.1.13. Si $\mathbb{F} = \mathbb{F}_q$ y $\mathbb{F}_s = \mathbb{F}_{q^s}$ entonces la función $N_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ cumple con las propiedades siguientes:

i) $N_{\mathbb{F}_s/\mathbb{F}}(\alpha\beta) = N_{\mathbb{F}_s/\mathbb{F}}(\alpha)N_{\mathbb{F}_s/\mathbb{F}}(\beta)$ para $\alpha, \beta \in \mathbb{F}_s$;

ii) $N_{\mathbb{F}_s/\mathbb{F}}$ manda $\mathbb{F}_s$ sobre $\mathbb{F}$ y $\mathbb{F}_s^*$ sobre $\mathbb{F}^*$;

iii) $N_{\mathbb{F}_s/\mathbb{F}}(a) = a^s$ para todo $a \in \mathbb{F}$;

iv) $N_{\mathbb{F}_s/\mathbb{F}}(\alpha^q) = N_{\mathbb{F}_s/\mathbb{F}}(\alpha)$ para todo $\alpha \in \mathbb{F}_s$.

Demostración. i) Se sigue inmediatamente de la definición.

ii) En el corolario que precede a este teorema, vimos que, en efecto, $N_{\mathbb{F}_s/\mathbb{F}}$ mapea $\mathbb{F}_s$ en $\mathbb{F}$. Ahora $N_{\mathbb{F}_s/\mathbb{F}}(\alpha) = 0$ si y sólo si $\alpha = 0$, de donde $N_{\mathbb{F}_s/\mathbb{F}}$ mapea $\mathbb{F}_s^*$ en $\mathbb{F}^*$. Para ver que este mapeo es sobre, basta verificar que $N_{\mathbb{F}_s/\mathbb{F}} : \mathbb{F}_s^* \longrightarrow \mathbb{F}^*$ es sobre. Como este mapeo es un homomorfismo de grupos (recordemos que $N_{\mathbb{F}_s/\mathbb{F}}$ es multiplicativo), tenemos que $\operatorname{im}(N_{\mathbb{F}_s/\mathbb{F}}) \cong \mathbb{F}_s^*/\ker(N_{\mathbb{F}_s/\mathbb{F}})$. Si $d = |\ker(N_{\mathbb{F}_s/\mathbb{F}})|$, tenemos que $q^s - 1/d = |\operatorname{im}(N_{\mathbb{F}_s/\mathbb{F}})| \leq q - 1$, por lo tanto:

$$\frac{q^s - 1}{q - 1} \leq d. \tag{2.2}$$

Por otro lado, cada elemento en el kernel de $N_{\mathbb{F}_s/\mathbb{F}}$ es raíz del polinomio $x^{q^s-1/q-1} - 1$ por lo que se cumple que $d \leq q^s - 1/q - 1$. Juntando esto con la fórmula anterior (2.2), tenemos que $d = q^s - 1/q - 1$ y así, usando los teoremas de homomorfismo de grupos:

$$|\operatorname{im}(N_{\mathbb{F}_s/\mathbb{F}})| = q - 1.$$

Por lo tanto, nuestra transformación es sobreyectiva.

iii) Si $a \in \mathbb{F}$, entonces $a^q = a$ y, por lo tanto, $a^{q^r} = a$ para todo $r \in \mathbb{N}$. Entonces $N_{\mathbb{F}_s/\mathbb{F}}(a) = a.a^q \cdots a^{q^{s-1}} = a^s$.

iv) Para todo $\alpha \in \mathbb{F}_s$, se cumple que $\alpha^{q^s} = \alpha$, entonces:

$$N_{\mathbb{F}_s/\mathbb{F}}(\alpha^q) = \alpha^q \alpha^{q^2} \cdots \alpha^{q^s} = \alpha^q \alpha^{q^2} \cdots \alpha^{q^{s-1}} \alpha = N_{\mathbb{F}_s/\mathbb{F}}(\alpha).$$

□

Análogo al resultado de transitividad para la traza, tenemos el siguiente teorema.

Teorema 2.1.14 (Relación de transitividad). Sea $\mathbb{F}$ un campo finito, $\mathbb{K}$ una extensión finita de $\mathbb{F}$ y sea $\mathbb{E}$ una extensión finita de $\mathbb{K}$. Entonces

$$N_{\mathbb{E}/\mathbb{F}}(\alpha) = N_{\mathbb{K}/\mathbb{F}}(N_{\mathbb{E}/\mathbb{K}}(\alpha)).$$

Demostración Supongamos que $\mathbb{F}$ tiene q elementos, que el grado de $\mathbb{K}/\mathbb{F}$ es n y el grado de $\mathbb{E}/\mathbb{K}$ es m, entonces por el teorema 1.3.1 el grado de $\mathbb{E}/\mathbb{F}$ es nm. Así

$$\begin{aligned} N_{\mathbb{K}/\mathbb{F}}(N_{\mathbb{E}/\mathbb{K}}(\alpha)) &= N_{\mathbb{K}/\mathbb{F}}(\alpha^{q^{mn}-1/q^n-1}) \\ &= (\alpha^{q^{mn}-1/q^n-1})^{(q^n-1/q-1)} \\ &= \alpha^{(q^{mn}-1/q^n-1)(q^n-1/q-1)} \\ &= \alpha^{q^{mn}-1/q-1} \\ &= N_{\mathbb{E}/\mathbb{F}}(\alpha) \end{aligned}$$

□

Observación 2.1.15. Sea $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{F}[x]$ el polinomio mínimo de $\alpha \in \mathbb{F}_s$, entonces sabemos que $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}})$ por lo que, si consideramos a los campos $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}_s$, entonces $[\mathbb{F}_s : \mathbb{F}(\alpha)] = s/d$ y $N_{\mathbb{F}(\alpha)/\mathbb{F}}(\alpha) = \alpha\alpha^q \cdots \alpha^{q^{d-1}} = (-1)^d a_d$. Como $\alpha \in \mathbb{F}(\alpha)$ entonces $N_{\mathbb{F}_s/\mathbb{F}(\alpha)}(\alpha) = \alpha^{s/d}$ y, por lo tanto

$$\begin{aligned} N_{\mathbb{F}_s/\mathbb{F}}(\alpha) &= N_{\mathbb{F}(\alpha)/\mathbb{F}}(N_{\mathbb{F}_s/\mathbb{F}(\alpha)}(\alpha)) \\ &= N_{\mathbb{F}(\alpha)/\mathbb{F}}(\alpha^{s/d}) \\ &= N_{\mathbb{F}(\alpha)/\mathbb{F}}(\alpha)^{s/d} \\ &= \left[(-1)^d a_d\right]^{s/d} \\ &= (-1)^s a_d^{s/d}. \end{aligned}$$

Que es lo que queríamos mostrar.

Ejemplo 2.1.16. Tomemos al campo con 4 elementos $\mathbb{F}_4$ como

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} = \{0, 1, \alpha, \alpha + 1\}.$$

Entonces los valores de la norma absoluta de $\mathbb{F}_4$ son

$$\begin{aligned} N_{\mathbb{F}_4}(0) &= 0 \\ N_{\mathbb{F}_4}(1) &= 1 \\ N_{\mathbb{F}_4}(\alpha) &= \alpha\alpha^2 = \alpha^3 = 1 \\ N_{\mathbb{F}_4}(\alpha^2) &= N_{\mathbb{F}_4}(\alpha) = 1 \text{ teorema 2.1.13 parte } iv) \end{aligned}$$

Para terminar esta sección, hagamos notar que la traza y la norma son, de hecho, la traza y el determinante de una matriz, veamos:

Nota 2.1.17. Sea $\alpha \in \mathbb{F}_s$. Consideremos al mapeo $u_\alpha : \mathbb{F}_s \longrightarrow \mathbb{F}_s$ definido por $\beta \longmapsto \alpha\beta$. Este mapeo es, claramente, una $\mathbb{F}$-transformación lineal. Afirmamos que $Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) =$ traza$([u_\alpha])$ y que $N_{\mathbb{F}_s/\mathbb{F}}(\alpha) = \det[u_\alpha]$, donde $[u_\alpha]$ es la matriz de la transformación en alguna base.

En efecto, consideremos a los campos $\mathbb{F}(\alpha) \subset \mathbb{F}_s$ como $\mathbb{F}$-espacios vectoriales. Si $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{F}[x]$ es el polinomio mínimo de α, sabemos que $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/ < f(x) >$. Sea $A = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ base de $\mathbb{F}(\alpha)$ sobre $\mathbb{F}$, y sea $B = \{f_1, f_2, \ldots, f_{s/d}\}$ una base de $\mathbb{F}_s$ sobre $\mathbb{F}(\alpha)$, entonces $AB = \{f_1, \alpha f_1, \ldots, \alpha^{d-1} f_1, \ldots, f_{s/d}, \alpha f_{s/d}, \ldots, \alpha^{d-1} f_{s/d}\}$ es base de $\mathbb{F}_s$ sobre $\mathbb{F}$. La matriz de u_α en esta base está dada por:

$$[u_\alpha]_{AB} = \begin{pmatrix} C_\alpha & 0 & \ldots & & \\ 0 & C_\alpha & 0 & & \\ & 0 & C_\alpha & 0 & \\ & \vdots & & \ddots & \\ & & & 0 & C_\alpha \end{pmatrix}$$

donde C_α es la matriz:

$$\begin{pmatrix} 0 & 0 & & & -a_d \\ 1 & 0 & & & -a_{d-1} \\ 0 & 1 & \ddots & & \vdots \\ & 0 & & 0 & \\ & & & 1 & -a_1 \end{pmatrix}.$$

Como la traza de C_α es $-a_1$ y su determinante es $(-1)^d a_d$, se sigue que:

$$\begin{aligned} \text{traza}[u_\alpha]_{AB} &= -\frac{s}{d}a_1 \\ &= Tr_{\mathbb{F}_s/\mathbb{F}}(\alpha) \end{aligned}$$

y que.

$$\begin{aligned} \det[u_\alpha]_{AB} &= [(-1)^d a_d]^{s/d} \\ &= (-1)^s a_d^{s/d} \\ &= N_{\mathbb{F}_s/\mathbb{F}}(\alpha). \end{aligned}$$

De esto mismo, podemos concluir que el polinomio característico de α (tal y como lo definimos en esta sección), coincide con la definición tradicional del polinomio característico de la transformación u_α (para un análisis más profundo en este sentido, ver el libro [Lor96]).

2.2 Caracteres

En esta sección trabajaremos con un tipo especial de homomorfismos entre grupos que junto con las sumas de Gauss definidas en la sección que precede nos ayudarán en el estudio del número de soluciones de ciertas ecuaciones sobre campos finitos. Aunque nuestro interés principal es estudiar estos homomorfismos para el grupo de las unidades de un campo finito, presentaremos la teoría para el caso general.

Sea G un grupo abeliano finito multiplicativo de orden d con elemento identidad 1_G.

Denotemos por $S^1 = \{z \in \mathbb{C} : |z| = 1_{\mathbb{C}}\}$ al grupo del círculo complejo.

Definición 2.2.1. Un *carácter* de G es un homomorfismo de grupos $\chi : G \longrightarrow S^1$ de G a $S^1 \subset \mathbb{C}$

Observación 2.2.2. Dado un carácter χ de G, se cumple lo siguiente:

1. $\chi(1_G) = 1_{\mathbb{C}}$;
2. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$ para todo $a \in G$. Donde la barra denota la conjugación compleja.

3. $\chi(a)$ es una d-ésima raíz de la unidad para toda $a \in G$.

Demostración. Todas estas son consecuencia inmediata de que χ es un homomorfismo y de que $\chi(a)^d = \chi(a^d) = \chi(1_G) = 1_{\mathbb{C}}$. □

Ejemplo 2.2.3. Definamos $\varepsilon : G \longrightarrow S^1$ por $\varepsilon(a) = 1_{\mathbb{C}}$ para toda $a \in G$. Claramente este mapeo es un carácter de G, al que llamaremos *carácter trivial*, o bien, *carácter identidad.*

Ejemplo 2.2.4. Sea G el grupo de las unidades del campo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. El símbolo de Jacobi $\left(\frac{a}{p}\right)$ es un carácter de $\mathbb{F}_p^*$ y es definido como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático} \\ -1 & \text{si } a \text{ es un no residuo cuadrático.} \end{cases}$$

Para los detalles ver el libro [IR90]

Ejemplo 2.2.5. Si tenemos un carácter χ de G, podemos definir un nuevo carácter $\overline{\chi}$, tal que $\overline{\chi}(a) = \overline{\chi(a)}$. Como la conjugación compleja abre productos, vemos que $\overline{\chi}$ es, en efecto, un carácter de G. A este carácter lo llamaremos *carácter conjugado de* χ.

Podemos darle una estructura algebraica al conjunto de caracteres de G de la siguiente manera:

1. Dados χ y λ caracteres de G, definimos al mapeo $\chi\lambda : G \longrightarrow S^1$ como: $\chi\lambda(a) = \chi(a)\lambda(a)$. Este mapeo es un carácter ya que:

$$\chi\lambda(ab) = \chi(ab)\lambda(ab) = \chi(a)\chi(b)\lambda(a)\lambda(b) = \chi(a)\lambda(a)\chi(b)\lambda(b) = \chi\lambda(a)\chi\lambda(b).$$

   Notemos que $\varepsilon\chi = \chi\varepsilon = \chi$.

2. Si χ es un carácter de G, definimos $\chi^{-1} : G \longrightarrow S^1$ tal que $\chi^{-1}(a) := \chi(a)^{-1} = \overline{\chi(a)} = \overline{\chi}(a)$. Éste es nuevamente un carácter de G, ya que $\overline{\chi}$ lo es. Notemos que $\chi^{-1}\chi = \chi\chi^{-1} = \varepsilon$.

Como consecuencia de lo anterior, tenemos el siguiente teorema.

Teorema 2.2.6. Sea G un grupo abeliano finito de orden d. El conjunto de caracteres de G forma un grupo abeliano finito con las operaciones recién definidas. Su elemento identidad es el carácter trivial. A este grupo lo denotaremos por $C(G)$.

Demostración. Que $C(G)$ es un grupo abeliano, es inmediato de lo anterior. Como la imagen de cada elemento de G bajo algún carácter es una d-ésima raíz de la unidad, y como hay solamente d d-ésimas raíces de la unidad, se sigue que solamente puede haber un número finito de caracteres. □

Teorema 2.2.7. Si G es un grupo cíclico de orden d, entonces $C(G)$ es, también, un grupo cíclico de orden d

Demostración. Sea g un generador de G. Así, para todo $a \in G$, $a = g^r$ para algún $r \in \mathbb{N}$ y $\chi(a) = \chi(g^r) = \chi(g)^r$ para todo $\chi \in C(G)$, con lo que vemos que cada carácter χ de G está totalmente determinado por su valor en g. Como $\chi(g)$ es una d-ésima raíz de la unidad y solamente hay d de ellas, tenemos que $|C(G)| \leq d$.

Sea $\lambda \quad G \longrightarrow S^1$ definido como $\lambda(g) = e^{2\pi i/d}$ éste es un carácter de G (recordemos que queda totalmente determinado por su valor en g). Tenemos que los caracteres $\varepsilon, \lambda, \lambda^2, \ldots, \lambda^{d-1}$, donde $\lambda^k(g) = e^{2\pi ik/d}$ son distintos entre ellos, ya que si $\lambda^r = \lambda^n$ con $0 \leq n, r < d$, entonces:

$$\lambda^r(g) = \lambda^n(g) \Rightarrow \lambda(g)^r = \lambda(g)^n \Rightarrow e^{2\pi ir/d} = e^{2\pi in/d} \Rightarrow e^{2\pi i(n-r)/d} = 1,$$

entonces $d|n-r$; pero como $0 \leq n, r < d$ se sigue que $n = r$. Esto demuestra que $d \leq |C(G)|$ y por lo tanto $|C(G)| = d$. Además λ es un generador de este grupo □

Observación 2.2.8. Si, en particular, $G = \mathbb{F}_q^*$, entonces $C(\mathbb{F}_q^*)$ es un grupo cíclico de orden $q-1$

Proposición 2.2.9. *Sea G un grupo cíclico de orden d. Entonces, para cada divisor m de d existe un único subgrupo de G de orden m.*

Demostración. Sea a un generador de G y m un divisor de d. Entonces el grupo generado por $a^{d/m}$ es un subgrupo de orden m. Si H es un subgrupo de orden m, entonces, como G es cíclico, H es cíclico y existe $n \in \mathbb{Z}$ tal que $H = < a^n >$, por lo que $1 = (a^n)^m = a^{nm}$, así, $dk = nm$ para alguna $k \in \mathbb{Z}$, de donde $a^n = (a^{d/m})^k \in < a^{d/m} >$, por lo tanto tenemos que $H = < a^n > \leq < a^{d/m} >$. Como ambos grupos tienen el mismo número de elementos, la igualdad se sigue. □

Corolario 2.2.10. *Si $\mathbb{F}_q$ es el campo finito con q elementos, entonces para cada divisor m de $q-1$, $C(\mathbb{F}_q^*)$ tiene un único subgrupo de orden m. Si λ es un generador de $C(\mathbb{F}_q^*)$, entonces $\lambda^{(q-1)/m}$ genera al subgrupo de orden m*

La demostración es inmediata de la proposición anterior.

Proposición 2.2.11. *Sea H un subgrupo del grupo abeliano finito G y sea ρ un carácter de H. Entonces ρ puede extenderse a un carácter χ de G; esto es, existe un carácter χ de G tal que $\chi(h) = \rho(h)$ para todo $h \in H$.*

Demostración. Si $H = G$, no hay nada por hacer. Supongamos que H es un subgrupo propio de G. Sea $a \in G$ un elemento tal que $a \notin H$. Denotemos por H_1 al subgrupo de G generado por a y H, i.e., $H_1 =< H, a >$.

La idea de la demostración es mostrar que ρ se puede extender a un carácter χ_1 de H_1, de esta manera se seguirá que es posible extenderlo hasta un carácter χ de G en un número finito de pasos.

Sea m el entero positivo más pequeño con la propiedad de que $a^m \in H$. Así, cada elemento $g \in H_1$ se pude escribir en forma única como $g = a^j h$ con $h \in H$ y $0 \leq j < m$; sea $w \in \mathbb{C}$ tal que cumple con $w^m = \rho(a^m)$, i.e., w es una raíz m-ésima de $\rho(a^m)$. Afirmamos que el mapeo $\chi_1 : H_1 \longrightarrow S^1$ definido por $\chi_1(g = a^j h) := w^j \rho(h)$ es un carácter de H_1. Para ver esto, notemos que si $g_1 = a^k h_1$ es otro elemento de H_1 con $0 \leq k < m$ y $h_1 \in H$, entonces $gg_1 = a^{j+k} h h_1$.

Si $j + k < m$, entonces:

$$\chi_1(gg_1) = \chi_1(a^{j+k} h h_1) = w^{j+k} \rho(h h_1) = w^j \rho(h) w^k \rho(h_1) = \chi(g)\chi(g_1).$$

Si $m \leq j + k$, entonces $gg_1 = a^{j+k-m}(a^m h h_1)$, por lo tanto:

$$\begin{aligned} \chi_1(gg_1) &= w^{j+k-m} \rho(a^m h h_1) \\ &= w^j w^k w^{-m} \rho(a^m) \rho(h) \rho(h_1) \\ &= w^j \rho(h) w^k \rho(h_1) 1_{\mathbb{C}} \\ &= \chi_1(g)\chi_1(g_1). \end{aligned}$$

Hemos utilizado que $w^{-m}\rho(a^m) = w^{-m}w^m = 1_{\mathbb{C}}$.

Así, χ_1 es un carácter de H_1 y, claramente, $\chi_1(h) = \rho(h)$ para toda $h \in H$, por lo que χ_1 extiende a ρ. Si $H_1 = G$, hemos terminado; si no, con este mismo argumento podemos extender χ_1 a un carácter χ_2 de un subgrupo H_2 de G, donde $H_2 =< H_1, a_1 >$ con $a_1 \notin H_1$. Como G es finito, este proceso termina en un número finito de pasos y, finalmente, podremos extender ρ a un carácter χ de G. □

Corolario 2.2.12. *Sea $h \in G$ con $h \neq 1_G$, entonces existe $\chi \in C(G)$ tal que $\chi(h) \neq 1_{\mathbb{C}}$.*

Demostración. Sea H el subgrupo de G generado por h. Supongamos que $|H| = d$, como H es cíclico, el carácter λ, definido en la demostración del teorema 2.2.7, nos muestra que $\lambda(h) = e^{2\pi\imath/d} \neq 1_{\mathbb{C}}$ y, por la proposición anterior, este carácter se pude extender a un carácter χ de G, por lo tanto, este carácter χ, cumple lo buscado. □

Corolario 2.2.13. *Sean $h_1 \neq h_2$ elementos de G, entonces existe un carácter $\chi \in C(G)$ tal que $\chi(h_1) \neq \chi(h_2)$.*

Demostración Aplicamos el corolario 2.2.12 para $g := h_1 h_2^{-1} \neq 1_G$, entonces existe $\chi \in C(G)$ tal que $\chi(h_1)\chi(h_2)^{-1} = \chi(h_1)\chi(h_2^{-1}) = \chi(h_1 h_2^{-1}) \neq 1_{\mathbb{C}}$, de donde $\chi(h_1) \neq \chi(h_2)$. □

En nuestro estudio para encontrar el número de soluciones a ecuaciones sobre campos finitos (ver capitulo 3), utilizaremos, como herramientas, sumas y sumas de productos de caracteres, por esta razón es importante que tengamos en cuenta los siguientes teoremas que nos serán de gran utilidad para encontrar este número.

Teorema 2.2.14. Si χ es un carácter no trivial de un grupo abeliano finito G, entonces:

$$\sum_{a \in G} \chi(a) = 0.$$

Demostración. Sea $T = \sum_{a \in G} \chi(a)$. Como χ es no trivial, existe $b \in G$ tal que $\chi(b) \neq 1_{\mathbb{C}}$, entonces:

$$\chi(b)T = \chi(b) \sum_{a \in G} \chi(a) = \sum_{a \in G} \chi(b)\chi(a) = \sum_{a \in G} \chi(ba). \tag{2.3}$$

Como G es un grupo, cuando a varía sobre los elementos de G también lo hace ba, así que la última suma de 2.3 es igual a $\sum_{x \in G} \chi(x) = T$, por lo tanto $\chi(b)T = T$, lo que implica que $T(\chi(b) - 1) = 0$ y como $\chi(b) \neq 1_{\mathbb{C}}$, tenemos que $T = 0$. □

Teorema 2.2.15. Si $a \in G$ (donde G es un grupo abeliano finito) y, además, $a \neq 1_G$. Entonces:

$$\sum_{\chi \in C(G)} \chi(a) = 0.$$

Demostración. Por el corolario 2.2.12, existe un carácter $\rho \in C(G)$ tal que $\rho(a) \neq 1_{\mathbb{C}}$. Sea $T = \sum_{\chi \in C(G)} \chi(a)$. Entonces

$$\rho(a)T = \rho(a) \sum_{\chi \in C(G)} \chi(a) = \sum_{\chi \in C(G)} \rho\chi(a).$$

Como $C(G)$ es un grupo y $\rho(a) \neq 1_{\mathbb{C}}$, cuando χ recorre $C(G)$, también lo hace $\rho\chi$, así que, $\sum_{\chi \in C(G)} \rho\chi(a) = \sum_{\lambda \in C(G)} \lambda(a) = T$, por lo tanto, $T(\rho(a) - 1_{\mathbb{C}}) = 0$ y, entonces, $T = 0$. □

Proposición 2.2.16. *El número de caracteres de un grupo abeliano finito G es igual a $|G|$.*

Demostración. Usando los teoremas anteriores, tenemos que

$$|C(G)| = \sum_{a \in G} \sum_{\chi \in C(G)} \chi(a) = \sum_{\chi \in C(G)} \sum_{a \in G} \chi(a) = |G|.$$

□

Los siguientes teoremas son conocidos como las *relaciones de ortogonalidad* para caracteres.

Sea $\delta(x, y)$ la delta de Kronecker, i.e., $\delta(x, y) = 1$ si $x = y$ y $\delta(x, y) = 0$ si $x \neq y$.

Teorema 2.2.17 (Relaciones de Ortogonalidad).

i) Sean ρ, χ dos caracteres de G. Entonces:

$$\frac{1}{|G|} \sum_{a \in G} \chi(a)\overline{\rho(a)} = \delta(\chi, \rho).$$

ii) Si g, h son elementos de G. Entonces:

$$\frac{1}{|G|} \sum_{\chi \in C(G)} \chi(g)\overline{\chi(h)} = \delta(g, h).$$

Demostración. i) Si $\chi = \rho$, entonces $\chi\overline{\rho} = \varepsilon$ con lo que:

$$\sum_{g \in G} \chi(g)\overline{\rho}(g) = \sum_{g \in G} 1_{\mathbb{C}} = |G|.$$

Si $\chi \neq \rho$, entonces $\chi\overline{\rho} \neq \varepsilon$. Por el teorema 2.2.14:

$$0 = \sum_{g \in G} \chi\overline{\rho}(g) = \sum_{g \subset G} \chi(g)\overline{\rho}(g) = \sum_{g \in G} \chi(g)\overline{\rho(g)}.$$

ii) Si $g = h$, entonces $\chi(g)\overline{\chi(g)} = 1_{\mathbb{C}}$, por lo que, usando la proposición 2.2.16, tenemos:

$$\sum_{\chi \in C(G)} \chi(g)\overline{\chi(g)} = |C(G)| = |G|.$$

Si $g \neq h$, entonces $\chi(g)\overline{\chi(h)} = \chi(g)\chi(h)^{-1} = \chi(g)\chi(h^{-1}) = \chi(gh^{-1})$. Como $gh^{-1} \neq 1_G$, aplicamos el teorema 2.2.15 y, entonces:

$$\sum_{\chi \in C(G)} \chi(g)\overline{\chi(h)} = \sum_{\chi \in C(G)} \chi(gh^{-1}) = 0.$$

□

Como una consecuencia inmediata de lo anterior, tenemos la siguiente aplicación.

Aplicación 2.2.18. Sea G un grupo abeliano finito. Si $f : G^n \longrightarrow G$ es un mapeo del producto cartesiano $G^n = G \times G \times G \times \cdots \times G$ (n factores) en G, entonces el número $N(h)$ de n-tuplas $(g_1, g_2, \ldots, g_n) \in G^n$ que son solución de la ecuación $f(y_1, y_2, \ldots, y_n) = h$ está dado por la fórmula:

$$N(h) = \frac{1}{|G|} \sum_{g_1 \in G} \sum_{g_2 \in G} \cdots \sum_{g_n \in G} \sum_{\chi \in C(G)} \chi(f(g_1, g_2, \ldots, g_n))\overline{\chi(h)}.$$

2.3 Caracteres en $\mathbb{F}_q$

Cuando estamos trabajando con un campo finito $\mathbb{F}_q$, encontramos dos estructuras fundamentales de grupo: el grupo aditivo de $\mathbb{F}_q$, al cual seguiremos denotando por $\mathbb{F}_q$; y al grupo multiplicativo $\mathbb{F}_q^*$. Así, tenemos dos conjuntos de caracteres, uno para cada tipo de estos grupos. En esta sección estudiaremos propiedades particulares de estos dos grupos y traduciremos los resultados generales para nuestro caso de estudio.

Definición 2.3.1. Sea $\mathbb{F}_q$ un campo finito. A los caracteres del grupo aditivo de $\mathbb{F}_q$ los llamaremos *caracteres aditivos* de $\mathbb{F}_q$. A los caracteres de $\mathbb{F}_q^*$ los llamaremos *caracteres multiplicativos* de $\mathbb{F}_q$.

Ejemplo 2.3.2. Sea $\mathbb{F}_s = \mathbb{F}_{p^s}$ una extensión finita (de grado s) del campo finito $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ con p primo. El mapeo $\psi : \mathbb{F}_s \longrightarrow S^1$, $c \longmapsto e^{2\pi i Tr_{\mathbb{F}_s}(c)/p}$ es un carácter aditivo de $\mathbb{F}_s$, donde $Tr_{\mathbb{F}_s}$ es la traza absoluta de $\mathbb{F}_s$, ya que para todo $c_1, c_2 \in \mathbb{F}_s$, $Tr_{\mathbb{F}_s}(c_1 + c_2) = Tr_{\mathbb{F}_s}(c_1) + Tr_{\mathbb{F}_s}(c_2)$ y, por lo tanto, $\psi(c_1 + c_2) = \psi(c_1)\psi(c_2)$

En la proposición siguiente, veremos que el carácter aditivo ψ (del ejemplo anterior) es de gran importancia, ya que cualquier carácter aditivo de $\mathbb{F}_q$ lo podemos escribir en términos de éste.

Proposición 2.3.3. *Sea $b \in \mathbb{F}_q$. La función ψ_b con $\psi_b(c) = \psi(bc)$ es un carácter aditivo de $\mathbb{F}_q$ y cada carácter aditivo de $\mathbb{F}_q$ lo podemos obtener de esta manera.*

Demostración. Primero veamos que ψ_b es, en efecto, un carácter de $\mathbb{F}_q$. Sean $c_1, c_2 \in \mathbb{F}_q$, entonces

$$\psi_b(c_1 + c_2) = \psi(bc_1 + bc_2) = \psi(bc_1)\psi(bc_2) = \psi_b(c_1)\psi_b(c_2).$$

por lo que ψ_b es un carácter aditivo para todo $b \in \mathbb{F}_q$.

Ahora veamos que hay q caracteres del tipo ψ_b con lo que, según la proposición 2.2.16, serán todos. Para lograr esto basta mostrar que si $a \neq b$ entonces $\psi_a \neq \psi_b$. Sean, pues, $a, b \in \mathbb{F}_q$ con $a \neq b$, entonces:

$$\psi_a(c)\psi_b(c)^{-1} = \psi(ac - bc) = \psi((a-b)c).$$

Como $Tr_{\mathbb{F}_q}$ es un mapeo suprayectivo, concluimos que ψ es no trivial. Como $a - b \neq 0$ y $\mathbb{F}_q^*$ es un grupo (multiplicativo), $(a-b)c$ recorre todo $\mathbb{F}_q^*$ cuando c lo hace. Así, existe $c_0 \in \mathbb{F}_q^*$ tal que $\psi((a-b)c_0) \neq 1_{\mathbb{C}}$, por lo que $\psi_a(c_0)\psi_b(c_0)^{-1} \neq 1_{\mathbb{C}}$ y, por lo tanto, $\psi_a \neq \psi_b$. □

Definición 2.3.4. Sea $\mathbb{F}$ un campo finito de característica p y sea $Tr_{\mathbb{F}}$ la traza absoluta de $\mathbb{F}$. Al carácter $\psi : \mathbb{F} \longrightarrow S^1$, $c \longmapsto e^{2\pi i Tr_{\mathbb{F}}(c)/p}$ lo llamaremos *carácter canónico de $\mathbb{F}$.*

Nota 2.3.5. Para evitar confusiones, al carácter idéntico del grupo de caracteres aditivos de $\mathbb{F}_q$ lo denotaremos por ψ_0 (ya que ψ_0 es, en efecto, el carácter tal que $\psi_0(c) = \psi(0c) = e^{2\pi i 0/q} = 1_{\mathbb{C}}$). Al carácter idéntico de $C(\mathbb{F}_q^*)$ lo denotaremos por ε, como en el caso general.

Proposición 2.3.6. *Sea $\mathbb{F}$ un campo finito con q elementos y sea $\mathbb{F}_s$ una extensión finita de $\mathbb{F}$. Denotemos por ψ al carácter canónico de $\mathbb{F}$ y por ϕ al carácter canónico de $\mathbb{F}_s$. Entonces se cumple la siguiente igualdad:*

$$\phi(\beta) = \psi(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta)) \quad \forall \quad \beta \in \mathbb{F}_s.$$

Demostración. Sea $\beta \in \mathbb{F}_s$, entonces:

$$\psi(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta)) = e^{(2\pi i(Tr_{\mathbb{F}}(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta))))/q} = e^{2\pi Tr_{\mathbb{F}_s}(\beta)/q} = \phi(\beta).$$

Hemos utilizado la propiedad de transitividad de la traza expuesta en el teorema 2.1.7. □

Corolario 2.3.7. *Si γ es un carácter aditivo de $\mathbb{F}_s$, entonces existe $b \in \mathbb{F}_s$ tal que $\gamma(\beta) = \psi(Tr_{\mathbb{F}_s/\mathbb{F}}(b\beta))$.*

Demostración. $\gamma(\beta) = \phi_b(\beta)$ para algún $b \in \mathbb{F}_s$, entonces:

$$\gamma(\beta) = \phi_b(\beta) = \phi(b\beta) = \psi(Tr_{\mathbb{F}_s/\mathbb{F}}(b\beta)).$$

□

Corolario 2.3.8. *Si ψ_a es un carácter aditivo de $\mathbb{F}$, entonces ψ'_a es un carácter aditivo $\mathbb{F}_s$, donde $\psi'_a(\beta) = \psi_a(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta))$.*

Demostración. Como $a \in \mathbb{F}$, por el teorema 2.1.6 parte *i)* y la proposición anterior, tenemos que $\psi_a(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta)) = \psi(aTr_{\mathbb{F}_s/\mathbb{F}}(\beta)) = \psi(Tr_{\mathbb{F}_s/\mathbb{F}}(a\beta)) = \phi_a(\beta)$, por lo tanto, $\phi_a(\beta) = \psi'_a(\beta)$.

□

Definición 2.3.9. Sea $\mathbb{F}_s$ una extensión finita del campo $\mathbb{F} = \mathbb{F}_q$ y sea ψ_a un carácter aditivo de $\mathbb{F}$. Al carácter $\psi'_a \in C(\mathbb{F}_s)$ definido por $\psi'_a(\beta) = \psi_a(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta))$, lo llamaremos *carácter derivado* (aditivo) de ψ_a.

Teorema 2.3.10. Sea $\mathbb{F}$ el campo finito con q elementos y $\mathbb{F}_s$, su extensión finita de grado s. Entonces

a) $\psi_a \neq \psi_b \Longrightarrow \psi'_a \neq \psi'_b$;

b) $\psi_a^m = \psi_0 \Longrightarrow \psi_a'^m = \psi_0$,

c) $\psi'_a(c) = \psi_a(c)^s \quad \forall \ c \in \mathbb{F}$.

Demostración. a) Si $\psi_a \neq \psi_b$, entonces existe $c \in \mathbb{F}$ tal que $\psi_a(c) \neq \psi_b(c)$, como $Tr_{\mathbb{F}_s/\mathbb{F}}$ es un mapeo suprayectivo (teorema 2.1.6 parte *i)*), tenemos que existe $\beta \in \mathbb{F}_s$ tal que $Tr_{\mathbb{F}_s/\mathbb{F}}(\beta) = c$, entonces $\psi'_a(\beta) \neq \psi'_b(\beta)$ y, por lo tanto, $\psi'_a \neq \psi'_b$.

b) Para todo $\beta \in \mathbb{F}_s$ tenemos que:

$$\begin{aligned} \psi_a'^m(\beta) &= \psi_a(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta))^m \\ &= \psi_a^m(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta)) \\ &= \psi_0(Tr_{\mathbb{F}_s/\mathbb{F}}(\beta)) \\ &= 1_{\mathbb{C}}. \end{aligned}$$

Por lo tanto, $\psi_a'^m = \psi_0$.

c) Usando el teorema 2.1.6 parte *ii)*, tenemos que $\psi'_a(c) = \psi_a(Tr_{\mathbb{F}_s/\mathbb{F}}(c)) = \psi_a(sc) = \psi_a(c)^s$.

□

De una manera similar, si χ es un carácter multiplicativo de $\mathbb{F}$, entonces χ', definido como $\chi'(\beta) = \chi(N_{\mathbb{F}_s/\mathbb{F}}(\beta))$, es un carácter multiplicativo de $\mathbb{F}_s$. En efecto,

$$\begin{aligned}\chi'(\alpha\beta) &= \chi(N_{\mathbb{F}_s/\mathbb{F}}(\alpha\beta)) \\ &= \chi(N_{\mathbb{F}_s/\mathbb{F}}(\alpha)N_{\mathbb{F}_s/\mathbb{F}}(\beta)) \\ &= \chi(N_{\mathbb{F}_s/\mathbb{F}}(\alpha))\chi(N_{\mathbb{F}_s/\mathbb{F}}(\beta)) \\ &= \chi'(\alpha)\chi'(\beta).\end{aligned}$$

Definición 2.3.11. Sea $\mathbb{F}_s$ una extensión finita del campo $\mathbb{F} = \mathbb{F}_q$ y sea χ un carácter multiplicativo de $\mathbb{F}$. Al carácter $\chi' \in C(\mathbb{F}_s^*)$ definido por $\chi'(\beta) = \chi(N_{\mathbb{F}_s/\mathbb{F}}(\beta))$, lo llamaremos *carácter derivado* (multiplicativo) de χ.

Para este caso, tenemos el teorema análogo al teorema 2.3.10.

Teorema 2.3.12. Sea $\mathbb{F}$ el campo finito con q elementos y $\mathbb{F}_s$, su extensión finita de grado s. Entonces

a) $\chi \neq \rho \Longrightarrow \chi' \neq \rho'$;

b) $\chi^m = \varepsilon \Longrightarrow \chi'^m = \varepsilon$;

c) $\chi'(a) = \chi(a)^s \ \ \forall \ \ a \in \mathbb{F}$.

Demostración. La demostración a este teorema es similar a la demostración el teorema 2.3.10, pero usando las propiedades de la norma expuestas en el teorema 2.1.13. □

Notación 2.3.13. Denotemos por $C_m(\mathbb{K}^*)$ al único subgrupo de caracteres de $C(\mathbb{K}^*)$ tales que su orden es un divisor de m, para el campo finito $\mathbb{K}$.

Corolario 2.3.14. *Sea m un divisor de $q-1$. Si χ varía sobre todos los caracteres multiplicativos de $\mathbb{F}$ tales que su orden es un divisor de m, i.e., $\chi \in C_m(\mathbb{F}_q^*)$, entonces χ' varía sobre todos los caracteres multiplicativos de $\mathbb{F}_s$ cuyo orden es un divisor de m i.e., $\chi' \in C_m(\mathbb{F}_s^*)$*

Demostración Por el corolario 2.2.10, sabemos que $C(\mathbb{F}^*)$ y $C(\mathbb{F}_s^*)$ tienen exactamente m caracteres cuyo orden es un divisor de m. Por lo que estos son $C_m(\mathbb{F}^*)$ y $C_m(\mathbb{F}_s^*)$ respectivamente

En virtud del teorema anterior, el mapeo $(\ )' : C_m(\mathbb{F}^*) \longrightarrow C_m(\mathbb{F}_s^*)$ tal que $\chi \longmapsto \chi'$ es inyectivo, el resultado es inmediato. □

Corolario 2.3.15. *El mapeo* $(\ )' : C_m(\mathbb{F}^*) \longrightarrow C_m(\mathbb{F}_s^*)$ *es un isomorfismo de grupos.*

Demostración. Por el teorema, basta mostrar que $(\chi\lambda)' = \chi'\lambda'$, pero esto es inmediato de la definición del carácter derivado y la definición del producto de caracteres. □

Definición 2.3.16. Al mapeo $(\ )' : C(\mathbb{F}^*) \longrightarrow C(\mathbb{F}_s^*)$ lo llamamos *mapeo derivación* entre los grupos : $C(\mathbb{F}^*)$ y $C(\mathbb{F}_s^*)$. Cuando el dominio y el contra dominio del mapeo queden claros, simplemente llamaremos a este mapeo como *mapeo derivación.*

Para terminar esta sección, dada la importancia que tiene para nosotros los caracteres de $\mathbb{F}_q$, presentaremos un teorema que, en realidad, traduce las propiedades generales de caracteres al caso de caracteres de $\mathbb{F}_q$.

Teorema 2.3.17. a) Sea g un generador de $\mathbb{F}_q^*$. La función λ definida por $\lambda(g^k) = e^{2\pi ik/(q-1)}$ es un carácter multiplicativo de $\mathbb{F}_q$.

b) $C(\mathbb{F}_q^*)$ es un grupo cíclico de orden $q-1$ con generador λ (definido como en a).

c) *Sean* ψ_a, ψ_b *caracteres aditivos de* $\mathbb{F}_q$. *Entonces*

$$\frac{1}{q}\sum_{c\in\mathbb{F}_q} \psi_a(c)\overline{\psi_b(c)} = \delta(a,b).$$

En particular

$$\sum_{c\in\mathbb{F}_q} \psi_a(c) = 0 \quad \text{para todo} \quad a \neq 0.$$

d) Si $c, d \in \mathbb{F}_q$ y ψ_b es un carácter aditivo de $\mathbb{F}_q$, tenemos

$$\frac{1}{q}\sum_{b\in\mathbb{F}_q} \psi_b(c)\overline{\psi_b(d)} = \delta(c,d)$$

e) Si χ, ρ son caracteres multiplicativos de $\mathbb{F}_q$, entonces

$$\frac{1}{q-1}\sum_{c\in\mathbb{F}_q^*}\chi(c)\overline{\rho(c)} = \delta(\chi,\rho).$$

En particular

$$\sum_{c\in\mathbb{F}_q^*}\chi(c) = 0 \quad \text{para} \quad \chi \neq \varepsilon.$$

f) Si $c, d \in \mathbb{F}_q^*$ y χ es un carácter multiplicativo de $\mathbb{F}_q$, entonces:

$$\frac{1}{q-1}\sum_{\chi}\chi(c)\overline{\chi(d)} = \delta(c,d).$$

Demostración. La demostración de este teorema, como ya mencionamos anteriormente, es simplemente la aplicación de los resultados para el caso general, vistos en la sección anterior. □

Ejemplo 2.3.18. Describamos a $C(\mathbb{F}_4^*)$. Como $\mathbb{F}_4^*$ es un grupo cíclico generado por α donde α es una raíz del polinomio $x^2+x+1 \in \mathbb{F}_2$ (ver ejemplo 1.4.16), vemos que podemos definir al carácter multiplicativo χ como $\chi(\alpha) = e^{2\pi i/3}$, sabemos que este carácter es generador de $C(\mathbb{F}_4^*)$ por lo que

$$\begin{array}{llll} \chi(0)=0 & \chi(1)=1 & \chi(\alpha)=e^{2\pi i/3} & \chi(\alpha^2)=e^{4\pi i/3} \\ \chi^2(0)=0 & \chi^2(1)=1 & \chi^2(\alpha)=e^{4\pi i/3} & \chi^2(\alpha^2)=e^{2\pi i/3}. \end{array}$$

Como $\chi^3 = \varepsilon$, tenemos descrito ya a $C(\mathbb{F}_4^*)$.

Ejemplo 2.3.19. Ahora describamos a $C(\mathbb{F}_4)$. Sea ϕ el carácter canónico de $\mathbb{F}_4$, entonces para todo $a \in \mathbb{F}_4$ tenemos que $\phi(a) = e^{2\pi i Tr_{\mathbb{F}_4}(a)/2} = e^{\pi i Tr_{\mathbb{F}_4}(a)}$. Tomando a $\mathbb{F}_4$ como $0, 1, \alpha, \alpha^2$ donde α es como en el ejemplo anterior y considerando los resultados del ejemplo 2.1.9 que dice:

$$Tr_{\mathbb{F}_4}(0) = 0, Tr_{\mathbb{F}_4}(1) = 0, Tr_{\mathbb{F}_4}(\alpha) = 1, Tr_{\mathbb{F}_4}(\alpha^2) = 1;$$

así como el hecho de que todo carácter aditivo de $\mathbb{F}_4$ es de la forma ϕ_a tenemos lo siguiente:

$$\begin{array}{llll} \phi_0(0)=1 & \phi_0(1)=1 & \phi_0(\alpha)=1 & \phi_0(\alpha^2)=1 \\ \phi_1(0)=1 & \phi_1(1)=1 & \phi_1(\alpha)=-1 & \phi_1(\alpha^2)=-1 \\ \phi_\alpha(0)=1 & \phi_\alpha(1)=\phi_1(\alpha)=-1 & \phi_\alpha(\alpha)=\phi_1(\alpha^2)=-1 & \phi_\alpha(\alpha^2)=\phi_1(1)=1 \\ \phi_{\alpha^2}(0)=1 & \phi_{\alpha^2}(1)=-1 & \phi_{\alpha^2}(\alpha)=1 & \phi_{\alpha^2}(\alpha^2)=\phi_1(\alpha)=-1. \end{array}$$

Los dos ejemplos anteriores nos serán de gran utilidad para ilustrar los resultados que obtendremos durante esta tesis.

2.4 Sumas de Gauss

Sean χ y ψ_a caracteres, multiplicativo y aditivo respectivamente, de $\mathbb{F}_q$.

Definición 2.4.1. Definimos a la *suma de Gauss* $g_a(\chi)$ asociada a los caracteres χ y ψ_a como

$$g_a(\chi) := \sum_{c\in\mathbb{F}_q^*} \chi(c)\psi_a(c).$$

Queremos estudiar cómo son las sumas de Gauss para distintos caracteres χ y ψ_a, cómo se relacionan entre sí y, además, qué valores posibles tienen éstas. Empecemos por dar algunas relaciones

Teorema 2.4.2. Sean $a \in \mathbb{F}_q^*$ y $b \in \mathbb{F}_q$, entonces:

$$g_{ab}(\chi) = \overline{\chi(a)}g_b(\chi).$$

Demostración. Si ψ es el carácter canónico de $\mathbb{F}_q$, entonces tenemos que $\psi_{ab}(c) = \psi(abc) = \psi_b(ac)$. Entonces:

$$\begin{aligned} g_{ab}(\chi) &= \sum_{c\in\mathbb{F}_q^*} \chi(c)\psi_{ab}(c) \\ &= \sum_{c\in\mathbb{F}_q^*} \chi(c)\psi_b(ac). \end{aligned} \tag{2.4}$$

Si hacemos $d = ac$, entonces d varía sobre todo $\mathbb{F}_q^*$ cuando c lo hace. Sustituyendo en 2.4 y reordenado la suma, nos queda

$$\begin{aligned} g_{ab}(\chi) &= \sum_{d\in\mathbb{F}_q^*} \chi(da^{-1})\psi_b(d) \\ &= \chi(a^{-1}) \sum_{d\in\mathbb{F}_q^*} \chi(d)\psi_b(d) \\ &= \overline{\chi(a)}g_b(\chi). \end{aligned}$$

Hemos usado la identidad $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$. □

Como consecuencia inmediata tenemos los siguientes corolarios.

Corolario 2.4.3. *Si* $a \neq 0$, *entonces* $g_a(\chi) = \overline{\chi(a)} g_1(\chi)$.

Demostración. Si ponemos $a = a1$ y usamos el teorema, la demostración es inmediata. □

Corolario 2.4.4. $g_{-a}(\chi) = \chi(-1) g_a(\chi)$.

Demostración. Como $-a = (-1)a$, el teorema nos dice que $g_{-a}(\chi) = \overline{\chi(-1)} g_a(\chi)$; pero como $\chi(-1) = \pm 1$, se tiene que $\overline{\chi(-1)} = \chi(-1)$. □

Notación 2.4.5. De ahora en adelante, denotaremos a la suma $g_1(\chi)$ simplemente como $g(\chi)$.

Teorema 2.4.6. $g_a(\overline{\chi}) = \chi(-1)\overline{g_a(\chi)}$

Demostración. Como $\overline{\psi_a(c)} = \psi_a(-c)$ tenemos que:

$$\begin{aligned} \overline{g_a(\chi)} &= \sum_{c \in \mathbb{F}_q^*} \overline{\chi(c)\psi_a(c)} \\ &= \sum_{c \in \mathbb{F}_q^*} \overline{\chi(c)}\psi_a(-c). \end{aligned}$$

Si hacemos $c = -d$, entonces:

$$\begin{aligned} \overline{g_a(\chi)} &= \sum_{d \in \mathbb{F}_q^*} \overline{\chi(-d)}\psi_a(d) \\ &= \overline{\chi(-1)} \sum_{d \in \mathbb{F}_q^*} \overline{\chi}(d)\psi_a(d) \\ &= \chi(-1)^{-1} g_a(\overline{\chi}). \end{aligned}$$

□

El siguiente teorema nos da los valores explícitos de la Suma de Gauss asociada a ciertos caracteres y, además, nos da el valor de la norma para los casos faltantes.

Teorema 2.4.7. a) $g_0(\varepsilon) = q - 1$;

b) $g_a(\varepsilon) = -1$ para $a \neq 0$;

c) $g_0(\chi) = 0$ para $\chi \neq \varepsilon$;

d) Si $\chi \neq \varepsilon$ y $a \neq 0$, entonces $|g_a(\chi)| = q^{1/2}$.

Demostración. a) $g_0(\varepsilon) = \sum_{c\in\mathbb{F}_q^*} \varepsilon(c)\psi_0(c) = \sum_{c\in\mathbb{F}_q^*} 1 = q-1$.

b) $g_a(\varepsilon) = \sum_{c\in\mathbb{F}_q^*} \psi_a(c) = \sum_{c\in\mathbb{F}_q} \psi_a(c) - \psi_a(0)$. Por el teorema 2.3.17 parte *iii)*, sabemos que $\sum_{c\in\mathbb{F}_q} \psi_a(c) = 0$ y como $\psi_a(0) = 1$ se sigue que $g_a(\varepsilon) = -1$.

c) $g_0(\chi) = \sum_{c\in\mathbb{F}_q^*} \chi(c)\psi_0(c) = \sum_{c\in\mathbb{F}_q^*} \chi(c) = 0$. La última igualdad se sigue del teorema 2.3.17 parte *iv)*.

d) La demostración de esta parte la obtendremos calculando de dos maneras diferentes la suma

$$\sum_{a\in\mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)}. \tag{2.5}$$

Desarrollando las sumas tenemos que

$$\begin{aligned} g_a(\chi)\overline{g_a(\chi)} &= \sum_{c\in\mathbb{F}_q^*} \chi(c)\psi_a(c) \sum_{b\in\mathbb{F}_q^*} \overline{\chi(b)\psi_a(b)} \\ &= \sum_{c\in\mathbb{F}_q^*}\sum_{b\in\mathbb{F}_q^*} \chi(c)\overline{\chi(b)}\psi_a(c-b) \end{aligned}$$

entonces

$$\sum_{a\in\mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)} = \sum_{c\in\mathbb{F}_q^*}\sum_{b\in\mathbb{F}_q^*} \chi(c)\overline{\chi(b)} \sum_{a\in\mathbb{F}_q} \psi_a(c-b).$$

Usando el teorema 2.3.17 parte *iii)* y la ecuación $\psi_a(c-b) = \psi_{c-b}(a)$, tenemos que si $c = b$, entonces $\sum_a \psi_a(c-b) = q$ y si $c \neq b$, entonces $\sum_a \psi_a(c-b) = 0$. Por lo tanto:

$$\begin{aligned} \sum_{a\in\mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)} &= \sum_{c\in\mathbb{F}_q^*}\sum_{b\in\mathbb{F}_q^*} \chi(c)\overline{\chi(b)}q\delta(c,b) \\ &= q\sum_{c\in\mathbb{F}_q^*} \chi(c)\overline{\chi(c)} \\ &= q(q-1) \end{aligned} \tag{2.6}$$

Por otro lado, para $a \neq 0$ tenemos que $g_a(\chi)\overline{g_a(\chi)} = \overline{\chi(a)}g(\chi)\chi(a)\overline{g(\chi)} = g(\chi)\overline{g(\chi)} = |g(\chi)|^2$. Como $g_0(\chi) = 0$ para $\chi \neq \varepsilon$, por la parte c) de este teorema tenemos que

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

Comparando con 2.6 nos queda que $|g(\chi)|^2 = q$. Finalmente, por el corolario 2.4.3 tenemos que

$$|g_a(\chi)| = |\overline{\chi(a)}g(\chi)| = |\overline{\chi(a)}||g(\chi)| = |g(\chi)|$$

y la demostración esta completa.

□

Proposición 2.4.8. $g_a(\chi)g_a(\overline{\chi}) = \chi(-1)q$

Demostración. Usando el teorema 2.4.6 y la parte *d)* del teorema 2.4.7, tenemos que

$$\begin{aligned} g_a(\chi)g_a(\overline{\chi}) &= g_a(\chi)\overline{g_a(\chi)}\chi(-1) \\ &= \chi(-1)|g_a(\chi)|^2 = \chi(-1)q. \end{aligned}$$

□

Terminaremos esta sección con unas ecuaciones conocidas como *expansiones de Fourier* para caracteres de un campo finito.

Teorema 2.4.9 (Expansiones de Fourier).
Sea $\mathbb{F}$ el campo finito con q elementos. Entonces:

a) Si χ es un carácter multiplicativo de $\mathbb{F}$, entonces:

$$\chi(c) = \frac{1}{q}\sum_{a\in\mathbb{F}} g_{-a}(\chi)\psi_a(c) \text{ Para todo } c \in \mathbb{F}^*;$$

b) Si $a \in \mathbb{F}$, entonces:

$$\psi_a(c) = \frac{1}{q-1}\sum_{\chi\in C(\mathbb{F}^*)} g_a(\overline{\chi})\chi(c) \text{ Para todo } c \in \mathbb{F}^*$$

Demostración. a) Usando el teorema 2.3.17 *d)*, tenemos que

$$\begin{aligned} \chi(c) &= \sum_{d\in\mathbb{F}^*} \chi(d)\delta(d,c) \\ &= \frac{1}{q}\sum_{d\in\mathbb{F}^*} \chi(d)\sum_{a\in\mathbb{F}} \psi_a(c)\overline{\psi_a(d)} \\ &= \frac{1}{q}\sum_{a\in\mathbb{F}} \psi_a(c)\sum_{d\in\mathbb{F}^*} \chi(d)\psi_{-a}(d) \\ &= \frac{1}{q}\sum_{a\in\mathbb{F}} g_{-a}(\chi)\psi_a(c) \end{aligned}$$

para todo $c \in \mathbb{F}^*$.

b) Usando el teorema 2.3.17 parte *f)*, tenemos:

$$\begin{aligned}\psi_a(c) &= \sum_{d\in\mathbb{F}} \psi_a(d)\delta(d,c) \\ &= \frac{1}{q-1}\sum_{d\in\mathbb{F}} \psi_a(d) \sum_{\chi\in C(\mathbb{F}^*)} \chi(c)\overline{\chi(d)} \\ &= \frac{1}{q-1}\sum_{\chi\in C(\mathbb{F}^*)} \chi(c) \sum_{d\in\mathbb{F}} \psi_a(d)\overline{\chi(d)} \\ &= \frac{1}{q-1}\sum_{\chi\in C(\mathbb{F}^*)} g_a(\overline{\chi})\psi_a(d)\end{aligned}$$

para todo $c \in \mathbb{F}^*$.

□

Este teorema muestra la importancia que tienen las Sumas de Gauss en la transición de la estructura multiplicativa a la estructura aditiva de los caracteres de $\mathbb{F}$.

Nota 2.4.10. Extendamos la definición de carácter multiplicativo a todo $\mathbb{F}_q$ de la siguiente manera:

$$\chi(0) = \begin{cases} 0 & \text{si } \chi \neq \varepsilon. \\ 1 & \text{si } \chi = \varepsilon. \end{cases}$$

Vemos que para $\chi \neq \varepsilon$, podemos considerar a la suma de Gauss $g_a(\chi) = \sum_{c\in\mathbb{F}_q^*} \chi(c)\psi_a(c)$, como una suma sobre todo $\mathbb{F}_q$, i.e., $g_a(\chi) = \sum_{c\in\mathbb{F}_q} \chi(c)\psi_a(c)$.

De ahora en adelante, para $\chi \neq \varepsilon$, consideraremos indistintamente a la suma de Gauss, como suma sobre $\mathbb{F}_q$, o bien, sobre $\mathbb{F}_q^*$, según nos convenga para los cálculos.

2.5 Relación Hasse-Davenport

La demostración de la relación de Hasse-Davenport está estrechamente relacionada con un tipo de series, así que primero estudiaremos a estas series para luego aplicar los resultados al caso que nos interesa

2.5.1 Estudio de la serie $L(z)$

Denotemos por $\Phi \subset \mathbb{F}_q[x]$ al conjunto de todos los polinomios mónicos de $\mathbb{F}_q$ y por Φ_k al subconjunto de Φ, formado por los polinomios mónicos de grado k.

Como cada $f \in \Phi_k$ es de la forma $f = x^k + c_1 x^{k-1} + \cdots + c_k$, se sigue que Φ_k tiene exactamente q^k elementos.

Si $\lambda : \Phi \longrightarrow \mathbb{C}$ es un mapeo multiplicativo, i.e., $\lambda(fg) = \lambda(f)\lambda(g)$ y, además, $|\lambda(f)| \leq 1$ para todo $f \in \Phi$, entonces definimos a la serie de potencias $L(z)$ asociada a λ como:

$$L(z) = \sum_{k=0}^{\infty} \left(\sum_{g \in \Phi_k} \lambda(g) \right) z^k. \tag{2.7}$$

Si a_k es el coeficiente de z^k, entonces $|a_k| \leq q^k$ ya que $|\lambda(f)| \leq 1$, entonces $|a_k| t^k \leq 1$ con $t = q^{-1}$, de donde concluimos que $L(z)$ converge normalmente para $|z| < q^{-1}$. En lo que resta, siempre supondremos que $z \in \{w \in \mathbb{C} : |w| < q^{-1}\}$.

Proposición 2.5.1. $L(z) = \prod_f (1 - \lambda(f) z^{\deg f})^{-1}$. *Donde el producto es sobre todos los polinomios mónicos irreducibles de* $\mathbb{F}_q[x]$.

Demostración. Reordenando a $L(z)$ tenemos que ésta es igual a $\sum_{g \in \Phi} \lambda(g) z^{\deg g}$. Como $\mathbb{F}_q[x]$ es un dominio de factorización única, tenemos que

$$\lambda(g) = \lambda(f_1^{m_1} f_2^{m_2} \cdots f_r^{m_r}) = \lambda(f_1)^{m_1} \lambda(f_1)^{m_2} \cdots \lambda(f_r)^{m_r},$$

donde $f_1, f_2, \ldots, f_r$ son polinomios mónicos irreducibles de $\mathbb{F}_q[x]$. Tenemos las siguientes igualdades:

$$\begin{aligned} \sum_{g \in \Phi} \lambda(g) z^{\deg g} &= \prod_f (1 + \lambda(f) z^{\deg(f)} + \lambda(f^2) z^{\deg(f^2)} + \cdots) \\ &= \prod_f \left(\sum_{n=0}^{\infty} \lambda(f)^n z^{n \deg(f)} \right) \\ &= \prod_f \left(\sum_{n=0}^{\infty} (\lambda(f) z^{\deg(f)})^n \right). \end{aligned} \tag{2.8}$$

Donde el producto es sobre todos los polinomios mónicos irreducibles de $\mathbb{F}_q[x]$. Como $|\lambda(f) z^{\deg(f)}| \leq q^{-\deg(f)} < 1$, entonces la suma en 2.8 es igual a $(1 - \lambda(f) z^{\deg f})^{-1}$, por lo

tanto

$$L(z) = \prod_f (1 - \lambda(f) z^{\deg f})^{-1}$$

□

Si ahora aplicamos logaritmo a $L(z)$, diferenciamos y multiplicamos por z, tenemos la igualdad siguiente.

Corolario 2.5.2. $z\frac{d\log L(z)}{dz} = \sum_{s=1}^{\infty} L_s z^s$ *con* $L_s = \sum_f \deg(f)\lambda(f)^{s/\deg(f)}$, *donde la suma es sobre todos los polinomios mónicos irreducibles de* $\mathbb{F}_q[x]$, *cuyo grado es un divisor de* s.

Demostración. Por la proposición 2.5.1, $L(z) = \prod_f (1 - \lambda(f) z^{\deg f})^{-1}$, así que

$$z\frac{d\log L(z)}{dz} = \sum_f \frac{\lambda(f)\deg(f) z^{\deg(f)}}{1 - \lambda(f) z^{\deg(f)}}. \tag{2.9}$$

Como $\frac{1}{1-\lambda(f)z^{\deg(f)}} = \sum_{n=0}^{\infty} \left[\lambda(f) z^{\deg(f)}\right]^n$, substituimos en 2.9 para obtener:

$$\begin{aligned} z\frac{d\log L(z)}{dz} &= \sum_f \lambda(f)\deg(f) z^{\deg(f)} \sum_{n=0}^{\infty} \left[\lambda(f) z^{\deg(f)}\right]^n \\ &= \sum_f \deg(f) \sum_{n=0}^{\infty} \left[\lambda(f) z^{\deg(f)}\right]^{n+1} \\ &= \sum_f \deg(f) \sum_{n=1}^{\infty} \left[\lambda(f) z^{\deg(f)}\right]^n \\ &= \sum_f \deg(f) \sum_{n=1}^{\infty} \lambda(f)^n z^{n\deg(f)}. \end{aligned}$$

Si $s = n\deg(f)$, entonces el coeficiente de z^s esta determinado por los polinomios mónicos irreducibles, cuyo grado es un divisor de s, y está dado por $\sum_f \deg(f)\lambda(f)^{s/\deg(f)}$. □

Teorema 2.5.3. Supongamos que existe t, tal que $\sum_{g\in\Phi_k} \lambda(g) = 0$ para todo $k > t$ Entonces existen números complejos $w_1, w_2, \ldots, w_t$ (no necesariamente diferentes de cero), tales que

$$L_s = -w_1^s - w_2^s \cdots - w_t^s.$$

Demostración. De la definición de $L(z)$ (ver ecuación 2.7), tenemos que éste es un polinomio de grado menor o igual a t, así, podemos escribirlo como $L(z) = (1 - w_1 z) \cdots (1 - w_2 z)(1 - w_t z)$, donde los w_i, son las raíces recíprocas de $L(z)$ en $\mathbb{C}$. Entonces, para z lo suficientemente pequeño

$$\begin{aligned} z\frac{d\log L(z)}{dz} &= -\sum_{n=1}^{t} \frac{w_n z}{1 - w_n z} \\ &= -\sum_{n=1}^{t} w_n z \sum_{j=0}^{\infty} w_n^j z^j \\ &= \sum_{j=0}^{\infty} \left(\sum_{n=1}^{t} -w_n^{j+1} \right) z^{j+1} \\ &= \sum_{s=1}^{\infty} \left(\sum_{n=1}^{t} -w_n^s \right) z^s. \end{aligned}$$

Comparando con el corolario a la proposición 2.5.1, tenemos lo deseado. □

Observación 2.5.4. Bajo las hipótesis del teorema, vemos que $L(z)$ es un polinomio tal que las w_i son sus raíces recíprocas, i.e., $1/w_i$ es raíz de $L(z)$.

2.5.2 Relación Hasse-Davenport

En la sección 2.3, introducimos los conceptos de caracteres derivados χ' y ψ_a' de $\mathbb{F}_{q^s}$, donde χ y ψ_a son caracteres de $\mathbb{F}_q$ (multiplicativo y aditivo respectivamente). Nuestro objetivo en esta sección es estudiar la relación entre la suma de Gauss $g_a(\chi) = \sum_{c \in \mathbb{F}_q} \chi(c)\psi_a(c)$ y la suma derivada $g_a(\chi') = \sum_{\alpha \in \mathbb{F}_{q^s}} \chi'(\alpha)\psi_a'(\alpha)$.

Denotemos, como en la sección anterior, por Φ al conjunto de los polinomios mónicos de $\mathbb{F}_q$, y por Φ_k a los polinomios mónicos de grado k. Sea $\lambda : \Phi \longrightarrow \mathbb{C}$ el mapeo definido por $\lambda(1) = 1$ y, para $f \neq 1$:

$$\lambda(x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n) = \psi_a(c_1)\chi(c_n),$$

para χ y ψ_a fijos.

Lema 2.5.5. $\lambda(fg) = \lambda(f)\lambda(g)$.

Demostración. Si $f = x^n - c_1x^{n-1} + \cdots + (-1)^n c_n$ y $g = x^m - d_1x^{m-1} + \cdots + (-1)^m d_m$, entonces $fg = x^{n+m} - (c_1 + d_1)x^{n+m-1} + \cdots + (-1)^{n+m}c_n d_m$ y, por lo tanto

$$\begin{aligned}\lambda(fg) &= \psi_a(c_1 + d_1)\chi(c_n d_m) \\ &= \psi_a(c_1)\chi(c_n)\psi_a(d_1)\chi(d_m) \\ &= \lambda(f)\lambda(g).\end{aligned}$$

□

Lema 2.5.6. *Sea* $\alpha \in \mathbb{F}_{q^s}$ *y* $f(x) \in \mathbb{F}_q[x]$, *su polinomio mínimo. Entonces* $\lambda(f)^{s/d} = \chi'(\alpha)\psi'_a(\alpha)$, *donde* $d = \deg f$.

Demostración. Si $g(x) = x^m - c_1x^{m-1} + \cdots + (-1)^m c_m \in \mathbb{F}_q[x]$ es el polinomio característico de α, entonces $g(x) = f(x)^{s/d}$, por lo tanto, $\lambda(g) = \lambda(f^{s/d}) = \lambda(f)^{s/d}$. Por otro lado usando las proposiciones 2 1.4 y 2.1.11, tenemos que $\lambda(g) = \psi_a(c_1)\chi(c_m) = \psi_a(Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha))\chi(N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha))$ con lo que concluimos que $\lambda(f)^{s/d} = \chi'(\alpha)\psi'_a(\alpha)$. □

Como $|\lambda(f)| \leq 1$ para todo $f \in \Phi$, podemos considerar a la serie $L(z)$ asociada a λ, tal y como le hicimos en la subsección anterior y, por lo tanto, considerar a la serie $z\frac{d\log L(z)}{dz} = \sum_{s=1}^{\infty} L_s z^s$. Tenemos el siguiente e importante resultado.

Lema 2.5.7. $L_s = g_a(\chi')$.

Demostración Si $f(x)$ es un polinomio mónico irreducible de $\mathbb{F}_q[x]$, cuyo grado es un divisor de s, entonces para cualquier raíz α de f, sabemos que $\lambda(f)^{s/d} = \chi'(\alpha)\psi'_a(\alpha)$, por lo tanto $d\lambda(f)^{s/d} = \sum_{i=1}^{d} \chi'(\alpha_i)\psi'_a(\alpha_i)$, donde d es el grado de f y $\alpha_1, \alpha_2, \ldots, \alpha_d$ son sus raíces.

Usando la proposición 1.4.20 del capítulo 1, que dice: el polinomio $x^{q^s} - x$ es el producto de todos los polinomios mónicos irreducibles de $\mathbb{F}_q[x]$ cuyo grado es un divisor de s; tenemos que cada tal polinomio irreducible tiene a todas sus raíces en $\mathbb{F}_{q^s}$, y conversamente, cada elemento en $\mathbb{F}_{q^s}$ es raíz de uno, y sólo uno de tales polinomios (recordemos que $\mathbb{F}_{q^s}$ es el

campo de descomposición de $x^{q^s} - x$). Así, tenemos que

$$\begin{aligned} L_s &= \sum_f \deg(f)\lambda(f)^{s/\deg(f)} \\ &= \sum_f \left(\sum_{i=1}^{\deg(f)} \chi'(\alpha_i)\psi'_a(\alpha_i) \right) \\ &= \sum_{\alpha \in \mathbb{F}_{q^s}} \chi'(\alpha)\psi'_a(\alpha) \\ &= g_a(\chi'). \end{aligned}$$

Donde las primeras sumas son sobre todos los polinomios mónicos irreducibles, cuyo grado es un divisor de s. □

Ahora juntemos todos estos resultados para demostrar el teorema que le da el nombre a este capítulo.

Teorema 2.5.8 (Relación Hasse-Davenport). Sean χ' y ψ'_a los caracteres de $\mathbb{F}_{q^s}$, derivados de $\chi \in C(\mathbb{F}_q^*)$ y $\psi_a \in C(\mathbb{F}_q)$ respectivamente. Entonces

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

Demostración. Lo que haremos para demostrar este teorema es ver que $L(z) = 1 + g_a(\chi)$, con lo que, usando el teorema 2.5.3 y la observación que le precede, se seguirá que $L_s = -(-g_a(\chi))^s$ y, comparando con el lema 2.5.7, se tendrá la relación buscada.

Si $k > 1$, entonces $\sum_{g \in \Phi_k} \lambda(g) = 0$. En efecto, $\lambda(x^k - c_1 x^{k-1} + \cdots + (-1)^k c_k) = \psi_a(c_1)\chi(c_k)$, con lo que cada par (c_1, c_k) aparece q^{k-2} veces en los polinomios de Φ_k, entonces:

$$\begin{aligned} \sum_{g \in \Phi_k} \lambda(g) &= \sum_{(c_1,c_k)} \lambda(x^k - c_1 x^{k-1} + \cdots + (-1)^k c_k) \\ &= q^{k-2} \sum_{(c_1,c_k)} \psi_a(c_1)\chi(c_k) \\ &= q^{k-2} \left(\sum_{c_1} \psi_a(c_1) \right) \left(\sum_{c_k} \chi(c_k) \right) \\ &= 0. \end{aligned}$$

Hemos usado el teorema 2.3.17 parte *c)*, o bien, parte *e)*. Así:

$$\begin{aligned} L(z) &= \sum_{k=0}^{\infty} \left(\sum_{g \in \Phi_k} \lambda(g) \right) z^k \\ &= 1 + \sum_{g \in \Phi_1} \lambda(g) z \\ &= 1 + \sum_{c_1 \in \mathbb{F}_q} \lambda(x - c_1). \end{aligned}$$

Pero, como $\sum_{c_1 \in \mathbb{F}_q} \lambda(x - c_1) = \sum_{c_1 \in \mathbb{F}_q} \psi_a(c_1)\chi(c_1) = g_a(\chi)$, tenemos que $L(z) = 1 + g_a(\chi)z$, con lo que $-g_a(\chi)$ es la *raíz recíproca* de $L(z)$. Usando el teorema 2.5.3, la observación que le precede y el lema 2.5 7 tenemos que:

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

□

Ejemplo 2.5.9. Tomemos $C(\mathbb{F}_4^*) = \{\chi, \chi^2, \varepsilon\}$ y $\phi = \phi_1 \in C(\mathbb{F}_4)$ como en los ejemplos 2.3.19 y 2.3 18 en la página 2.3.18. Como

$$\chi(0) = 0,\ \chi(1) = 1,\ \chi(\alpha) = e^{2\pi\imath/3},\ \chi(\alpha^2) = e^{4\pi i/3}$$

y

$$\phi_1(0) = 1,\ \phi_1(1) = 1,\ \phi_1(\alpha) = -1,\ \phi_1(\alpha^2) = -1,$$

tenemos que

$$\begin{aligned} g(\chi) &= \sum_{a \in \mathbb{F}_4} \chi(a)\phi(a) \\ &= \chi(0)\phi(0) + \chi(1)\phi(1) + \chi(\alpha)\phi(\alpha) + \chi(\alpha^2)\phi(\alpha^2) \\ &= 0 + 1 + e^{2\pi\imath/3}(-1) + e^{4\pi\imath/3}(-1) \\ &= 1 - (e^{2\pi\imath/3} + e^{4\pi\imath/3}) \\ &= 1 - 2\Re(e^{2\pi\imath/3}) = 1 + 2(1/2) \\ &= 2. \end{aligned}$$

Como $\chi^2 = \overline{\chi}$ y $g(\overline{\chi}) = \chi(-1)g(\chi)$, encontramos que $g(\chi^2) = g(\chi) = 2$ ya que $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = \varepsilon(-1) = 1$. Finalmente, como $g_a(\chi) = \overline{\chi(a)}g(\chi)$ para $a \neq 0$ (corolario 2.4.3 página 2.4.3), vemos que podemos encontrar los valores de todas las posibles sumas de Gauss definidas sobre $\mathbb{F}_4$.

Ejemplo 2.5.10. Si $\mathbb{F}_{4^s}$ es la extensión finita de $\mathbb{F}_4$ de grado s, entonces tenemos al mapeo derivación $(\ )' : C(\mathbb{F}_4^*) \longrightarrow C(\mathbb{F}_{4^s}^*)$, así, por el ejemplo anterior y la relación de Hasse-Davenport (teorema anterior), tenemos que

$$-g(\chi') = (-g(\chi))^s = (-1)^s 2^s,$$

así que $g(\chi') = (-1)^{s+1}2^s$.

Capítulo 3

NÚMERO DE PUNTOS RACIONALES

En este capítulo daremos una fórmula para el número de ceros en $\mathbb{F}_{q^s}$, de la función polinomial de la forma

$$f = a_1 x_1^{l_1} + a_2 x_2^{l_2} + \cdots + a_n x_n^{l_n} - b \tag{3.1}$$

donde $a_1, a_2, \ldots, a_n, b$ están en $\mathbb{F}_q$. Por supuesto, estamos considerando a $\mathbb{F}_{q^s}$ como una extensión de $\mathbb{F}_q$ de grado s.

Dicho de otra manera, queremos dar una fórmula para $N_s(f) = |H_f(\mathbb{F}_{q^s})|$, i.e., el número de puntos $\mathbb{F}_{q^s}$-racionales de cualquier hipersuperficie (afín) de la forma $H_f(\overline{\mathbb{F}}_q)$ donde $a_1, a_2, \ldots, a_n, b$ están en $\mathbb{F}_q$.

Una vez teniendo esta fórmula, daremos una estimación para $N_s(f)$ que, en particular, nos ayudará para mostrar la existencia de soluciones para 3.1 en casos concretos.

3.1 La hipersuperficie $H_{x^l-a}(\overline{\mathbb{F}}_q)$

Como caso particular del polinomio 3.1 tenemos a $x^l - a$, con $a \in \mathbb{F}_q \subset \mathbb{F}_{q^s} \subset \overline{\mathbb{F}_q}$. Como veremos más adelante, estudiar el número de soluciones para este caso será de gran utilidad para estudiar el caso general de la ecuación 3 1

Tomemos al polinomio $x^l - a \in \mathbb{F}_q[x]$ y sea $H_{x^l-a}(\overline{\mathbb{F}}_q) \subset \mathbb{A}^1$ la hipersuperficie determinada por este polinomio.

Queremos saber bajo qué condiciones esta hipersuperficie tiene puntos $\mathbb{F}_{q^s}$-racionales y, de tener, cuántos hay de ellos. Notemos que esto es equivalente a decir cuándo la ecuación

$$x^l = a \tag{3.2}$$

tiene solución en $\mathbb{F}_{q^s}$ y, de tener solución, cuántas de ellas son distintas.

Nota 3.1.1. Por los resultados del capítulo 1 podemos considerar a $\mathbb{F}_{q^s}$ único, en el sentido de que si $\mathbb{K}$ es una extensión de $\mathbb{F}_q$ de grado s, entonces $\mathbb{K} \cong \mathbb{F}_{q^s}$.

Denotemos por $\mathbb{F}_{q^s}^*$ al grupo de las unidades de $\mathbb{F}_{q^s}$. Como $\mathbb{F}_{q^s}$ es finito, entonces también lo es su grupo de unidades. Sea $m = |\mathbb{F}_{q^s}^*| = q^s - 1$.

Proposición 3.1.2. *Tomemos $a \in \mathbb{F}_q^*$. La ecuación $x^l = a$ tiene solución en $\mathbb{F}_{q^s}$, si y sólo si $a^{m/d} = 1$, con $d = (m, l)$.*

Demostración. Por el teorema 1.1.12 sabemos que $\mathbb{F}_{q^s}^*$ es un grupo cíclico. Si g es un generador de $\mathbb{F}_{q^s}^*$, como $a \in \mathbb{F}_q^* \subset \mathbb{F}_{q^s}^*$, existe $r < q^s \in \mathbb{Z}$ tal que $a = g^r$. Pongamos $x = g^y$ con y indeterminada. Así, dar solución a 3.2 es equivalente a resolver $g^{ly} = g^r$ en $\mathbb{F}_{q^s}^*$, que a su vez es equivalente a resolver la congruencia:

$$ly \equiv r (\mathrm{mod}\, m). \tag{3.3}$$

Observación 3.1.3. Sabemos que la congruencia 3.3 tiene solución si y sólo si $d|r$ y de tener solución, tiene d soluciones distintas.

Supongamos que 3.2 tiene solución, entonces $ly \equiv r (\mathrm{mod}\, m)$ también, y por lo tanto, existe $y_0 \in \mathbb{Z}$ tal que $g^{ly_0} = g^r = a$ en $\mathbb{F}_{q^s}^*$. Así

$$a^{m/d} = g^{\frac{(ly_0)m}{d}} = g^{(l/d)y_0 m} = 1; \text{ ya que } \frac{l}{d} \in \mathbb{Z} \text{ y } g^m = 1.$$

Ahora supongamos que $a^{m/d} = 1$, entonces $g^{rm/d} = 1 = g^0$ en $\mathbb{F}_{q^s}^*$, y entonces

$$rm/d \equiv 0 (\mathrm{mod}\, m) \Rightarrow m | \frac{mr}{d} \Rightarrow d|r,$$

por la observación 3.1.3, la congruencia 3.3 tiene solución y, por lo tanto, $x^l = a$ es soluble. □

De la demostración anterior, tenemos el siguiente corolario:

Corolario 3.1.4. *Si $a \in \mathbb{F}_q^* \subset \mathbb{F}_{q^s}^*$ y si $x^l = a$ tiene solución, entonces hay d soluciones distintas. Donde $d = (l, m)$.*

Nota 3.1.5. si $a = 0$, tenemos que $x^l = a$ sólo tiene una solución: la solución trivial.

En resumen, tenemos el siguiente teorema

Teorema 3.1.6. Si $H := H_{x^l-a}(\overline{\mathbb{F}}_q) \subset \mathbb{A}(\overline{\mathbb{F}}_q)$ con $a \in \mathbb{F}_q$ entonces:

1. Si $a = 0$, H sólo tiene un punto $\mathbb{F}_{q^s}$-racional y es el 0.
2. Si $a \neq 0$, H tiene puntos $\mathbb{F}_{q^s}$-racionales si, y sólo si, $a^{m/d} = 1$ en $\mathbb{F}_{q^s}$. Donde $m = |\mathbb{F}_{q^s}^*|$ y $d = (m, l)$. Si H tiene puntos $\mathbb{F}_{q^s}$-racionales, entonces tiene exactamente d de ellos.

Ahora que ya hemos determinado el número $N_s(x^l - a)$ de puntos $\mathbb{F}_{q^s}$-racionales; daremos una expresión para $N_s(x^l - a)$ en términos de caracteres, lo que nos ayudará a manipular estos números.

Lema 3.1.7. *Si $a \in \mathbb{F}_q^*$ y $H_{x^l-a}(\overline{\mathbb{F}}_q)$ no tiene puntos $\mathbb{F}_{q^s}$-racionales, entonces existe un carácter $\chi^{(s)} \in C(\mathbb{F}_{q^s}^*)$ (ver página 38) tal que*

a) $(\chi^{(s)})^d = \varepsilon$. Donde $d = (m, l)$ y $m = |\mathbb{F}_{q^s}^*| = q^s - 1$.

b) $\chi^{(s)}(a) \neq 1$.

Demostración. Sea g un generador de $\mathbb{F}_{q^s}^*$ y sea λ el generador de $C(\mathbb{F}_{q^s}^*)$ tal que $\lambda(g^k) = e^{2\pi i(k/m)}$; tal como en el teorema 2.3.17 parte a). Pongamos $\chi^{(s)} = \lambda^{m/d}$. Entonces

$$\chi^{(s)}(g) = \lambda^{m/d}(g) = \lambda(g)^{m/d} = e^{2\pi i/d}.$$

Como $a = g^r$, para alguna $r \in \mathbb{Z}$ y $x^l - a$ no es soluble, debemos tener que d no divide a r, (ver demostración de proposición 3.1.2). Entonces:

$$\chi^{(s)}(a) = (\chi^{(s)}(g))^r = e^{2\pi i(r/d)} \neq 1.$$

Además $(\chi^{(s)})^d = (\lambda)^m = \varepsilon$ ya que $C(\mathbb{F}_{q^s}^*)$ es un grupo cíclico de orden m. □

Teorema 3.1.8.

$$N_s(x^l - a) = \sum_{(\chi^{(s)})^d = \varepsilon} \chi^{(s)}(a).$$

Donde la suma es sobre todos los caracteres cuyo orden es un divisor de d.

Demostración. Si $a = 0$, entonces $x^l - 0$ sólo tiene una solución, $x = 0$, por lo tanto H sólo tiene un punto $\mathbb{F}_{q^s}$-racional. Ahora

$$\sum_{(\chi^{(s)})^d=\varepsilon} \chi^{(s)}(0) = 1$$

ya que $\varepsilon(0) = 1$ y $\chi^{(s)}(0) = 0$ para cualquier otro carácter $\chi^{(s)} \neq \varepsilon$.

Si $a \neq 0$ y H no tiene puntos $\mathbb{F}_{q^s}$-racionales, por el lema 3.1.7, existe un carácter ρ cuyo orden es un divisor de d, tal que $\rho(a) \neq 1$. Sea $T = \sum_{(\chi^{(s)})^d=\varepsilon} \chi^{(s)}(a)$, entonces

$$\rho(a)T = \rho(a) \sum_{(\chi^{(s)})^d=\varepsilon} \chi^{(s)}(a) = \sum_{(\chi^{(s)})^d=\varepsilon} \rho(a)\chi^{(s)}(a) = \sum_{(\chi^{(s)})^d=\varepsilon} \rho\chi^{(s)}(a) = T. \tag{3.4}$$

De donde $T(\rho(a) - 1) = 0$, y entonces $T = 0$. La última igualdad en 3.4 se sigue gracias a que el orden de $\rho\chi^{(s)}$ es un divisor de d, y $\rho\chi^{(s)}$ varía sobre todos estos caracteres cuando $\chi^{(s)}$ lo hace.

Finalmente, Por el corolario 2.2.10 sabemos que hay exactamente d caracteres cuyo orden es un divisor de d. Así, si $a \neq 0$ y H tiene d puntos $\mathbb{F}_{q^s}$-racionales, tenemos que la ecuación $x^l = a$ tiene solución en $\mathbb{F}_{q^s}$. Sea $b \in \mathbb{F}_{q^s}$ tal que $b^l = a$, entonces

$$\sum_{(\chi^{(s)})^d=\varepsilon} \chi^{(s)}(a) = \sum_{(\chi^{(s)})^d=\varepsilon} \chi^{(s)}(b^l) = \sum_{(\chi^{(s)})^d=\varepsilon} (\chi^{(s)}(b))^l = \sum_{(\chi^{(s)})^d=\varepsilon} 1 = d.$$

Lo último gracias a que $d|l$, y entonces $(\chi^{(s)}(b))^l = 1$. □

Corolario 3.1.9. $N_s(x^l - a) = N_s(x^d - a)$.

Demostración. Como $d = (m, l)$, se tiene que $d = (d, l)$ y, por lo tanto:

$$N_s(x^d - a) = \sum_{(\chi^{(s)})^d=\varepsilon} \chi^{(s)}(a) = N_s(x^l - a).$$

□

Observación 3.1.10. En realidad, para obtener los resultados de esta sección, no hemos utilizado que $a \in \mathbb{F}_q$, i.e., todos los resultados anteriores son igualmente válidos si tomamos $a \in \mathbb{F}_{q^s}$.

3.2 Sumas de Jacobi

En la sección 3.4 veremos que las sumas de Jacobi, que definiremos en esta sección, están estrechamente relacionadas con la fórmula que daremos para $N_s(f)$; sin embargo, para facilitar la exposición, en esta sección presentaremos las propiedades que usaremos para dicho fin

Denotemos por $L_0(t) \subset \mathbb{A}^n(\mathbb{F}_{q^s})$, al conjunto de los puntos $\mathbb{F}_{q^s}$-racionales de la hipersuperficie:

$$H_{t_1+t_2+\cdots+t_n} \subset \mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}}_q);$$

y por $L(t) \subset \mathbf{A}^n(\mathbb{F}_{q^s})$ al conjunto de los puntos $\mathbb{F}_{q^s}$-racionales de la hipersuperficie

$$H_{t_1+t_2+\ \ +t_n-1} \subset \mathbb{A}^n.$$

Proposición 3.2.1. $|L_0(t)| = |L(t)| = q^{s(n-1)}$.

Demostración. Si tomamos $t_1, \ldots, t_{n-1}$ elementos cualesquiera de $\mathbb{F}_{q^s}$, entonces t_n queda completamente determinado para cumplir con la ecuación $t_1 + t_2 + \cdots + t_n = 0$, o bien, con la ecuación $t_1 + t_2 + \ \ \cdot + t_n = 1$. Como en $\mathbb{F}_{q^s}$ hay q^s elementos, tenemos

$$|L_0(t)| = q^{s(n-1)} = |L(t)|.$$

□

Definición 3.2.2. Sean $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$ caracteres multiplicativos de $\mathbb{F}_{q^s}$.

i) Una *Suma de Jacobi* está dada por la fórmula

$$\begin{aligned} J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) &= \sum_{L(t)} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n) \\ &= \sum_{t_1+t_2+\cdots+t_n=1} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n). \end{aligned}$$

Donde la suma es sobre todas las n-adas $(t_1, \ \ldots, t_n) \in L(t)$.

ii) Una *Suma-cero de Jacobi* esta dada por la fórmula

$$\begin{aligned} J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) &= \sum_{L_0(t)} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n) \\ &= \sum_{t_1+t_2+\cdots+t_n=0} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n). \end{aligned}$$

Donde la suma es sobre todas las n-adas $(t_1, \ldots, t_n) \in L_0(t)$.

Observación 3.2.3. Para cualquier permutación ρ de $\{1,\dots,n\}$ se cumple que

$$J(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_n^{(s)}) = J(\chi_{\rho(1)}^{(s)},\chi_{\rho(2)}^{(s)},\dots,\chi_{\rho(n)}^{(s)})$$

y que

$$J_0(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_n^{(s)}) = J_0(\chi_{\rho(1)}^{(s)},\chi_{\rho(2)}^{(s)},\dots,\chi_{\rho(n)}^{(s)}).$$

Proposición 3.2.4. *i)* $J_0(\varepsilon,\varepsilon,\dots,\varepsilon) = J(\varepsilon,\varepsilon,\dots,\varepsilon) = q^{s(n-1)}$.

ii) Si algunos de los $\chi_i^{(s)}$ *son triviales, pero no todos. Entonces* $J_0(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_n^{(s)}) = J(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_n^{(s)}) = 0$.

iii) Supongamos que $\chi_n^{(s)} \neq \varepsilon$. *Entonces*

$$J_0(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_n^{(s)}) = \begin{cases} 0, & \text{si } \prod_{i=1}^n \chi_i^{(s)} \neq \varepsilon \\ \chi_n^{(s)}(-1)(q^s-1)J(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_{n-1}^{(s)}), & \text{en otro caso.} \end{cases}$$

Demostración. i) $J(\varepsilon,\dots,\varepsilon) = \sum_{L(t)} \varepsilon(t_1)\cdots\varepsilon(t_n) = \sum_{L(t)} 1 = |L(t)| = q^{s(n-1)}$. Análogo para $J_0(\varepsilon,\dots,\varepsilon)$.

ii) Por la observación 3.2.3 podemos suponer que $\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_r^{(s)}$ no son triviales y que $\chi_{r+1}^{(s)} = \chi_{r+2}^{(s)} = \cdots = \chi_n^{(s)} = \varepsilon$. Tenemos que:

$$\begin{aligned} J(\chi_1^{(s)},\chi_2^{(s)},\dots,\chi_n^{(s)}) &= \sum_{t_1+t_2+\cdots+t_n=1} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n) \\ &= \sum_{t_1,t_2,\dots,t_{n-1}} \chi_1^{(s)}(t_1)\cdots\chi_r^{(s)}(t_r)\varepsilon(t_{r+1})\cdots\varepsilon(1-t_1-t_2-\cdots-t_{n-1}) \\ &= \sum_{t_1,t_2,\dots,t_{n-1}} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_r^{(s)}(t_r)1 \\ &= \left(\sum_{t_1}\chi_1^{(s)}(t_1)\right)\left(\sum_{t_2}\chi_1^{(s)}(t_2)\right)\cdots\left(\sum_{t_r}\chi_r^{(s)}(t_r)\right)\left(\sum_{t_{r+1},\dots,t_{n-1}} 1\right) \\ &= \left(\sum_{t_1}\chi_1^{(s)}(t_1)\right)\left(\sum_{t_2}\chi_2^{(s)}(t_2)\right)\cdots\left(\sum_{t_r}\chi_r^{(s)}(t_r)\right) q^{s(n-r-1)} = 0. \end{aligned}$$

Hemos usado el teorema 2.3.17 que dice que $\sum_{t_i}\chi_i^{(s)}(t_i) = 0$.

Para la Suma-cero de Jacobi, la demostración es totalmente análoga.

iii) Si $t_1 + t_2 + \cdots + t_n = 0$, pongamos $w = t_n = -t_1 - t_2 - \cdots - t_{n-1}$. Si hacemos variar w en $\mathbb{F}_{q^s}$, tenemos que

$$J_0(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = \sum_{L_0(t)} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(w)$$

$$= \sum_w \left(\sum_{t_1+\cdots+t_{n-1}=-w} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_{n-1}^{(s)}(t_{n-1}) \right) \chi_n^{(s)}(w). \tag{3.5}$$

Si $w = 0$, entonces $\chi_n^{(s)}(w) = 0$ y por lo tanto podemos suponer que $w \neq 0$.

Pongamos atención en la suma interna de 3.5:

$$\sum_{t_1+\cdots+t_{n-1}=-w} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_{n-1}^{(s)}(t_{n-1}) \tag{3.6}$$

Como $w \neq 0$, la ecuación $t_i = -wt_i'$, tiene solución en $\mathbb{F}_{q^s}$ para t_i'. Sustituyendo en 3.6 nos queda

$$\sum_{t_1+\cdots+t_{n-1}=-w} \chi_1^{(s)}(t_1)\cdots\chi_{n-1}^{(s)}(t_{n-1}) = \sum_{t_1'+\cdots+t_{n-1}'=1} \chi_1^{(s)}(-wt_1')\cdots\chi_{n-1}^{(s)}(-wt_{n-1}')$$

$$= \chi_1^{(s)}\cdots\chi_{n-1}^{(s)}(-w) \sum_{t_1'+\cdots+t_{n-1}'=1} \chi_1^{(s)}(t_1')\cdots\chi_{n-1}^{(s)}(t_{n-1}')$$

$$= \chi_1^{(s)}\cdots\chi_{n-1}^{(s)}(-1)\chi_1^{(s)}\cdots\chi_{n-1}^{(s)}(w)J(\chi_1^{(s)},\ldots,\chi_{n-1}^{(s)}).$$

Poniendo esto en 3 5, vemos que $J_0(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)})$ es igual a

$$\sum_w \left[\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)}(-1)\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)}(w)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)})\right]\chi_n^{(s)}(w)$$

$$= \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)}(-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}) \sum_w \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(w). \tag{3.7}$$

Si $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} \neq \varepsilon$ entonces, por el teorema 2.3.17 parte e), la suma en 3.7 es igual a cero Si $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$ entonces $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)} = (\chi_n^{(s)})^{-1} = \overline{\chi_n^{(s)}}$, y tenemos que

$$\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)}(-1) = (\chi_n^{(s)})^{-1}(-1) = \chi_n^{(s)}((-1)^{-1}) = \chi_n^{(s)}(-1).$$

Sustituyendo en 3.7 nos queda

$$J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = \chi_n^{(s)}(-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}) \sum_w \varepsilon(w)$$

$$= \chi_n^{(s)}(-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)})(q^s - 1).$$

□

3.3 Relación entre sumas de Gauss y sumas de Jacobi

La relación entre las Sumas de Gauss y las Sumas de Jacobi que a continuación presentaremos, además de ser muy interesante por sí misma, nos ayudará a estimar el valor de $N_s(f)$.

Teorema 3.3.1. Supongamos que $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$ son caracteres no triviales de $\mathbb{F}_{q^s}^*$ y que $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}$ tampoco es trivial. Tomemos a la suma de Gauss $g(\chi^{(s)})$. Entonces

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)})g(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}).$$

Demostración.

$$\begin{aligned} g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) &= \left(\sum_{t_1}\chi_1^{(s)}(t_1)\psi(t_1)\right)\cdots\left(\sum_{t_n}\chi_n^{(s)}(t_n)\psi(t_n)\right) \\ &= \sum_{t_1,t_2,\ldots,t_n}\chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n)\psi(t_1+t_2+\cdots+t_n). \end{aligned}$$

Si tomamos $w = t_1 + t_2 + \cdots + t_n$, hacemos variar w en $\mathbb{F}_{q^s}$ y agrupamos términos respecto a w, tenemos

$$\begin{aligned} g(\chi_1^{(s)})\cdots g(\chi_n^{(s)}) &= \sum_w\left(\sum_{t_1+\cdots+t_n=w}\chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n)\right)\psi(w) \\ &= J_0(\chi_1^{(s)},\ldots,\chi_n^{(s)})\psi(0) + \sum_{w\neq 0}\left(\sum_{t_1+\cdots+t_n=w}\chi_1^{(s)}(t_1)\cdots\chi_n^{(s)}(t_n)\right)\psi(w). \end{aligned} \tag{3.8}$$

Para $w \neq 0$, hagamos la sustitución $t_i = wt_i'$, entonces la suma interna de 3.8, se convierte en

$$\begin{aligned} \sum_{t_1+t_2+\cdots+t_n=w}\chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\cdots\chi_n^{(s)}(t_n) &= \chi_1^{(s)}\cdots\chi_n^{(s)}(w)\sum_{t_1'+t_2'+\cdots+t_n'=1}\chi_1^{(s)}(t_1')\chi_2^{(s)}(t_2')\cdots\chi_n^{(s)}(t_n') \\ &= \chi_1^{(s)}\cdots\chi_n^{(s)}(w)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}). \end{aligned}$$

Poniendo esto en 3.8 obtenemos

$$g(\chi_1^{(s)})\cdots g(\chi_n^{(s)}) = J_0(\chi_1^{(s)},\ldots,\chi_n^{(s)}) + J(\chi_1^{(s)},\ldots,\chi_n^{(s)})\sum_{w\neq 0}\chi_1^{(s)}\cdots\chi_n^{(s)}(w)\psi(w). \tag{3.9}$$

Como estamos suponiendo que $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} \neq \varepsilon$, por la proposición 3.2.4 parte *iii)*, se cumple que $J_0(\chi_1^{(s)},\ldots,\chi_n^{(s)}) = 0$. Como $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(0) = 0$, entonces

$$\sum_{w\neq 0}\chi_1^{(s)}\cdots\chi_n^{(s)}(w)\psi(w) = \sum_{w}\chi_1^{(s)}\cdots\chi_n^{(s)}(w)\psi(w) = g(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}).$$

Poniendo esto en 3.9 nos queda

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)})g(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}).$$

□

Corolario 3.3.2. *Supongamos que $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$ no son triviales; pero $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}$ sí lo es. Entonces*

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = \chi_n^{(s)}(-1)q^s J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}).$$

Demostración. Observemos que $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)} \neq \varepsilon$. Aplicando el teorema anterior

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_{n-1}^{(s)}) = J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)})g(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)}).$$

Multiplicando ambos lados de la igualdad por $g(\chi_n^{(s)})$

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)})g(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)})g(\chi_n^{(s)}). \qquad (3.10)$$

Como $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$, entonces $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_{n-1}^{(s)} = (\chi_n^{(s)})^{-1} = \overline{\chi_n^{(s)}}$, y por la proposición 2.4.8 $g(\chi_n^{(s)})g(\overline{\chi_n^{(s)}}) = \chi_n^{(s)}(-1)q^s$. Sustituyendo en 3.10

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = \chi_n^{(s)}(-1)q^s J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}).$$

□

Corolario 3.3.3. *Supongamos que $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$ no son triviales; pero $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}$ sí lo es. Entonces:*

$$J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = -\chi_n^{(s)}(-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}).$$

Además, suponemos que $J(\chi^{(s)}) = 1$.

Demostración. Por la ecuación 3.9, en la demostración al teorema 3.3.1, que también es válida en este caso, tenemos que $g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)})$ es igual a

$$J_0(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) + J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)})\sum_{w\neq 0}\psi(w), \tag{3.11}$$

ya que $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$.

Por el teorema 2.3.17 parte *c)* sabemos que $\sum_w \psi(w) = 0$, y como $\psi(0) = 1$, tenemos que $\sum_{w\neq 0}\psi(w) = -1$. Por la proposición 3.2.4 parte *iii)* tenemos

$$J_0(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = \chi_n^{(s)}(-1)(q^s-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)});$$

juntando esto con 3.11 nos queda

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = \chi_n^{(s)}(-1)(q^s-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}) - J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}). \tag{3.12}$$

Por otro lado, el corolario 3.3.2 nos dice que

$$g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)}) = \chi_n^{(s)}(-1)q^s J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}). \tag{3.13}$$

Comparando 3.12 y 3.13 nos queda

$$J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = -\chi_n^{(s)}(-1)J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_{n-1}^{(s)}).$$

que es lo que queríamos demostrar. □

Usando los resultados anteriores, podemos calcular los valores absolutos (las normas) de las sumas de Jacobi.

Teorema 3.3.4. Supongamos que $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$ no son triviales.

1. Si $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} \neq \varepsilon$, entonces

$$\left|J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)})\right| = q^{s(n-1)/2}$$

2. Si $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$, entonces

$$\left|J_0(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)})\right| = (q^s-1)q^{(sn/2)-s}$$

3 Si $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$, entonces

$$\left|J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)})\right| = q^{(sn/2)-s}$$

Demostración. 1. Por el teorema 3.3.1 sabemos que

$$J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) = \frac{g(\chi_1^{(s)})g(\chi_2^{(s)})\cdots g(\chi_n^{(s)})}{g(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)})}.$$

Como por el teorema 2.4.7, $|g(\chi_i^{(s)})| = q^{s/2}$, entonces

$$\left|J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)})\right| = q^{n(s/2)-(s/2)} = q^{s(n-1)/2}.$$

2 Por la proposición 3.2 4 parte *iii)*, tenemos que

$$J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) = \chi_n^{(s)}(-1)(q^s - 1)J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_{n-1}^{(s)});$$

entonces, usando la parte 1, tenemos

$$\begin{aligned}\left|J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ \ldots, \chi_n^{(s)})\right| &= (q^s - 1)\left|J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_{n-1}^{(s)})\right| \\ &= (q^s - 1)q^{s(n-2)/2} = (q^s - 1)q^{(sn/2)-s}\end{aligned}$$

3. Por el corolario 3 3.3

$$J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) = -\chi_n^{(s)}(-1)J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_{n-1}^{(s)}).$$

Como $\chi_1^{(s)}\chi_2^{(s)}\ldots\chi_{n-1}^{(s)} \neq \varepsilon$, usando la parte 1, nos queda

$$\left|J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)})\right| = \left|J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_{n-1}^{(s)})\right| = q^{s(n-2)/2} = q^{(sr/2)-s}.$$

□

3.4 La hipersuperficie H_f

En esta sección tomaremos a $\mathbb{F}$ como un campo finito con q elementos, i.e., $\mathbb{F} = \mathbb{F}_q$ y a $\mathbb{F}_s$ como la extensión de $\mathbb{F}$ de grado s, i.e., $\mathbb{F}_s = \mathbb{F}_{q^s}$.

Una vez estudiadas las propiedades de las sumas de Jacobi, las usaremos para dar una fórmula para $N_s(f)$, el número de puntos $\mathbb{F}_s$-racionales de la hipersuperficie determinada por

el polinomio $f = a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n} - b$ en $\mathbb{F}[x_1, x_2, \ldots, x_n]$. Más aún, daremos una estimación para este número.

Denotemos por $R(u)$ al conjunto de las n-adas $(u_1, \ldots, u_n) \in \mathbb{A}^n(\mathbb{F}_s)$, que son solución de la ecuación polinomial lineal

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = b. \tag{3.14}$$

Observación 3.4.1. Si $(x_1, \ldots, x_n)$ es un punto $\mathbb{F}_s$-racional de la hipersuperficie $H_f(\overline{\mathbb{F}}_q)$, entonces, haciendo $u_i = x_i^{l_i}$, tenemos que $(u_1, \ldots, u_n) \in R(u)$. Inversamente, si tomamos $(u_1, \ldots, u_n) \in R(u)$ sujeto a la condición de que $u_i = x_i^{l_i}$ tenga solución para cada i, entonces $(x_1, \ldots, x_n)$ es un punto $\mathbb{F}_s$-racional de $H_f(\overline{\mathbb{F}}_q)$, para todas las posibles soluciones x_i de $u_i = x_i^{l_i}$.

Denotemos por $N_s(f)$, al número de puntos $\mathbb{F}_s$-racionales de la hipersuperficie $H_f(\overline{\mathbb{F}}_q)$. Denotemos por d_i al máximo común divisor de l_i y $q^s - 1 = |\mathbb{F}_s^*|$, i.e., $d_i = (q^s - 1, l_i)$.

Ahora pasemos al teorema más importante de este capítulo.

Teorema 3.4.2. Sea $f = a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n} - b$. Si $b = 0$, entonces:

$$N_s(f) = q^{s(n-1)} + \sum \chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1}) \cdots \chi_n^{(s)}(a_n^{-1})J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}).$$

La suma es sobre todas las n-tuplas de caracteres $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$, tales que: $\chi_i^{(s)} \neq \varepsilon$ para $i = 1, \ldots, n$, $(\chi_i^{(s)})^{d_i} = \varepsilon$ y $\chi_1^{(s)}\chi_2^{(s)} \cdots \chi_n^{(s)} = \varepsilon$.

Si $b \neq 0$, entonces:

$$N_s(f) = q^{s(n-1)} + \sum \chi_1^{(s)}\chi_2^{(s)} \cdots \chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1}) \cdots \chi_n^{(s)}(a_n^{-1})J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}).$$

La suma es sobre todas las n-tuplas de caracteres $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$, tales que $\chi_i^{(s)} \neq \varepsilon$ para $i = 1, \ldots, n$ y $(\chi_i^{(s)})^{d_i} = \varepsilon$.

Demostración. Por la observación 3.4.1, tenemos que:

$$N_s(f) = \sum_{R(u)} N_s(x_1^{l_1} - u_1)N_s(x_2^{l_2} - u_2) \cdots N_s(x_n^{l_n} - u_n),$$

donde la suma es sobre las n-adas $(u_1, \ldots, u_n) \in R(u)$.

Por el teorema 3.1.8 y la observación 3.1.10:

$$N_s(x_j^{l_j} - u_j) = \sum_{(\chi_j^{(s)})^{d_j}=\varepsilon} \chi_j^{(s)}(u_j),$$

donde la suma es sobre todos los caracteres $\chi_j^{(s)}$, cuyo orden es un divisor de d_j. Así, tenemos que

$$\begin{aligned} N_s(f) &= \sum_{R(u)} \left(\sum_{(\chi_1^{(s)})^{d_1}=\varepsilon} \chi_1^{(s)}(u_1) \right) \left(\sum_{(\chi_2^{(s)})^{d_2}=\varepsilon} \chi_2^{(s)}(u_2) \right) \cdots \left(\sum_{(\chi_n^{(s)})^{d_n}=\varepsilon} \chi_n^{(s)}(u_n) \right) \\ &= \sum_{R(u)} \left(\sum_{\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}} \chi_1^{(s)}(u_1)\chi_2^{(s)}(u_2)\ldots\chi_n^{(s)}(u_n) \right) \\ &= \sum_{\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}} \left(\sum_{R(u)} \chi_1^{(s)}(u_1)\chi_2^{(s)}(u_2)\ldots\chi_n^{(s)}(u_n) \right). \end{aligned} \tag{3.15}$$

Donde la suma externa de 3.15 es sobre todas las n-tuplas de caracteres $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$ tales que el orden de $\chi_j^{(s)}$ es un divisor de d_j para $j = 1, \ldots, n$.

Si b=0, hagamos la sustitución $u_i = a_i^{-1}t_i$, entonces sumar sobre $R(u)$ es equivalente a sumar sobre $L_0(t)$ (donde $L_0(t)$ es como en la sección 3.2). Usando la propiedad multiplicativa de los caracteres $\chi_i^{(s)}$, la suma interna de 3.15 se transforma en

$$\begin{aligned} &\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\ldots\chi_n^{(s)}(a_n^{-1}) \sum_{L_0(t)} \chi_1^{(s)}(t_1)\chi_2^{(s)}(t_2)\ldots\chi_n^{(s)}(t_n) \\ &\qquad = \chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\ldots\chi_n^{(s)}(a_n^{-1}) J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}). \end{aligned} \tag{3.16}$$

Usando la proposición 3.2.4, sabemos que: si $\chi_1^{(s)} = \chi_2^{(s)} = \cdots = \chi_n^{(s)} = \varepsilon$, entonces $J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) = q^{s(n-1)}$; si algunos, pero no todos los $\chi_i^{(s)}$ son triviales, entonces $J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) = 0$; si $\chi_i^{(s)} \neq \varepsilon$ para $i = 1, \ldots, n$, y además, $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} \neq \varepsilon$, entonces $J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}) = 0$. Por lo tanto

$$N_s(f) = q^{s(n-1)} + \sum \chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1}) J_0(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}).$$

Donde la suma es sobre todas las n-tuplas de caracteres $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$, tales que: $\chi_i^{(s)} \neq \varepsilon$ para $i = 1, \ldots, n$, $(\chi_i^{(s)})^{d_i} = \varepsilon$ y $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$.

Si $b \neq 0$, hagamos la sustitución $u_i = ba_i^{-1}t_i$, entonces sumar sobre $R(u)$ es equivalente a sumar sobre $L(t)$ (donde $L(t)$ es como en la sección 3.2) y la suma interna de 3.15 se transforma en

$$\begin{aligned}\sum_{L(t)} &\chi_1\chi_2\cdots\chi_n(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_n(a_n^{-1})\chi_1(t_1)\chi_2(t_2)\cdots\chi_n(t_n)\\ &= \chi_1\chi_2\cdots\chi_n(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_n(a_n^{-1})\sum_{L(t)}\chi_1(t_1)\chi_2(t_2)\cdots\chi_n(t_n)\\ &= \chi_1\chi_2\cdots\chi_n(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_n(a_n^{-1})J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}). \qquad (3.17)\end{aligned}$$

Si $\chi_1 = \chi_2 = \cdots = \chi_n = \varepsilon$, entonces $J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = q^{s(n-1)}$ y si algunos, pero no todos los $\chi_i^{(s)}$ son triviales, entonces $J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}) = 0$. Por lo tanto

$$N_s(f) = q^{s(n-1)} + \sum \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}).$$

Donde la suma es sobre todas las n-tuplas de caracteres $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$, tales que $\chi_i^{(s)} \neq \varepsilon$ para $i = 1,\ldots,n$ y $(\chi_i^{(s)})^{d_i} = \varepsilon$. □

De este teorema se desprende el siguiente corolario, que nos da una estimación para el número $N_s(f)$.

Corolario 3.4.3. *1. Para $H_f(\overline{\mathbb{F}}_q)$ con $f = a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n}$, sea M el número de n-tuplas $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$,*
tales que: $\chi_i^{(s)} \neq \varepsilon$ para $i = 1,\ldots,n, (\chi_i^{(s)})^{d_i} = \varepsilon$ y $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$. Entonces:

$$\left|N_s(f) - q^{s(n-1)}\right| \leq M(q^s - 1)q^{s(n/2)-s}.$$

2. Para $H_f(\overline{\mathbb{F}}_q)$ con $f = a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n} - b$ y $b \neq 0$, sea M_0 el número de n-tuplas $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$, tales que: $\chi_i^{(s)} \neq \varepsilon$ para $i = 1,\ldots,n$, $(\chi_i^{(s)})^{d_i} = \varepsilon$ y $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)} = \varepsilon$; sea M_1 el número de n-tuplas $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)}$, tales que $\chi_i^{(s)} \neq \varepsilon$ para $i = 1,\ldots,n$, $(\chi_i^{(s)})^{d_i} = \varepsilon$ y $\chi_1^{(s)}\chi_2^{(s)}\ldots\chi_n^{(s)} \neq \varepsilon$. Entonces:

$$\left|N_s(f) - q^{s(n-1)}\right| \leq M_0(q^{s(n/2)-s}) + M_1(q^{s(n-1)/2}).$$

Demostración. 1. Por el teorema, sabemos que:

$$\left|N_s(f) - q^{s(n-1)}\right| = \left|\sum \chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})J_0(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_n^{(s)})\right|. \qquad (3.18)$$

Como la imagen de $\chi^{(s)}$ es un subconjunto de S^1, tenemos que $|\chi^{(s)}(u)| = 1$ para todo $u \in \mathbb{F}_s^*$, entonces:

$$\left|\sum \chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})\right| \leq \sum \left|\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})\right| = M.$$

Sustituyendo esto en 3.18 y usando el teorema 3.3.4, tenemos:

$$\left|N_s(f) - q^{s(n-1)}\right| \leq M(q^s - 1)q^{s(n/2)-s}.$$

2. En este caso, se cumple que

$$\left|N_s(f) - q^{s(n-1)}\right| = \left|\sum \chi_1^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\cdots\chi_n^{(s)}(a_n^{-1})J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)})\right|. \tag{3.19}$$

A la suma:

$$\sum \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})$$

de la ecuación 3.19, la podemos descomponer como

$$\sum_{\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}=\varepsilon} \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1}) + \sum_{\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}\neq\varepsilon} \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1}).$$

Donde la primer suma es sobre las n-tuplas de caracteres $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$ tales que $\prod_{i=1}^n \chi_i^{(s)} = \varepsilon$ y la segunda suma es sobre las n-tuplas de caracteres $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_n^{(s)}$ tales que $\prod_{i=1}^n \chi_i^{(s)} \neq \varepsilon$. Como

$$\left|\sum_{\chi_1^s\chi_2^s\cdots\chi_n^s=\varepsilon} \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})\right| \leq \sum_{\chi_1^s\chi_2^s\cdots\chi_n^s=\varepsilon} \left|\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})\right| = M_0$$

y

$$\left|\sum_{\chi_1^s\chi_2^s\cdots\chi_n^s\neq\varepsilon} \chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})\right| \leq \sum_{\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}\neq\varepsilon} \left|\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_n^{(s)}(b)\chi_1^{(s)}(a_1^{-1})\chi_2^{(s)}(a_2^{-1})\cdots\chi_n^{(s)}(a_n^{-1})\right| = M_1,$$

usando nuevamente el teorema 3.3.4 y substituyendo en 3.19, obtenemos

$$\left|N_s(f) - q^{s(n-1)}\right| \leq M_0(q^{s(n/2)-s}) + M_1(q^{s(n-1)/2}).$$

Que es lo que queríamos demostrar. □

En el siguiente ejemplo ilustraremos todo lo desarrollado en este capítulo.

Ejemplo 3.4.4. Calculemos el número de puntos $\mathbb{F}_{q^s}$ racionales de $H_{3x^2+2y^2-1}(\overline{\mathbb{F}}_q) \subset \mathbb{A}^2(\overline{\mathbb{F}}_q)$, donde $\mathbb{F}$ es un campo cuya característica es diferente de dos y diferente de 3.

Sea $f = 3x^2 + 2y^2 - 1$, entonces si nos fijamos en todos los pares $(a, b) \in \mathbb{F}_{q^s}^2$ tales que $a + b = 1$, tenemos que

$$N_s(f) = \sum_{a+b=1} N(3x^2 - a)N(2y^2 - b) = \sum_{a+b=1} N(x^2 - 3^{-1}a)N(y^2 - 2^{-1}b),$$

como $N(x^2 - c) = 1 + \chi^{(s)}(c)$ donde $\chi^{(s)}$ es el carácter de orden dos en $C(\mathbb{F}_s^*)$ (teorema 3.1.8 página 63), nos queda que

$$\begin{aligned} N_s(f) &= \sum_{a+b=1} N(x^2 - 3^{-1}a)N(y^2 - 2^{-1}b) \\ &= \sum_{a+b=1} [1 + \chi^{(s)}(3^{-1}a)][1 + \chi^{(s)}(2^{-1}b))] \\ &= \sum_{a+b=1} 1 + \sum_{a+b=1} \chi^{(s)}(3^{-1}a) + \sum_{a+b=1} \chi^{(s)}(2^{-1}b) + \sum_{a+b=1} \chi^{(s)}(3^{-1}a)\chi^{(s)}(2^{-1}b) \\ &= q^s + \chi^{(s)}(3^{-1})\chi^{(s)}(2^{-1})J(\chi^{(s)}, \chi^{(s)}). \end{aligned}$$

Las suma $\sum_{a+b=1} \chi^{(s)}(3^{-1}a) = 0$ ya que ésta es igual a la suma $\chi^{(s)}(3^{-1}) \sum_a \chi^{(s)}(a)$ que es cero por el teorema 2.3.17 parte *e)*. Como $\chi^{(s)}$ tiene orden dos, $J(\chi^{(s)}, \chi^{(s)}) = J(\chi^{(s)}, \overline{\chi^{(s)}}) = -\chi^{(s)}(-1)$ (corolario 3.3.3 página 69) por lo que:

$$N_s(f) = q^s - \chi^{(s)}(3^{-1}2^{-1})\chi^{(s)}(-1) = q^s - \chi^{(s)}(6^{-1})\chi^{(s)}(-1).$$

Esto nos da la siguiente estimación:

$$|N_s(f) - q^s| \leq |\chi^{(s)}(6^{-1})\chi^{(s)}(-1)| = 1$$

lo que nos muestra que $N_s(f) \neq 0$, o bien, que la ecuación $3x^2 + 2y^2 = 1$ siempre tiene solución en $\mathbb{F}_{q^s}$. Más aún, si $q = p^m$ donde p es la característica de $\mathbb{F}_q$, entonces $\chi^{(s)}(c) =$

$(\chi(c))^{ms}\ \forall\ c \in \mathbb{F}_p$, en particular para -1 y para 6^{-1}, donde χ es el caracter multiplicativo de orden dos sobre el campo primo de $\mathbb{F}_q$, es decir en $C(\mathbb{F}_p^*)$ (teorema 2.3.12 parte *c)*) y como $\chi(-1) = (-1)^{(p-1)/2}$ encontramos que

$$\begin{aligned} N_s(f) &= q^s - (-1)^{ms(p-1)/2}(\chi(6^{-1}))^{ms} \\ &= p^{ms} - (-1)^{ms(p-1)/2}(\chi(6^{-1}))^{ms}. \end{aligned}$$

En particular esto nos dice que la ecuación $3x^2+2y^2 = 1$ tiene 4 soluciones en $\mathbb{F}_5 \times \mathbb{F}_5$ ya que $N(f) = 5 - (-1)^4 = 4$. Si verificamos este resultado haciendo la substitución, encontramos que en efecto, las soluciones en $\mathbb{F}_5 \times \mathbb{F}_5$ son 4 y están dadas por: $(1,2)$; $(1,3)$; $(4,2)$; $(4,3)$.

Capítulo 4

LAS CONJETURAS DE WEIL

En su "último" teorema, podemos ver que Fermat se preguntó sobre el número de soluciones enteras de la ecuación $x^l + y^l = z^l$ o, equivalentemente, sobre el número de soluciones en $\mathbb{Q}$ de $x^l + y^l = 1$.

En el lenguaje de Geometría Algebraica esto es equivalente a preguntarse sobre el número de puntos $\mathbb{Q}$-racionales de la curva $V(x^l+y^l-1) \subset \mathbb{A}^2(\overline{\mathbb{Q}})$; o bien, si consideramos los puntos al infinito, sobre el número de puntos $\mathbb{Q}$-racionales de la curva $\overline{V}(x^l + y^l - z^l) \subset \mathbb{P}^2(\overline{\mathbb{Q}})$.

Por analogía con lo anterior, definamos como *hipersuperficies de Fermat* sobre un campo finito a las hipersuperficies dadas por polinomios de la forma

$$f = a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l \tag{4.1}$$

donde cada $a_i \in \mathbb{F}_q$ con $\prod_{i=0}^n a_i \neq 0$ para $i = 0, \ldots, n$ y $\mathbb{F}_q$ es el campo finito con q elementos.

Si tomamos una de estas hipersuperficies $\overline{H}_f(\overline{\mathbb{F}}_q) \subset \mathbb{P}^n(\overline{\mathbb{F}}_q)$ nos preguntamos sobre el número de puntos $\overline{N}_s = |\overline{H}_f(\mathbb{F}_{q^s})|$ $\mathbb{F}_{q^s}$-racionales, de $\overline{H}_f(\overline{\mathbb{F}}_q)$ para cada extensión $\mathbb{F}_{q^s}$ de $\mathbb{F}_q$.

En 1949, A. Weil publicó un artículo titulado: "Número de soluciones de ecuaciones sobre campos finitos", en el que da una serie de conjeturas (ahora teoremas) para la función zeta asociada a cualquier variedad algebraica no singular ([Wei49]), que en nuestro caso de estudio es la serie

$$\mathcal{Z}_f(u) := \exp(\sum_{s=1}^{\infty} \overline{N}_s u^s/s).$$

Además da una fórmula para los números $\overline{N}_s$ en términos de las sumas de Gauss y las sumas de Jacobi para las hipersuperficies de Fermat con lo que demuestra la racionalidad de la función zeta para dichas hipersuperficies.

En este capítulo mostraremos la validez de las conjeturas para las hipersuperficies de Fermat (el objetivo principal de esta tesis) basándonos en las ideas expuestas por Weil en su artículo.

4.1 La función zeta de una hipersuperficie proyectiva

Sea $\mathbb{F}_q$ un campo finito con q elementos y fijemos una cerradura algebraica $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$. Denotemos por $\mathbb{F}_{q^s}$, a la única extensión de $\mathbb{F}_q$ de grado s, i.e., $\mathbb{F}_{q^s}$ es el campo finito con q^s elementos.

Sea $f \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ un polinomio homogéneo. Recordemos que por $\overline{H}_f(\mathbb{F}_{q^s}) \subset \mathbb{P}^n(\mathbb{F}_{q^s})$ denotamos al conjunto de puntos $\mathbb{F}_{q^s}$-racionales de la hipersuperficie proyectiva determinada por este polinomio.

Una manera de estudiar a los números $\overline{N}_s = |\overline{H}_f(\mathbb{F}_{q^s})|$, es introduciendo la serie de potencias

$$\sum_{i=1}^{\infty} \overline{N}_s u^s \tag{4.2}$$

y preguntarnos sobre la forma de esta serie, i.e., nos podríamos preguntar si existe una función "manejable" con la que podamos obtener información acerca de los números $\overline{N}_s$. A la serie 4.2, la podemos considerar como una serie formal, o bien, como una serie de variable compleja; en este último caso, notemos que

$$\overline{N}_s \leq \frac{q^{s(n+1)} - 1}{q^s - 1} = 1 + q^s + q^{2s} + \cdots + q^{ns} \leq (n+1)q^{ns}.$$

Por lo tanto, si $u \in \mathbb{C}$ es tal que $|u| < q^{-n}$, entonces $\overline{N}_s |u|^s < n + 1$ y, entonces, se sigue que 4.2 converge normalmente para todos los $u \in \mathbb{C}$ tales que $|u| < q^{-n}$. Ver el libro de Remert [Rem91].

La serie 4.2 es importante ya que si $S(u) := \sum_{i=1}^{\infty} \overline{N}_s u^s$, entonces

$$\overline{N}_k = \frac{S^k(0)}{k!},$$

donde $S^k(u)$ es la k-ésima derivada de $S(u)$ (vista formalmente, o bien, como la derivada de una función analítica compleja en el disco de radio q^{-n}).

Sea $\exp(u) := \sum_{s=0}^{\infty} \frac{u^s}{s!}$ (nuevamente podemos ver a esta serie de manera formal, o bien, como una serie compleja que es, por cierto, analítica en todo $\mathbb{C}$).

Definición 4.1.1. La *función zeta* de la hipersuperficie determinada por f, es la serie dada por

$$\mathcal{Z}_f(u) := \exp\left(\sum_{s=1}^{\infty} \frac{\overline{N}_s u^s}{s}\right).$$

Notemos que si consideramos a $\mathcal{Z}_f(u)$ como serie de potencias compleja, ésta converge en el disco $\{u \in \mathbb{C} : |u| < q^{-n}\}$.

Nota 4.1.2. Si conocemos a $\mathcal{Z}_f(u)$, entonces podemos recobrar los números $\overline{N}_s$ mediante la fórmula

$$\overline{N}_s = \frac{1}{(s-1)!} \frac{d^s}{du^s} \log(\mathcal{Z}_f(u))\Big|_{u=0}.$$

Como veremos más adelante, resulta conveniente trabajar con $\mathcal{Z}_f(u)$ en vez de la serie 4.2, a pesar de que esta última parezca más natural. Es por esto que centraremos nuestra atención en esta función recién definida.

Ejemplo 4.1.3. Si $f \equiv 0$ entonces $\overline{H}_f(\mathbb{F}_s)$ es igual a $\mathbb{P}^n(\mathbb{F}_s)$, de aquí que $\overline{N}_s = \frac{q^{s(n+1)}-1}{q^s-1} = \sum_{i=0}^{n} q^{si}$. De esto se sigue que

$$\sum_{s=1}^{\infty} \frac{\overline{N}_s u^s}{s} = \sum_{s=1}^{\infty} \left(\sum_{i=0}^{n} \frac{q^{si} u^s}{s}\right) = \sum_{i=0}^{n} \left(\sum_{s=1}^{\infty} \frac{(q^i u)^s}{s}\right). \tag{4.3}$$

Usando la identidad $\sum_{i=1}^{\infty} w^s/s = -\log(1-w)$ en 4.3, tenemos:

$$\sum_{s=1}^{\infty} \frac{\overline{N}_s u^s}{s} = -\sum_{i=1}^{n} \log(1 - q^i u), \tag{4.4}$$

exponenciando la ecuación 4.4, tenemos que

$$\mathcal{Z}_0(u) = \frac{1}{(1-u)(1-qu)\cdots(1-q^n u)}.$$

Ejemplo 4.1.4. Ahora tomemos al polinomio $f = x_0x_1 - x_2x_3 \in \mathbb{F}[x_0, x_1, x_2, x_3]$. Sabemos que el número $\overline{N}_s$ de puntos $\mathbb{F}$-racionales proyectivos de la hipersuperficie determinada por f, está dado por

$$\overline{N}_s = \frac{N_s - 1}{q^s - 1}$$

donde N_s es el número de puntos $\mathbb{F}$-racionales de $H_f(\overline{\mathbb{F}}_q) \subset \mathbb{A}^{n+1}$. Así que calculemos primero N_s.

Por un razonamiento análogo a la observación 3.4.1 se cumple que

$$N_s = \sum_{a-b=0} N(xy = a)N(xy = b) = \sum_{a\in\mathbb{F}_s} N(xy = a)^2. \tag{4.5}$$

Donde $N(xy = a)$ es el número de soluciones de la ecuación $xy = a$ en $\mathbb{F}_{q^s}$.

Como $N(xy = 0) = 2(q^s - 1) + 1$ y $N(xy = a) = q^s - 1$ para $a \neq 0$, tenemos que $N_s = 4(q^s - 1)^2 + 4(q^s - 1) + 1 + (q^s - 1)^3$, por lo tanto

$$\begin{aligned}\overline{N}_s &= \frac{N_s - 1}{q^s - 1} \\ &= (q^s - 1)^2 + 4(q^s - 1) + 4 \\ &= (q^s + 1)^2 = q^{2s} + 2q^s + 1\end{aligned}$$

y así

$$\begin{aligned}\sum_{s=1}^{\infty} \frac{\overline{N}_s u^s}{s} &= \sum_{s=1}^{\infty} \left(\frac{(q^2u)^s}{s} + 2\frac{(qu)^s}{s} + \frac{u^s}{s} \right) \\ &= -\log(1 - q^2u) - 2\log(1 - qu) - \log(1 - u).\end{aligned}$$

Ahora, aplicando exponencial en ambos lados de la igualdad obtenemos

$$Z_f(u) = \frac{1}{(1 - q^2u)(1 - qu)^2(1 - u)}.$$

Ejemplo 4.1.5. Ahora nuestro problema consiste en determinar el número de matrices de 2×2 con coeficientes en $\mathbb{F}_q$, que tengan determinante igual a cero.

Si a cada matriz $M = \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix}$ le asociamos el punto $(x_0, x_1, x_2, x_3) \in \mathbb{A}^4(\mathbb{F}_q)$ (que es claramente una biyección), entonces las matrices con determinante igual a cero resultan ser los puntos $\mathbb{F}_q$-racionales de la hipersuperficie $H_{x_0x_3 - x_1x_2} \subset \mathbb{A}^4(\overline{\mathbb{F}}_q)$.

Por el ejemplo 4.1.4, el número de matrices con determinante cero está dado por la fórmula

$$N(x_0x_3 - x_1x_2) = (q-1)^3 + 4(q-1)^2 + 4(q-1) + 1 = q(q^2+q-1).$$

Así, en $\mathcal{M}^{2\times 2}(\mathbb{F}_5)$ hay 145 matrices no invertibles y, por lo tanto, $5^4 - 145 = 480$ matrices invertibles.

4.2 Las conjeturas de Weil

Para una variedad proyectiva suave V (sin puntos singulares) sobre $\mathbb{F}_q$ de dimensión d las conjeturas de Weil se pueden establecer de la siguiente manera:

Sea $Z_V(t)$ la función zeta asociada a V. Entonces

W1 *Racionalidad:*

$$Z_V(t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_2(t)P_2(t)\cdots P_{2d}(t)}, \tag{4.6}$$

donde $d = dimV$, $P_r(t) \in \mathbb{C}[x]$ para todo $r = 1, 2, \ldots, 2d$ y $P_r(0) = 1$.

W2 *Integridad:*

$$P_0(t) = 1 - t, \qquad P_{2d}(t) = 1 - q^d t, \tag{4.7}$$

y para $r = 1, 2, \ldots, 2d$ tenemos que $P_r(t) = \prod(1 - w_{r,i}t)$, donde los $w_{r,i}$ son ciertos enteros algebraicos.

W3 *La ecuación funcional:* Existe un número E tal que la función zeta satisface la siguiente ecuación funcional[1]

$$Z_V(1/q^d t) = \pm q^{dE/2} t^E Z_V(t). \tag{4.8}$$

W4 *La Hipótesis de Riemann:*

Los valores absolutos de cada uno de los números $w_{r,i}$ es $q^{r/2}$. Es decir, $|w_{r,i}| = q^{r/2}$.

[1] El número E es la característica de Euler de la variedad, que puede ser definida en forma puramente algebraica como el número de auto intersección de la diagonal de $V \times V$ (ver [AP95] ó [Har77]).

W5 *Números de Betti*

Si V es la reducción de una variedad proyectiva suave Y definida sobre $\mathbb{C}$, entonces el grado B_r del polinomio $P_r(t)$ es el r-ésimo número de Betti de la variedad compleja $Y(\mathbb{C})$ y $E = \sum_r (-1)^r B_r$.

Como mencionamos anteriormente, nosotros mostraremos la validez de estas conjeturas para las hipersuperficies de Fermat, sin embargo, ya que el estudio de los números de Betti rebasa los objetivos de la tesis (el lector interesado puede revisar los libros [Har77, Apendice C] o [FK88]), en la última conjetura mostraremos lo siguiente:

W5' *Grados:* $E = (-1)^n \deg(P) - n = \sum_r (-1)^r B_r$, y si l divide a $q-1$ entonces el grado de $P(t)$ es

$$l^{-1}[(l-1)^{n+1} + (-1)^{n+1}(l-1)].$$

donde l es el grado del polinomio que me determina a la hipersuperficie de Fermat.

Notemos que para nuestro caso de estudio, si $f = a_0 x_0^l + a_1 x_1^l + \cdots + a_n x_n^l$ la dimensión de nuestras hipersuperficies es $n-1$, i.e., $d = n-1$.

4.3 La racionalidad

En esta sección mostraremos que la función zeta asociada a una hipersuperficie de Fermat es racional, tal y como conjeturó Weil en su artículo [Wei49]. Para lograr esto necesitamos expresar a los números $\overline{N}_s$ de puntos $\mathbb{F}_{q^s}$-racionales proyectivos de la hipersuperficie, en términos de las sumas de Gauss, lo que nos permitirá utilizar fuertemente la relación de Hasse-Davenport (teorema 2.5.8) que como veremos más adelante, es fundamental en esta demostración.

Primero demos una caracterización de la racionalidad de la función zeta, que nos permitirá acotar a los números $\overline{N}_s$.

Lema 4.3.1. *La función zeta es racional si, y sólo si, existen números complejos α_i, β_j tales que*

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

donde $\overline{N}_s$ es el número de puntos $\mathbb{F}_{q^s}$-racionales de la hipersuperficie proyectiva $\overline{H}_f(\overline{\mathbb{F}}_q) \subset \mathbb{P}^n(\overline{\mathbb{F}}_q)$.

Demostración. Supongamos que $\mathcal{Z}_f(t)$ es racional Por la definición de la función zeta, vemos que si expandemos a $\mathcal{Z}_f(t)$ en serie de potencias alrededor del cero, entonces el término constante es uno, además, podemos suponer que si $\mathcal{Z}_f(t) = P(t)/Q(t)$ con $P(t)$ y $Q(t)$ polinomios, entonces $P(0) = Q(0) = 1$, ya que de lo contrario, si $P(0) = a$ y $Q(0) = b$, entonces $1 = \mathcal{Z}_f(0) = P(0)/Q(0) = a/b$ y, por lo tanto, $a = b$. Así, tenemos que $\mathcal{Z}_f(t) = \frac{aP'(t)}{bQ'(t)} = \frac{P'(t)}{Q'(t)}$ donde $P'(0) = Q'(0) = 1$.

Con esto, podemos suponer que

$$\mathcal{Z}_f(t) = \frac{\prod_i(1-\alpha_i t)}{\prod_j(1-\beta_j t)} \text{ donde los } \alpha_i, \beta_j \in \mathbb{C}. \tag{4.9}$$

Aplicamos logaritmo a ambos lados de la igualdad

$$\log(\mathcal{Z}_f(t)) = \sum_i \log(1-\alpha_i t) - \sum_j \log(1-\beta_j t)$$

derivando implícitamente y multiplicando por t obtenemos:

$$\frac{t\mathcal{Z}_f'(t)}{\mathcal{Z}_f(t)} = \sum_j \frac{\beta_j t}{1-\beta_j t} - \sum_i \frac{\alpha_i t}{1-\alpha_i t}.$$

Como la expansión en serie de potencias de $\frac{t\beta_j}{1-t\beta_j}$ al rededor del cero es $\sum_{s=1}^{\infty}(t\beta_j)^s$ (análogo para $\frac{t\alpha_i}{1-t\alpha_i}$), tenemos la siguiente igualdad

$$\frac{t\mathcal{Z}_f'(t)}{\mathcal{Z}_f(t)} = \sum_{s=1}^{\infty}\left(\sum_j \beta_j^s - \sum_i \alpha_i^s\right) t^s. \tag{4.10}$$

Por otro lado, de la definición de $\mathcal{Z}_f(t)$, tenemos que $\log(\mathcal{Z}_f(t)) = \sum_{s=1}^{\infty} \frac{\overline{N}_s t^s}{s}$, entonces

$$\frac{t\mathcal{Z}_f'(t)}{\mathcal{Z}_f(t)} = \sum_{s=1}^{\infty} \overline{N}_s t^s. \tag{4.11}$$

Comparando los coeficientes de las ecuaciones 4 10 y 4.11, tenemos que:

$$\overline{N}_s = \sum_j \beta_j^s - \sum_i \alpha_i^s,$$

con lo que demostramos la primera parte.

Ahora supongamos que $\overline{N}_s = \sum_j \beta_j^s - \sum_i \alpha_i^s$, entonces

$$\sum_{s=1}^{\infty} \frac{\overline{N}_s t^s}{s} = \sum_{s=1}^{\infty} \left(\sum_j (\beta_j t)^s / s - \sum_i (\alpha_i t)^s / s \right)$$
$$= \sum_j \left(\sum_{s=1}^{\infty} (\beta_j t)^s / s \right) - \sum_i \left(\sum_{s=1}^{\infty} (\alpha_i t)^s / s \right).$$

Como $-\log(1-w) = \sum_{s=1}^{\infty} w^s/s$, tenemos que:

$$\sum_{s=1}^{\infty} \frac{\overline{N}_s t^s}{s} = -\sum_j \log(1-\beta_j t) + \sum_i \log(1-\alpha_i t)$$
$$= \log\left(\prod_i (1-\alpha_i t) \right) - \log\left(\prod_j (1-\beta_j t) \right),$$

tomando exponencial en ambos lados, nos queda:

$$Z_f(t) = \frac{\prod_i (1-\alpha_i t)}{\prod_j (1-\beta_j t)}.$$

□

Teorema 4.3.2. Si $f = a_0 x_0^l + a_1 x_1^l + \cdots + a_n x_n^l \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$, entonces el número de puntos $\mathbb{F}_{q^s}$-racionales $\overline{N}_s$ de $\overline{H}_f(\overline{\mathbb{F}}_q)$ está dado por la fórmula:

$$\overline{N}_s = q^{s(n-1)} + q^{s(n-2)} + \cdots + q^s + 1$$
$$+ \frac{1}{q^s} \sum_{\chi_0^{(s)} \cdots \chi_n^{(s)}} \chi_0^{(s)}(a_0^{-1}) \cdots \chi_n^{(s)}(a_n) g(\chi_0^{(s)}) \cdots g(\chi_n^{(s)}),$$

donde los $\chi_i^{(s)}$ son caracteres multiplicativos de $\mathbb{F}_{q^s}$ para cada $i \in \{0, 1, \ldots, n\}$ tales que $(\chi_i^{(s)})^{d_s} = \varepsilon$, $\chi_i^{(s)} \neq \varepsilon$ y $\prod_{i=0}^n \chi_i^{(s)} = \varepsilon$ donde d_s es el máximo común divisor entre l y $q^s - 1$.

Demostración. Si N_s es el número de puntos $\mathbb{F}_{q^s}$-racionales de $H_f(\overline{\mathbb{F}}_q) \subset \mathbb{A}^{n+1}(\overline{\mathbb{F}}_q)$, entonces $\overline{N}_s = \frac{N_s - 1}{q^s - 1}$. Así, por el teorema 3.4.2, especializado en este caso, sabemos que

$$N_s = q^{sn} + \sum \chi_0^{(s)}(a_0^{-1}) \chi_1^{(s)}(a_1^{-1}) \cdots \chi_n^{(s)}(a_n^{-1}) J_0(\chi_0^{(s)}, \chi_1^{(s)}, \ldots, \chi_n^{(s)}) \qquad (4.12)$$

donde la suma es sobre todas las $(n+1)$-tuplas de caracteres de $\mathbb{F}_{q^s}$ tales que $\chi_i^{(s)} \neq \varepsilon$ para $i \in \{0, 1, \ldots, n\}$, $(\chi_i^{(s)})^{d_s} = \varepsilon$ y $\prod_{i=0}^n \chi_i^{(s)} = \varepsilon$ donde d_s es el máximo común divisor entre $q^s - 1$ y l.

Por otro lado, por la proposición 3.2.4 parte *iii)* sabemos que:

$$J_0(\chi_0^{(s)}, \chi_1^{(s)}, \dots, \chi_n^{(s)}) = \chi_0^{(s)}(-1)(q^s - 1)J(\chi_1^{(s)}, \chi_2^{(s)}, \dots, \chi_n^{(s)}) \tag{4.13}$$

y por el teorema 3.3.1 tenemos:

$$J(\chi_1^{(s)}, \chi_2^{(s)}, \dots, \chi_n^{(s)}) = \frac{g(\chi_1^{(s)})g(\chi_2^{(s)}) \cdots g(\chi_n^{(s)})}{g(\chi_1^{(s)}\chi_2^{(s)} \cdots \chi^{(s)})} \tag{4.14}$$

Nota 4.3.3. Las hipótesis del teorema 3.3.1 se cumplen ya que $\chi_i^{(s)} \neq \varepsilon$ para i contenido en $\{0, 1, \dots, n\}$ y como $\prod_{i=0}^{n} \chi_i^{(s)} = \varepsilon$ entonces $\prod_{i=1}^{n} \chi_i^{(s)} = (\chi_0^s)^{-1} \neq \varepsilon$.

Siendo así, multiplicamos y dividimos por $g(\chi_0^{(s)})$ la segunda parte de la igualdad 4.14 para obtener

$$\begin{aligned} J(\chi_1^{(s)}, \chi_2^{(s)}, \dots, \chi_n^{(s)}) &= \frac{g(\chi_0^{(s)})g(\chi_1^{(s)})g(\chi_2^{(s)}) \cdots g(\chi_n^{(s)})}{g(\chi_0^{(s)})g(\chi_1^{(s)}\chi_2^{(s)} \cdots \chi_n^{(s)})} \\ &= \frac{g(\chi_0^{(s)})g(\chi_1^{(s)})g(\chi_2^{(s)}) \cdots g(\chi_n^{(s)})}{\chi_0^{(s)}(-1)q^s}. \end{aligned}$$

Hemos utilizado que $g(\chi_0^{(s)})g(\chi_1^{(s)}\chi_2^{(s)} \cdots \chi_n^{(s)}) = g(\chi_0^{(s)})g((\chi_0^{(s)})^{-1}) = g(\chi_0^{(s)})\overline{g(\chi_0^{(s)})}$ y aplicamos la proposición 2.4.8 Así, sustituyendo 4.14 en 4.13 nos queda:

$$J_0(\chi_0^{(s)}, \chi_1^{(s)}, \dots, \chi_n^{(s)}) = \frac{q^s - 1}{q^s} g(\chi_0^{(s)})g(\chi_1^{(s)})g(\chi_2^{(s)}) \cdots g(\chi_n^{(s)}).$$

Por lo tanto, $\overline{N}_s$ es igual a

$$\frac{q^{sn} - 1}{q^s - 1} + \frac{1}{q^s} \sum_{\chi_0^{(s)} \cdots \chi_n^{(s)}} \chi_0^{(s)}(a_0^{-1}) \cdots \chi_n^{(s)}(a_n^{-1}) g(\chi_0^{(s)}) \cdots g(\chi_n^{(s)})$$

donde la suma es sobre todas la $n+1$-tuplas de caracteres sujetas a las condiciones de la proposición. □

Para convertir más manejable la información que nos presenta el teorema anterior, presentamos la siguiente notación.

Notación 4.3.4. Denotemos por Δ_s al subconjunto de $\bigoplus_{i=0}^{n} C(\mathbb{F}_{q^s}^*)$ formado por todas las $(n+1)$-adas de caracteres $(\chi_0^{(s)}, \chi_1^{(s)}, \cdots \chi_n^{(s)})$ tales que $(\chi_i^{(s)})^{d_s} = \varepsilon$, $\chi_i^{(s)} \neq \varepsilon$ y $\prod_{i=0}^{n} \chi_i^{(s)} = \varepsilon$ donde d_s es el máximo común divisor entre l y $q^s - 1$.

Sea $C_{d_s}(\mathbb{F}_{q^s}^*)$ (ver notación 2.3.13) el único subgrupo de $C(\mathbb{F}_{q^s}^*)$ de orden d_s (ver el corolario 2.2.10). Entonces tenemos, más precisamente, que $\Delta_s \subset \bigoplus_{i=0}^n C_{d_s}(\mathbb{F}_{q^s}^*)$ donde estamos considerando a $\bigoplus_{i=0}^n C_{d_s}(\mathbb{F}_{q^s}^*)$ como un grupo.

Proposición 4.3.5. *El conjunto* Δ_s *tiene* $d_s^{-1}((d_s-1)^{n+1}+(-1)^{n+1}(d_s-1))$ *elementos.*

Demostración. Como $\prod_{i=0}^n \chi_i = \varepsilon$ con cada $\chi_i \neq \varepsilon$, tenemos que si escogemos libremente a $\chi_0, \chi_1, \cdots, \chi_{n-1}$ entonces el caracter χ_n queda determinado por la condición $\prod_{i=0}^n \chi_i = \varepsilon$, así tenemos que $|\Delta_s| = (d_s-1)^n - M$, donde M es el número de n-adas tales que $\prod_{i=0}^{n-1} \chi_i = \varepsilon$. Esto claramente implica que

$$|\Delta_s| = (d_s-1)^n - (d_s-1)^{n-1} + (d_s-1)^{n-2} + \cdots + (-1)^{n-1}(d_s-1).$$

Para ver que esta suma es como nos dice la proposición, hagamos $R = (d_s-1)$ y sea $T_k := \sum_{j=0}^{k-1}(-1)^j R^{k-j}$ con $k \geq 1$, notemos que $T_1 = 1$ (con esta notación $|\Delta_s| = T_n$). Es fácil ver que se cumplen las siguientes igualdades:

$$T_k = RT_{k-1} + (-1)^{k-1}R, \qquad T_k + T_{k-1} = R^k$$

que, resolviendo el sistema, tenemos que $T_k = (1+R)^{-1}[R^{k+1} + (-1)^{k+1}R]$. Substituyendo k por n y R por (d_s-1) tenemos lo deseado. □

Notación 4.3.6. 1. Denotemos por Δ a la unión de todos los Δ_s. Es decir, $\Delta := \bigcup_{s\in\mathbb{N}} \Delta_s$.

2. Dado $\alpha \in \Delta$, entonces denotemos por s_α al entero positivo tal que $\alpha \in \Delta_{s_\alpha}$ (notemos que $\Delta_s \bigcap \Delta_k = \emptyset$ siempre que $s \neq k$).

3. Dado $\alpha \in \Delta$, denotemos por ρ_α al orden de α visto como un elemento del grupo $C_{d_{s_\alpha}}(\mathbb{F}_{q^{s_\alpha}}^*)$ (notemos que ρ_α divide a $d_{s_\alpha} = (l, q^{s_\alpha}-1)$ y por lo tanto divide a l y a $q^{s_\alpha}-1$).

4. Sea $\Gamma : \Delta \longrightarrow \mathbb{C}$ el mapeo definido por $\alpha \longmapsto \Gamma(\alpha)$, si $\alpha = (\chi_0^{(s_\alpha)}, \chi_1^{(s_\alpha)}, \cdots, \chi_n^{(s_\alpha)})$, entonces

$$\Gamma(\alpha) := \frac{1}{q^{s_\alpha}} \chi_0^{(s_\alpha)}(a_0^{-1})\chi_1^{(s_\alpha)}(a_1^{-1}) \cdots \chi_n^{(s_\alpha)}(a_n^{-1}) g(\chi_0^{(s_\alpha)}) g(\chi_1^{(s_\alpha)}) \cdots g(\chi_n^{(s_\alpha)}).$$

Con la notación recién introducida, el teorema 4.3.2 nos asegura que

$$\overline{N}_s = \sum_{i=0}^{n-1}(q^i)^s + \sum_{\alpha\in\Delta_s}\Gamma(\alpha). \tag{4.15}$$

Lo que haremos a continuación es estudiar a la suma $\sum_{\alpha\in\Delta_s}\Gamma(\alpha)$ dando algunos resultados sobre el conjunto Δ y los números complejos $\Gamma(\alpha)$.

Notación 4.3.7. Sea $\alpha \in \Delta$. Denotemos por μ_α al entero positivo más pequeño tal que ρ_α *divide a* $q^{\mu_\alpha} - 1$.

Proposición 4.3.8. *Dado $\alpha \in \Delta$ tenemos que μ_α divide a s_α. Más aún, si ν es un entero positivo, entonces $\rho_\alpha | q^\nu - 1$ si, y sólo si, $\mu_\alpha | \nu$.*

Demostración. Como $\rho_\alpha | q^{s_\alpha} - 1$ (ver la notación 4.3.6) basta demostrar la segunda parte de la proposición.

Supongamos que $\rho_\alpha | q^\nu - 1$, entonces ρ_α debe dividir al máximo común divisor entre $q^\nu - 1$ y $q^{\mu_\alpha} - 1$. Por el lema 1 3.9 del capítulo 1 sabemos que $(q^\nu - 1, q^{\mu_\alpha} - 1) = q^r - 1$ para algún entero r tal que $1 \leq r \leq \mu_\alpha$. Por la minimalidad de μ_α tenemos que $r = \mu_\alpha$ y entonces $q^{\mu_\alpha} - 1$ divide a $q^\nu - 1$ y por el lema 1 3.3 del capítulo 1 concluimos que μ_α divide a ν.

Ahora supongamos que μ_α divide a ν, por el lema 1.3.3 tenemos que $q^{\mu_\alpha} - 1$ divide a $q^\nu - 1$, y como $\rho_\alpha | q^{\mu_\alpha} - 1$ entonces también ρ_α divide a $q^\nu - 1$. □

Observación 4.3.9. Con lo anterior, lo que estamos viendo es que las extensiones finitas $\mathbb{F}_{q^\nu}$ de $\mathbb{F}_q$ tales que ρ_α divide a $q^\nu - 1$ son para las que $\mathbb{F}_{q^{\mu_\alpha}} \subset \mathbb{F}_{q^\nu}$ y sólo estas. Esto a su vez implica que hay una inyección del grupo $C(\mathbb{F}^*_{q^{\mu_\alpha}})$ en el grupo $C(\mathbb{F}^*_{q^\nu})$ dado por el mapeo derivación (ver el teorema 2.3.12 y sus corolarios). De hecho, el mapeo derivación (restringido al dominio) es un isomorfismo entre $C_{\rho_\alpha}(\mathbb{F}^*_{q^{\mu_\alpha}})$ y $C_{\rho_\alpha}(\mathbb{F}^*_{q^\nu})$. Este mapeo se puede extender de manera natural a un isomorfismo entre $\bigoplus_{i=0}^n C_{\rho_\alpha}(\mathbb{F}^*_{q^{\mu_\alpha}})$ y $\bigoplus_{i=0}^n C_{\rho_\alpha}(\mathbb{F}^*_{q^\nu})$, o bien, a una inyección entre $\bigoplus_{i=0}^n C(\mathbb{F}^*_{q^{\mu_\alpha}})$ y $\bigoplus_{i=0}^n C(\mathbb{F}^*_{q^\nu})$.

Notación 4.3.10. Sean μ y ν dos enteros positivos tales que μ divide a ν, y sea

$$(\ )' : \bigoplus_{i=0}^n C(\mathbb{F}^*_{q^\mu}) \longrightarrow \bigoplus_{i=0}^n C(\mathbb{F}^*_{q^\nu})$$

el mapeo derivación "generalizado". Dado $\alpha \in \bigoplus_{i=0}^n C(\mathbb{F}^*_{q^\mu})$ denotemos por α', o bien por $\alpha \circ N_{\mathbb{F}_{q^\nu}/\mathbb{F}_{q^\mu}}$ a la imagen de α bajo este mapeo.

Observación 4.3.11. Observemos que si $\alpha = (\chi_0, \chi_1, \dots, \chi_n)$, entonces $\alpha' = \alpha \circ N_{\mathbb{F}_{q^\nu}/\mathbb{F}_{q^\mu}} = (\chi_0', \chi_1', \dots, \chi_n')$ donde cada χ_i' es igual a $\chi_i' \circ N_{\mathbb{F}_{q^\nu}/\mathbb{F}_{q^\mu}}$.

Proposición 4.3.12. *Sean μ, ν enteros positivos tales que $\mu|\nu$, entonces el mapeo $\Delta_\mu \longrightarrow \Delta_\nu$ tal que $\alpha \longmapsto \alpha'$ es una inyección.*

Demostración. Como $(\ )' : \bigoplus_{i=0}^n C(\mathbb{F}_{q^\mu}^*) \longrightarrow \bigoplus_{i=0}^n C(\mathbb{F}_{q^\nu}^*)$ es inyectivo y $\Delta_\mu \subset \bigoplus_{i=0}^n C(\mathbb{F}_{q^\mu}^*)$ basta mostrar que el mapeo está bien definido, i.e., que si $\alpha \in \Delta_\mu$, entonces $\alpha' \in \Delta_\nu$.

Sea $\alpha = (\chi_0, \chi_1, \dots, \chi_n)$, entonces $\alpha' = (\chi_0', \chi_1', \dots, \chi_n')$. Como cada $\chi_i \neq \varepsilon$ y el mapeo derivación es inyectivo, entonces $\chi_i' \neq \varepsilon$. Como $\prod_{i=0}^n \chi_i' = (\prod_{i=0}^n \chi_i)'$ (ya que la derivación es un homomorfismo de grupos) y $\prod_{i=0}^n \chi_i = \varepsilon$ entonces $\prod_{i=0}^n \chi_i' = \varepsilon$. Finalmente, como χ y χ' tienen el mismo orden y $d_\mu | d_\nu$ (ya que $\mu|\nu$ entonces $q^\mu - 1 | q^\nu - 1$ y entonces d_μ divide a $q^\nu - 1$, por lo tanto, divide a d_ν) concluimos que $\alpha' \in \Delta_\nu$. □

Teorema 4.3.13. Para cada $\alpha \in \Delta$ existe un único elemento $\widehat{\alpha} \in \Delta_{\mu_\alpha}$ tal que $\alpha = \widehat{\alpha}' = \widehat{\alpha} \circ N_{\mathbb{F}_{q^{s_\alpha}}/\mathbb{F}_{q^{\mu_\alpha}}}$.

Demostración. Tomemos $\alpha \in \Delta$, entonces $\alpha \in \Delta_{s_\alpha} \subset \bigoplus_{i=0}^n C(\mathbb{F}_{q^{s_\alpha}}^*)$; más aún,

$$\alpha \in \bigoplus_{i=0}^n C_{\rho_\alpha}(\mathbb{F}_{q^{s_\alpha}}^*).$$

Como el mapeo derivación es un isomorfismo entre $\bigoplus_{i=0}^n C_{\rho_\alpha}(\mathbb{F}_{q^{s_\alpha}}^*)$ y $\bigoplus_{i=0}^n C_{\rho_\alpha}(\mathbb{F}_{q^{\mu_\alpha}}^*)$ (observación 4.3.9), existe un único elemento $\widehat{\alpha} \in \bigoplus_{i=0}^n C_{\rho_\alpha}(\mathbb{F}_{q^{\mu_\alpha}}^*)$ tal que $\alpha = \widehat{\alpha}'$. Necesitamos mostrar que $\widehat{\alpha} \in \Delta_{\mu_\alpha}$, para ver esto supongamos que $\widehat{\alpha} = (\chi_0, \chi_1, \dots, \chi_n)$, entonces $\alpha = (\chi_0', \chi_1', \dots, \chi_n')$. Como $\alpha \in \Delta_{s_\alpha}$, entonces cada $\chi_i' \neq \varepsilon$, lo que implica que $\chi_i \neq \varepsilon$; como $\prod_{i=1}^n \chi_i' = \varepsilon$ entonces $(\prod_{i=1}^n \chi_i)' = \varepsilon$ y por la inyectividad del mapeo, $\prod_{i=1}^n \chi_i = \varepsilon$; finalmente, tenemos que $\widehat{\alpha}^{d_{\mu_\alpha}} = e := \bigoplus_{i=0}^n \varepsilon$ ya que $\widehat{\alpha}^{\rho_\alpha} = e$ y ρ_α divide a l y a $q^{\mu_\alpha} - 1$ (ver los comentarios en la notación 4.3.6), por lo tanto divide a d_{μ_α}. Como μ_α divide a s_α, la unicidad nos la da la proposición anterior. □

Definición 4.3.14. Dado $\alpha \in \Delta$ definimos por *elemento primitivo de* α, al elemento $\widehat{\alpha}$ del teorema anterior. Al conjunto $P := \{\widehat{\alpha} : \alpha \in \Delta\}$ lo llamamos el *conjunto primitivo.*

Observación 4.3.15. Observemos que $\widehat{\alpha}$ y α tienen el mismo orden, i.e., $\rho_{\widehat{\alpha}} = \rho_\alpha$. También $\mu_{\widehat{\alpha}} = \mu_\alpha$. Más aún $\widehat{(\widehat{\alpha})} = \widehat{\alpha}$ ya que como $\mu_{\widehat{(\widehat{\alpha})}} = \mu_{\widehat{\alpha}} = \mu_\alpha$, entonces $\widehat{(\widehat{\alpha})} \in \Delta_{\mu_\alpha}$ y como el mapeo derivación es la identidad en Δ_{μ_α}, tenemos que $\widehat{(\widehat{\alpha})} = \widehat{(\widehat{\alpha})}' = \widehat{\alpha}$.

Teorema 4.3.16. Sea $\alpha \in \Delta$ y supongamos que existe $\beta \in \Delta$ tal que $\alpha = \beta' = \beta \circ N_{\mathbb{F}_{q^{s\alpha}}/\mathbb{F}_{q^{s\beta}}}$. Entonces $\beta = \widehat{\alpha}' = \widehat{\alpha} \circ N_{\mathbb{F}_{q^{s\beta}}/\mathbb{F}_{q^{\mu_\alpha}}}$.

Demostración. Sea $\beta \in \Delta$ tal que $\alpha = \beta' = \beta \circ N_{\mathbb{F}_{q^{s\alpha}}/\mathbb{F}_{q^{s\beta}}}$. Primero veamos que $\mu_\alpha = \mu_\beta$. En efecto, como la derivación es un homomorfismo inyectivo entre los grupos $\bigoplus_{i=0}^{n} C(\mathbb{F}^*_{q^{s\alpha}})$ y $\bigoplus_{i=0}^{n} C(\mathbb{F}^*_{q^{s\beta}})$, tenemos que ambos elementos tienen el mismo orden, i.e. $\rho_\alpha = \rho_\beta$ por lo que $\mu_\alpha = \mu_\beta$. Esto implica que $\widehat{\alpha}$ y $\widehat{\beta}$ están en Δ_{μ_α}. Así, tenemos que $\alpha = \beta \circ N_{\mathbb{F}_{q^{s\alpha}}/\mathbb{F}_{q^{s\beta}}}$ y como $\beta = \widehat{\beta} \circ N_{\mathbb{F}_{q^{s\beta}}/\mathbb{F}_{q^{\mu_\alpha}}}$ usando la relación de transitividad de la norma (teorema 2.1.14), tenemos que $\alpha = \widehat{\beta} \circ N_{\mathbb{F}_{q^{s\alpha}}/\mathbb{F}_{q^{\mu_\alpha}}}$. Finalmente, usando la unicidad de $\widehat{\alpha}$ concluimos que $\widehat{\alpha} = \widehat{\beta}$. □

Corolario 4.3.17. *Sean α y β elementos de Δ tales que $\beta' = \alpha$, entonces $\widehat{\alpha} = \widehat{\beta}$.*

La demostración de este corolario está incluida en la demostración del teorema.

Ahora definamos una relación entre los elementos de Δ de la siguiente manera. Diremos que α y β están relacionados, si ambos tienen el mismo elemento primitivo, es decir, si $\widehat{\alpha} = \widehat{\beta}$. Esta relación es claramente una relación de equivalencia en donde cada α esta relacionado con su elemento primitivo $\widehat{\alpha}$. Así vemos que los elementos de P son, de alguna manera, representantes canónicos de las clases de equivalencia.

Esta relación de equivalencia induce una partición en Δ dada por las clases de equivalencia. Esta partición resultará finita tal y como veremos a continuación.

Proposición 4.3.18. *El conjunto $P = \{\widehat{\alpha} : \alpha \in \Delta\}$ es un conjunto finito.*

Demostración. Como el conjunto $\{\rho_\alpha : \alpha \in \Delta\}$ es finito (ya que cada ρ_α es un divisor de l), entonces también lo es el conjunto $\{\mu_\alpha\}$, y por ende, sólo hay un número finito de conjuntos Δ_{μ_α}. Como cada $\widehat{\alpha} \in \Delta_{\mu_\alpha}$ y Δ_{μ_α} es finito (proposición 4.3.5 página 88) el resultado se sigue. □

De lo anterior, podemos concluir el siguiente e importante teorema

Teorema 4.3.19. Si $P = \{\widehat{\alpha}_1, \widehat{\alpha}_2, \ldots, \widehat{\alpha}_m\}$, y $[\widehat{\alpha}_i]$ denota a la clase de equivalencia de $\widehat{\alpha}_i$. Entonces $\Delta = \bigcup_{i=1}^{m} [\widehat{\alpha}_i]$

Antes de ver en que se traducen los resultados anteriores en el análisis de la racionalidad de la función zeta, demos una proposición más; que será fundamental en la prueba del teorema principal de esta sección

Proposición 4.3.20. *Para cada $\lambda \in \mathbb{N}$ y cada $\widehat{\alpha} \in P$, denotemos por $\widehat{\alpha}^{(\lambda)}$ al elemento $\widehat{\alpha} \circ N_{\mathbb{F}_{q^{\lambda\mu_\alpha}}/\mathbb{F}_{q^{\mu_\alpha}}}$, es decir, $\widehat{\alpha}^{(\lambda)} := \widehat{\alpha} \circ N_{\mathbb{F}_{q^{\lambda\mu_\alpha}}/\mathbb{F}_{q^{\mu_\alpha}}}$. Entonces*

$$[\widehat{\alpha}] = \{\widehat{\alpha}^{(\lambda)} : \lambda \in \mathbb{N}\}.$$

Demostración. Por el corolario 4.3.17, cada $\widehat{\alpha}^{(\lambda)}$ está en $[\widehat{\alpha}]$. Ahora, si $\beta \in [\widehat{\alpha}]$ entonces β esta relacionado con $\widehat{\alpha}$ y entonces $\widehat{\beta} = \widehat{\alpha}$ (ver observación 4.3.15) con lo que existe $\lambda \in \mathbb{N}$ $(\lambda = s_\beta/\mu_\alpha)$ tal que $\beta = \widehat{\alpha}' = \widehat{\alpha} \circ N_{\mathbb{F}_{q^{\lambda\mu_\alpha}}/\mathbb{F}_{q^{\mu_\alpha}}}$. □

Corolario 4.3.21. *Si $P = \{\widehat{\alpha}_1, \widehat{\alpha}, \ldots, \widehat{\alpha}_m\}$, entonces:*

$$\Delta = \bigcup_{i=1}^{m} \{\widehat{\alpha}_i^{(\lambda)} : \lambda \in \mathbb{N}\}.$$

La demostración es inmediata de los resultados anteriores.

Ahora sí, veamos en que se traducen los resultados anteriores en el análisis de los números $\overline{N}_s$. Pongamos atención en la serie $\sum_{s=1}^{\infty} \overline{N}_s t^s/s$. Usando la ecuación 4.15 de la página 89 y la identidad $\sum_{s=1}^{\infty} w^s/s = -\log(1-w)$ tenemos que

$$\begin{aligned}
\sum_{s=1}^{\infty} \frac{\overline{N}_s t^s}{s} &= \sum_{s=1}^{\infty} \sum_{i=0}^{n-1} \frac{(q^i t)^s}{s} + \sum_{s=1}^{\infty} \sum_{\alpha \in \Delta_s} \frac{\Gamma(\alpha) t^s}{s} \\
&= -\sum_{i=0}^{n-1} \log(1 - q^i t) + \sum_{\alpha \in \Delta} \frac{\Gamma(\alpha) t^{s_\alpha}}{s_\alpha} \\
&= -\sum_{i=0}^{n-1} \log(1 - q^i t) + \sum_{\widehat{\alpha} \in P} \sum_{\beta \in [\widehat{\alpha}]} \frac{\Gamma(\beta) t^{s_\beta}}{s_\beta} \\
&= -\sum_{i=0}^{n-1} \log(1 - q^i t) + \sum_{\widehat{\alpha} \in P} \sum_{\lambda=1}^{\infty} \frac{\Gamma(\widehat{\alpha}^{(\lambda)}) t^{\mu_{\widehat{\alpha}} \lambda}}{\mu_{\widehat{\alpha}} \lambda} \\
&= -\sum_{i=0}^{n-1} \log(1 - q^i t) + \sum_{\widehat{\alpha} \in P} \frac{1}{\mu_{\widehat{\alpha}}} \sum_{\lambda=1}^{\infty} \frac{\Gamma(\widehat{\alpha}^{(\lambda)}) t^{\mu_{\widehat{\alpha}} \lambda}}{\lambda}.
\end{aligned} \tag{4.16}$$

Para poder concluir es necesario que estudiemos a los números $\Gamma(\alpha)$. Más concretamente queremos dar una relación entre $\Gamma(\widehat{\alpha}^{(\lambda)})$ y $\Gamma(\widehat{\alpha})$.

Recordemos algunos resultados de los capítulos anteriores que nos serán de gran utilidad.

1. Si $s = \lambda\mu$, $\chi \in C(\mathbb{F}_{q^\mu}^*)$ y $\chi' \in C(\mathbb{F}_{q^s}^*)$, entonces $\chi'(a) = (\chi(a))^\lambda$ (teorema 2.3.12).

2. Si $s = \lambda\mu$, $\chi \in C(\mathbb{F}_{q^\mu}^*)$ y $\chi' \in C(\mathbb{F}_{q^s}^*)$, entonces $-g(\chi') = [-g(\chi)]^\lambda$. (teorema 2.5.8 página 58)

3. Si $\alpha \in \Delta$ entonces existe un $\widehat{\alpha} \in P$ tal que $\alpha = \widehat{\alpha}^{(\lambda)}$ para algún $\lambda \in \mathbb{Z}$ (ver proposición 4.3.20) y su corolario.

Lema 4.3.22. *Sea $\widehat{\alpha} \in P$. Entonces:*

$$\Gamma(\widehat{\alpha}^{(\lambda)}) = (-1)^{n+1}[(-1)^{n+1}\Gamma(\widehat{\alpha})]^\lambda.$$

Demostración Supongamos que $\widehat{\alpha} = (\chi_0, \chi_1, \ldots, \chi_n)$, entonces $\widehat{\alpha}^{(\lambda)} = (\chi_0', \chi_1', \ldots, \chi_n')$. Así:

$$\begin{aligned}
\Gamma(\widehat{\alpha}^{(\lambda)}) &= \frac{1}{q^{s_\alpha}} \prod_{i=0}^{n} \chi_i'(a_i^{-1}) g(\chi_i') \\
&= \frac{1}{q^{\mu_\alpha \lambda}} \prod_{i=0}^{n} [\chi_i(a_i^{-1})]^\lambda (-1)[-g(\chi_i)]^\lambda \\
&= (-1)^{n+1} \left[\frac{(-1)^{n+1}}{q^{\mu_\alpha}} \prod_{i=0}^{n} \chi_i(a_i^{-1}) g(\chi_i) \right]^\lambda \\
&= (-1)^{n+1}[(-1)^{n+1}\Gamma(\widehat{\alpha})]^\lambda.
\end{aligned}$$

□

Con este lema, encontramos que la suma $\sum_{\lambda=1}^{\infty} \frac{\Gamma(\widehat{\alpha}^{(\lambda)}) t^{\mu_{\widehat{\alpha}} \lambda}}{\lambda}$ en la ecuación 4.16 la podemos convertir a

$$(-1)^{n+1} \sum_{\lambda=1}^{\infty} \frac{[(-1)^{n+1}\Gamma(\widehat{\alpha}) t^{\mu_{\widehat{\alpha}}}]^\lambda}{\lambda},$$

que, usando la identidad $-\log(1-w^s) = \sum_{s=1}^{\infty} w^s/s$, se reduce a

$$(-1)^n \log[1 - (-1)^{n+1}\Gamma(\widehat{\alpha}) t^{\mu_{\widehat{\alpha}}}];$$

con lo que

$$\sum_{s=1}^{\infty} \frac{\overline{N}_s t^s}{s} = (-1)^n \sum_{\widehat{\alpha} \in P} \frac{1}{\mu_{\widehat{\alpha}}} \log[1 - (-1)^{n+1}\Gamma(\widehat{\alpha}) t^{\mu_{\widehat{\alpha}}}] - \sum_{i=0}^{n-1} \log(1 - q^i t). \tag{4.17}$$

Finalmente, veamos que podemos eliminar a los $1/\mu_{\widehat{\alpha}}$. Para lograr esto, demos algunos resultados

Sea σ el q-automorfismo de Frobenius (ver pagina 22) entonces el grupo $< \sigma > \subset \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ actúa en $C(\mathbb{F}_{q^s})$, para todo $s \in \mathbb{N}$ de la siguiente manera

$$\begin{aligned} < \sigma > \times C(\mathbb{F}_{q^s}) &\longrightarrow C(\mathbb{F}_{q^s}) \\ (\sigma^n, \chi) &\longmapsto \sigma^n\chi, \end{aligned}$$

donde $\sigma^n\chi := \chi \circ \sigma^n$ (la acción esta bien definida, y es acción en efecto, ya que σ es un automorfismo y $\sigma|_{\mathbb{F}_{q^s}} \in \mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$).

Observación 4.3.23. si n es positivo entonces $\sigma^n\chi = \chi^{q^n}$, y si n es negativo, entonces $\sigma^n\chi = \chi^{q^{rs+n}}$ en donde $rs+n$ es positivo. En efecto, como $\sigma|_{\mathbb{F}_{q^s}}$ genera a $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) = \{1, \sigma, \sigma^2, \ldots, \sigma^{s-1}\}$ tenemos que $\sigma^n\chi(a) = \chi(a^{q^r}) = \chi^{q^r}(a)$ para r cualquier entero positivo congruente a n modulo s. Por lo tanto, dado cualquier $\phi \in < \sigma >$ existe un entero positivo n tal que $\phi\chi = \chi^{q^n} = \sigma^n\chi$, por lo que, para efectos de la acción del grupo, siempre podemos suponer que para todo elemento $\sigma^n \in < \sigma >$, n es un entero positivo y entonces $\sigma^n\chi = \chi^{q^n}$ siempre.

Proposición 4.3.24. *Para cada $\sigma^n \in < \sigma >$ el mapeo $\sigma^n : C(\mathbb{F}_{q^s}^*) \longrightarrow C(\mathbb{F}_{q^s}^*)$ tal que $\chi \longmapsto \sigma^n\chi$ es un isomorfismo de grupos.*

Demostración. Basta demostrar la proposición para $n = 1$ ya que la composición de isomorfismos es un isomorfismo.

Primero veamos que es un homomorfismo de grupos. Sean χ, λ dos caracteres en $C(\mathbb{F}_{q^s}^*)$ entonces

$$\begin{aligned} \sigma(\chi\lambda) &= \chi\lambda \circ \sigma \\ &= (\chi \circ \sigma)(\lambda \circ \sigma) \\ &= (\sigma\chi)(\sigma\lambda). \end{aligned}$$

Para mostrar que es un isomorfismo, basta mostrar que el homomorfismo es inyectivo. Supongamos que $\sigma\chi = \varepsilon$, entonces $\chi^q = \varepsilon$ y el orden ρ de χ debe dividir a q. como ρ también divide a $q^s - 1$ y $(q, q^s - 1) = 1$, concluimos que $\rho = 1$ y, por lo tanto, $\chi = \varepsilon$. □

Como consecuencia inmediata de esta proposición, tenemos el siguiente corolario.

Corolario 4.3.25. *Si $\alpha = (\chi_0, \chi_1, \ldots, \chi_n) \in \Delta_s$, entonces tenemos que*

$$\sigma^n\alpha := (\sigma^n\chi_0, \sigma^n\chi_1, \ldots, \sigma^n\chi_n) \in \Delta_s.$$

Con lo anterior, podemos considerar ahora la acción de $< \sigma >$ en Δ de la siguiente mantera.

$$< \sigma > \times \Delta \longrightarrow \Delta$$
$$(\sigma^n, \alpha) \longmapsto \sigma^n \alpha.$$

Lema 4.3.26. *Supongamos que* $\mathbb{F}_{q^\mu} \subset \mathbb{F}_{q^s}$. *Consideremos a los mapeos derivación* $(\ )' : C'(\Xi^*_{q^\mu}) \longrightarrow C(\Xi^*_{q^s})$ *y* $(\ )' : \Delta \longrightarrow \Delta$. *Entonces:*

1 $(\sigma^n \chi)' = \sigma^n \chi'$. *Para* $\chi \in C(\mathbb{F}^*_{q^\mu})$.

2 $(\sigma^n \alpha)' = \sigma^n \alpha'$. *Para* $\alpha \in \Delta$.

Demostración Dado $\alpha = (\chi_0, \chi_1, \cdots, \chi_n) \in \Delta$, entonces $\sigma^n \alpha = (\sigma^n \chi_0, \sigma^n \chi_1, \sigma^n \ldots, \sigma^n \chi_n)$. por lo que, si la primera parte del lema es verdadera, entonces también lo es la segunda Así pues, basta demostrar la primera parte. Así $(\sigma^n \chi)' = (\chi^{q^n})'$, como el mapeo derivación es un homomorfismo de grupos, lo podemos intercambiar con q^n, entonces $(\chi^{q^n})' = \chi'^{q^n} = \sigma^n \chi'$ y tenemos el resultado □

Corolario 4.3.27. *Sea* $\widehat{\alpha} \in P$, *entonces* $\sigma^n \widehat{\alpha} = \widehat{\sigma^n \alpha}$.

Demostración. Primero observemos que si $\widehat{\alpha} \in \Delta_{\mu_\alpha}$, entonces $\sigma^n \widehat{\alpha}$ también está en Δ_{μ_α} (corolario 4.3.25). Consideremos al mapeo derivación $(\ )' : \Delta_{\mu_\alpha} \longrightarrow \Delta_{s_\alpha}$, entonces $\widehat{\alpha}' = \alpha$ y por el lema anterior tenemos que:

$$(\sigma^n \widehat{\alpha})' = \sigma^n \widehat{\alpha}' = \sigma^n \alpha \in \Delta_{s_\alpha}.$$

Por la unicidad de $\widehat{\sigma^n \alpha}$ tenemos que $\sigma^n \widehat{\alpha} = \widehat{\sigma^n \alpha}$. □

Este corolario lo que nos está asegurando es que si $\widehat{\alpha} \in P$ entonces también $\sigma^n \widehat{\alpha} \in P$ lo que nos demuestra que $< \sigma >$ actúa en P.

Notación 4.3 28. Sea $< \sigma > \times P \longrightarrow P$ la acción de $< \sigma >$ en P. Denotemos por

$$\Theta(\widehat{\alpha}) := \{\phi \widehat{\alpha} : \phi \in < \sigma >\}$$

a la órbita de α

Lo que queremos hacer es mostrar que cualesquiera dos elementos en P que estén en la misma órbita, tienen el mismo valor bajo Γ, es decir, queremos mostrar que si $\widehat{\beta} \in \Theta(\widehat{\alpha})$, entonces $\Gamma(\widehat{\beta}) = \Gamma(\widehat{\alpha})$. Para lograr esto tenemos que estudiar la relación entre $g(\chi)$ y $g(\sigma^n\chi)$ donde $g(\chi)$ es la suma de Gauss asociada χ.

Lema 4.3.29. *Sea* $\chi \in \mathbb{F}_{q^\mu}$ *y* $\sigma^n \in <\sigma>$, *entonces* $g(\sigma^n\chi) = g(\chi)$.

Demostración. Recordemos que $g(\chi) = \sum_{a\in\mathbb{F}_{q^\mu}} \chi(a)\psi(a)$, donde $\psi \in C(\mathbb{F}_{q^\mu})$ es el carácter aditivo canónico de $\mathbb{F}_{q^\mu}$, es decir, $\psi(a) = e^{2\pi i Tr_{\mathbb{F}_{q^\mu}}(a)/p}$ donde p es la característica de $\mathbb{F}_{q^\mu}$ y $Tr_{\mathbb{F}_{q^\mu}}$ es la traza absoluta (ver páginas 44 y 29). Afirmamos que $Tr_{\mathbb{F}_{q^\mu}}(\sigma^n(a)) = Tr_{\mathbb{F}_{q^\mu}}(a)$. En efecto, como $\sigma(a) = a^q$, usando el teorema 2.1.6 parte *iii*) y aplicando inducción sobre n, tenemos la igualdad. Esto nos dice que $\psi(\sigma^n(a)) = \psi(a)$ y entonces:

$$\begin{aligned} g(\sigma^n\chi) &= \sum_{a\in\mathbb{F}_{q^\mu}} \sigma^n\chi(a)\psi(a) \\ &= \sum_{a\in\mathbb{F}_{q^\mu}} \chi(\sigma^n(a))\psi(\sigma^n(a)) \\ &= g(\chi). \end{aligned}$$

La última igualdad se sigue gracias a que $\sigma^n|_{\mathbb{F}_{q^\mu}}$ es un elemento de $\mathrm{Gal}(\mathbb{F}_{q^\mu}/\mathbb{F}_q)$ y por lo tanto, cundo a varía sobre $\mathbb{F}_{q^\mu}$ también lo hace $\sigma^n(a)$. □

Teorema 4.3.30. Sea $\widehat{\alpha} \in P$ y $<\sigma> \times P \longrightarrow P$ la acción de $<\sigma>$ en P. Si $\widehat{\beta} \in \Theta(\widehat{\alpha})$ entonces $\Gamma(\widehat{\beta}) = \Gamma(\widehat{\alpha})$.

Demostración. Como $\widehat{\beta} \in \Theta(\widehat{\alpha})$, existe $n \in \mathbb{N}$ tal que $\widehat{\beta} = \sigma^n\widehat{\alpha}$. Si $\widehat{\alpha} = (\chi_0, \chi_1, \ldots, \chi_n)$, entonces $\sigma^n\chi(a) = \chi(\sigma^n(a)) = \chi(a)$ para toda $a \in \mathbb{F}_q$. Como $g(\sigma^n\chi) = g(\chi)$ tenemos que:

$$\begin{aligned} \Gamma(\beta) &= \Gamma(\sigma^n\widehat{\alpha}) \\ &= \frac{1}{q^{\mu_\alpha}} \prod_{i=0}^{n} \sigma^n\chi_i(a_i^{-1})g(\sigma^n\chi_i) \\ &= \frac{1}{q^{\mu_\alpha}} \prod_{i=0}^{n} \chi_i(a_i^{-1})g(\chi_i) \\ &= \Gamma(\widehat{\alpha}). \end{aligned}$$

□

Teorema 4.3.31. Dado $\widehat{\alpha} \in P$ entonces $|\Theta(\widehat{\alpha})| = \mu_\alpha$.

Demostración. Sea $\mathbb{E}_{\widehat{\alpha}} := \{\psi \in < \sigma >: \psi\widehat{\alpha} = \widehat{\alpha}\}$ el estabilizador de $\widehat{\alpha}$. Entonces $|\Theta(\widehat{\alpha})| = |< \sigma > /\mathbb{E}_{\widehat{\alpha}}|$ (Este es un resultado de la teoría general de grupos. Para su demostración ver, por ejemplo [Rot94]).

Afirmamos que $\mathbb{E}_{\widehat{\alpha}} =< \sigma^{\mu_\alpha} >$. En efecto, $\sigma^n \in \mathbb{E}_{\widehat{\alpha}}$ si y sólo si $\widehat{\alpha}^{q^n} = \sigma^n\widehat{\alpha} = \widehat{\alpha}$ si y sólo si $\widehat{\alpha}^{q^n-1} = e$ (donde $e = \bigoplus_{i=o}^{n} \varepsilon$) si y sólo si ρ_α (el orden de $\widehat{\alpha}$) divide a $q^n - 1$ si y sólo si μ_α divide a n (Proposición 4.3.8, página 89) si, y sólo si, $\sigma^n \in < \sigma^{\mu_\alpha} >$.

Como $< \sigma > \cong \mathbb{Z}$ y $< \sigma^{\mu_\alpha} > \cong \mu_\alpha\mathbb{Z}$ tenemos que $|< \sigma > /\mathbb{E}_{\widehat{\alpha}}| = |\mathbb{Z}/\mu_\alpha\mathbb{Z}| = \mu_\alpha$, con lo que el teorema es verdadero. □

Tomando en cuenta estos dos últimos teoremas, vemos que si en la primer suma de la parte derecha de la ecuación 4.17 (página 93) la agrupamos por órbitas, podemos eliminar a los $\frac{1}{\mu_\alpha}$. Para ser más precisos, podemos escoger a un representante (fijo) por cada órbita en P, y si hay k órbitas, entonces los podemos numerar y obtener al conjunto $P/\sigma = \{\widehat{\alpha}_1, \widehat{\alpha}_2, \ldots, \widehat{\alpha}_k\}$ donde cada $\widehat{\alpha}_i$ es representante de alguna órbita y si $i \neq j$ entonces $\widehat{\alpha}_i \notin \Theta(\widehat{\alpha}_j)$. Así, la ecuación 4.17 se transforma en:

$$\sum_{s=1}^{\infty} \frac{\overline{N}_s t^s}{s} = (-1)^n \sum_{i=1}^{k} \log[1 - (-1)^{n+1}\Gamma(\widehat{\alpha}_i)t^{\mu_{\widehat{\alpha}_i}}] - \sum_{i=0}^{n-1} \log(1 - q^i t).$$

Aplicando exponencial a ambos lados de la igualdad tenemos ya el teorema más importante de la sección

Teorema 4.3.32 (Racionalidad). Sea $f = a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l$ La función zeta asociada a la hipersuperficie $H_f(\overline{\mathbb{F}}_q) \subset \mathbb{P}^n(\overline{\mathbb{F}}_q)$ es una función racional y está dada por

$$\mathcal{Z}_f(t) = \frac{P(t)^{(-1)^n}}{(1-t)(1-qt)\cdots(1-q^{n-1}t)} \tag{4.18}$$

donde $P(t) = \prod_{i=1}^{k}[1 - (-1)^{n+1}\Gamma(\widehat{\alpha}_i)t^{\mu_{\widehat{\alpha}_i}}]$.

De este teorema y el lema 4.3.1 (página 4.3 1) concluimos el siguiente corolario.

Corolario 4.3.33. *sea $\overline{N}_s$ el número de puntos $\mathbb{F}_{q^s}$-racionales de la hipersuperficie de Fermat determinada por f, entonces:*

$$\overline{N}_s = \sum_{i=0}^{n-1}(q^i)^s - (-1)^n \sum_{i=1}^{k}(w_i)^s,$$

donde las w_i son las raíces recíprocas de $P(t)$.

Para presentar el teorema anterior en la forma que dice la conjetura W1, definamos los polinomios $P_r(t)$ para $0 \leq r \leq 2(n-1)$ de la manera que sigue.

1. Si $n = 2m$, entonces, $P_{2i}(t) := (1 - q^i t)$ para $0 \leq i \leq n-1$. Si $i \neq m$ entonces $P_{2i-1}(t) := 1$ y para $i = m$, $P_{n-1} = P_{2m-1}(t) := P(t)$.

2. Si n es impar y $n = 2m+1$, entonces $P_{2i-1}(t) := 1$. Si $i \neq m$ entonces $P_{2i}(t) := (1-q^i t)$ y para $i = m$, $P_{n-1}(t) = P_{2m}(t) := (1 - q^m t)P(t)$.

Con esto vemos que en cualquier caso podemos escribir:

$$\mathcal{Z}_f(t) = \frac{P_1(t)P_3(t)\cdots P_{2(n-1)-1}(t)}{P_2(t)P_2(t)\cdots P_{2(n-1)}(t)}, \tag{4.19}$$

tal y como establece W1.

Ejemplo 4.3.34. Sea $f = x_0^3 + x_1^3 + x_2^3 \in \mathbb{F}_4[x_0, x_1, x_2]$, por la ecuación 4.15 en la página 89 sabemos que

$$\overline{N}_s = \sum_{i=0}^{1} (4^i)^s + \sum_{\alpha \in \Delta_s} \Gamma(\alpha) = 1 + 4^s + \sum_{\alpha \in \Delta_s} \Gamma(\alpha).$$

Como $d_s = (4^s - 1, 3) = 3$ tenemos que $|\Delta_s| = 3^{-1}(8-2) = 2$ (ver proposición 4.3.5) para todo entero positivo s, por lo que $\Delta_s = \{\alpha, \overline{\alpha}\}$ donde $\alpha = (\chi^{(s)}, \chi^{(s)}, \chi^{(s)})$ y $\chi^{(s)}$ el caracter multiplicativo de $\mathbb{F}_{4^s}$ de orden 3. Como $\rho_\alpha = 3$ entonces $\mu_\alpha = 1$ por lo que $\Delta_{\mu_\alpha} = \Delta_1$ y por lo tanto $P = \{\hat{\alpha}, \hat{\overline{\alpha}}\} = \Delta_1$. Calculemos $\Gamma(\hat{\alpha})$ y $\Gamma(\hat{\overline{\alpha}})$. Tenemos que si $\hat{\alpha} = (\chi, \chi, \chi)$ entonces

$$\begin{aligned} \Gamma(\hat{\alpha}) &= \frac{1}{4} g(\chi)^3 \\ &= \frac{2^3}{4} \quad \text{ver el ejemplo 2.5.9 en la página 59} \\ &= 2. \end{aligned}$$

Como $g(\overline{\chi}) = \overline{g(\chi)}$ (ejemplo 2.5.9) y $\overline{g(\chi)} = \overline{2} = 2 = g(\chi)$, tenemos que $\Gamma(\hat{\alpha}) = \Gamma(\hat{\overline{\alpha}}) = 2$ (ver también el teorema 4.6.5 en la página 103). Usando el lema 4.3.22 en la página 93 encontramos que $\Gamma(\alpha) = (-1)^3[(-1)^3\Gamma(\hat{\alpha})]^3 = -(-2)^3$ y por lo tanto

$$\overline{N}_s = 1 + 4^s + \Gamma(\alpha) + \Gamma(\overline{\alpha}) = 1 + 4^s - 2(-2)^s.$$

Notemos que para $s = 1$ tenemos que $\overline{N}_1 = 9$ tal y como calculamos en el ejemplo 1.6.17 en la página 27.

Con esta información, podemos calcular la función zeta asociada a la hipersuperficie de Fermat determinada por f. Como

$$\begin{aligned}\sum_{s=1}^{\infty} \overline{N}_s u^s/s &= \sum_{s=1}^{\infty} \frac{t^s}{s} + \sum_{s=1}^{\infty} \frac{(4t)^s}{s} - 2\sum_{s=1}^{\infty} \frac{(-2t)^s}{s} \\ &= -\log(1-u) - \log(1-4u) + 2\log(1+2u)\end{aligned}$$

concluimos que

$$\mathcal{Z}_f(u) = \frac{(1+2u)^2}{(1-u)(1-4u)}. \tag{4.20}$$

4.4 Integridad

Para los polinomios de la forma $(1 - q^i t)$ tenemos claramente que q^i es un entero algebraico. En seguida mostraremos que las raíces de $P(t)$ son también enteros algebraicos.

Observación 4.4.1. Recordemos que los enteros algebraicos $\overline{\mathbb{Z}}$ forman un anillo conmutativo con unidad. Más aún, cualquier raíz de un polinomio mónico con coeficientes en $\overline{\mathbb{Z}}$, también es entero algebraico [Lor96, p. 9-16].

Lema 4.4.2. *Para toda $\alpha \in \Delta$, $\Gamma(\alpha)$ es un entero algebraico.*

Demostración. Supongamos que $\alpha \in \Delta_s$ (es decir $s_\alpha = s$). Recordemos que

$$\Gamma(\alpha) := \frac{1}{q^s}\chi_0^{(s)}(a_0^{-1})\chi_1^{(s)}(a_1^{-1})\cdots\chi_n^{(s)}(a_n^{-1})g(\chi_0^{(s)})g(\chi_1^{(s)})\cdots g(\chi_n^{(s)}).$$

Tenemos que $\chi_i^{(s)}(a_i^{-1})$ es un entero algebraico para cada $0 \leq i \leq n$ ya que es una raíz de la unidad. Como los enteros algebraicos forman un anillo y $g(\chi_n^{(s)})$ es suma de productos de raíces de la unidad, tenemos que $g(\chi_n^{(s)})$ es también un entero algebraico. Finalmente, notemos que $\Gamma(\alpha)$ es producto de enteros algebraicos, con lo que $\Gamma(\alpha)$ también lo es. □

De este resultado se desprende el siguiente corolario

Corolario 4.4.3. *$\Gamma(\hat{\alpha}_i)$ es entero algebraico para toda $\hat{\alpha}_i \in P$.*

Observación 4.4.4. Por la observación 4.4.1 tenemos que si

$$x^{\mu\hat{\alpha}_i} - (-1)^{n+1}\Gamma(\hat{\alpha}_i) = \prod_{j=1}^{\mu\hat{\alpha}_i}(x - w_{i,j}), \tag{4.21}$$

entonces también cada $w_{i,j}$ es entero algebraico. Además tenemos que

$$\prod_{j=1}^{\mu\hat{\alpha}_i} w_{i,j} = (-1)^{\mu\hat{\alpha}_i}(-1)^{n+1}\Gamma(\hat{\alpha}_i).$$

Lema 4.4.5. *Si $P(t) = \prod_i^{\deg(P(t))}(1 - w_i t)$ ($P(t)$ es como en 4.18), entonces cada w_i es un entero algebraico.*

Demostración. Sabemos que

$$P(t) = \prod_{i=1}^{k}[1 - (-1)^{n+1}\Gamma(\widehat{\alpha}_i)t^{\mu\widehat{\alpha}_i}].$$

Como cada

$$[1 - (-1)^{n+1}\Gamma(\widehat{\alpha}_i)t^{\mu\widehat{\alpha}_i}] = \prod_{j=1}^{\mu\hat{\alpha}_i}(1 - w_{i,j}t),$$

donde los $w_{i,j}$ son como en la observación 4.4.4, tenemos que resultado se sigue. □

Juntando los resultados anteriores y fijándonos en la forma que tienen los polinomios $P_r(t)$ definidos al final de la sección anterior, tenemos el teorema principal de la sección.

Teorema 4.4.6 (Integridad). Si escribimos a $\mathcal{Z}_f(t)$ como

$$\mathcal{Z}_f(t) = \frac{P_1(t)P_3(t)\cdots P_{2(n-1)-1}(t)}{P_2(t)P_2(t)\cdots P_{2(n-1)}(t)}.$$

Entonces $P_0(t) = 1 - t$, $P_{2(n-1)}(t) = 1 - q^{n-1}t$ y para $r = 1, 2, \ldots, 2(n-1)$ tenemos que $P_r(t) = \prod(1 - w_{r,i}t)$, donde los $w_{r,i}$ son ciertos enteros algebraicos.

Ejemplo 4.4.7. Si $f = x_0^3 + x_1^3 + x_2^3 \in \mathbb{F}_4[x_0, x_1, x_2]$, el ejemplo 4.3.34 nos asegura que

$$\mathcal{Z}_f(u) = \frac{(1+2u)^2}{(1-u)(1-4u)},$$

que claramente verifica lo que el teorema establece.

4.5 Análogo a la hipótesis de Riemann

Como los polinomios de la forma $(1 - q^i t)$ son los $P_r(t)$ con $r = 2i$ y $r \neq n-1$, claramente tenemos que el valor absoluto de q^i es $q^{r/2}$ tal y como predice la conjetura W3. Veamos que las raíces recíprocas de $P_{n-1}(t)$ cumplen con que su norma es $q^{n-1/2}$, con lo que quedará totalmente mostrada la validez de W4 para las hipersuperficies de Fermat.

Lema 4.5.1. *Si $\alpha \in \Delta_s$ entonces $|\Gamma(\alpha)| = q^{s(n-1)/2}$.*

Demostración. Si $\alpha = (\chi_0, \chi_i, \cdots, \chi_n)$ entonces

$$\Gamma(\alpha) = \frac{1}{q^s} \prod_{i=0}^{n} \chi_i(a_i)^{-1} g(\chi_i).$$

Como $\chi_i(a_i^{-1})$ es raíz de la unidad, tiene norma igual a uno. Además cada $g(\chi_i)$ tiene norma igual a $q^{s/2}$ (ver teorema 2.4.7 en la página 50 y tomar en cuenta que cada χ_i es un carácter multiplicativo de $\mathbb{F}_{q^s}$). Juntando estos resultados, tenemos que:

$$|\Gamma(\alpha)| = \frac{1}{q^s}(q^{s/2})^{n+1} = q^{s(n-1)/2}.$$

□

Corolario 4.5.2. *Si $[1-(-1)^{n+1}\Gamma(\widehat{\alpha}_i)t^{\mu_{\widehat{\alpha}_i}}] = \prod_{j=1}^{\mu_{\widehat{\alpha}_i}}(1-w_{i,j}t)$, entonces cada $w_{i,j}$ tiene norma igual a $q^{(n-1)/2}$.*

Demostración. Por la observación 4.4.4 sabemos que $w_{i,j}^{\mu_{\widehat{\alpha}_i}} = (-1)^{n+1}\Gamma(\widehat{\alpha}_i)$, por lo que

$$|w_{i,j}|^{\mu_{\widehat{\alpha}_i}} = |w_{i,j}^{\mu_{\widehat{\alpha}_i}}| = |(-1)^{n+1}\Gamma(\widehat{\alpha}_i)| = q^{\mu_{\widehat{\alpha}_i}(n-1)/2}.$$

Así $|w_{i,j}| = q^{(n-1)/2}$. □

De esto, se desprende el siguiente e inmediato corolario.

Corolario 4.5.3. *Si $P(t) = \prod_{i=1}^{k}(1 - W_k)$, entonces $|W_k| = q^{(n-1)/2}$.*

Teorema 4.5.4 (Análogo a la hipótesis de Riemann). Si escribimos a $Z_f(t)$ como:

$$Z_f(t) = \frac{P_1(t)P_3(t)\cdots P_{2(n-1)-1}(t)}{P_2(t)P_2(t)\cdots P_{2(n-1)}(t)},$$

tenemos que $P_r(t) = \prod(1 - w_{r,i}t)$, donde los $w_{r,i}$ tienen norma igual a $q^{r/2}$.

Demostración. Por la forma en que se definieron los polinomios $P_r(t)$, tenemos que el resultado es claro para $r \neq n-1$. Sin embargo, tenemos que $P_{n-1}(t) = P(t)$ si n es par y $P_{n-1} = P(t)(1-q^{r/2}t)$ si n es impar (ver comentarios al final de la sección 4.3)); que por los resultados anteriores vemos que también es verdadero. □

De este teorema se desprende el siguiente corolario que nos permite dar una estimación de los números $\overline{N}_s$.

Corolario 4.5.5. $|\overline{N}_s - (q^{sn} - 1/q - 1)| \leq q^{sk(n-1)/2}$ *donde* $k = \deg P(t)$.

Demostración. Es inmediato del teorema anterior, el corolario que le precede y el corolario 4.3.33 en la página 97. □

Ejemplo 4.5.6. Para el caso en que $f = x_0^3 + x_1^3 + x_2^3 \in \mathbb{F}_4[x_0, x_1, x_2]$ tenemos que

$$\mathcal{Z}_f(t) = \frac{(1+2t)^2}{(1-t)(1-4t)}$$

(ejemplo 4.20), por lo que $P_0(t) = (1-t)$, $P_1(t) = (1+2t)^2$ y $P_2(t) = (1-4)$. que claramente verifica lo que el teorema asegura.

4.6 La ecuación funcional

Sabemos que la función zeta asociada a la hipersuperficie de Fermat determinada por f (f como en 4.1 página 79) está dada por:

$$\mathcal{Z}_f(t) := P(t)^{(-1)^n}/Q(t), \tag{4.22}$$

donde $P(t) = \prod_{i=1}^{k}[1-(-1)^{n+1}\Gamma(\hat{\alpha}_i)]$ y $Q(t) = \prod_{i=0}^{n-1}(1-q^i t)$. Como $\mathcal{Z}_f(1/q^{n-1}t) = P(1/q^{n-1}t)^{(-1)^n}/Q(1/q^{n-1}t)$ estudiemos por separado a $P(1/q^{n-1}t)$ y a $Q(1/q^{n-1}t)$.

Haciendo la substitución encontramos que:

$$\begin{aligned} P(1/q^{n-1}t) &= (-1)^{(n+1)(k+1)}\left[\prod_{i=1}^{k}\Gamma(\hat{\alpha}_i)\right]\left[q^{n-1}t\right]^{-\sum_{i=1}^{k}\mu_{\hat{\alpha}_i}}\prod_{i=1}^{k}\left[1-(-1)^{n+1}(q^{(n-1)\mu_{\hat{\alpha}_i}}/\Gamma(\hat{\alpha}_i))t^{\mu_{\hat{\alpha}_i}}\right]. \\ &= \pm\left[\prod_{i=1}^{k}\Gamma(\hat{\alpha}_i)\right]\left[q^{-M(n-1)}t^{-M}\right]\prod_{i=1}^{k}\left[1-(-1)^{n+1}(q^{(n-1)\mu_{\hat{\alpha}_i}}/\Gamma(\hat{\alpha}_i))t^{\mu_{\hat{\alpha}_i}}\right], \end{aligned} \tag{4.23}$$

donde $M := \sum_{i=1}^{k} \mu_{\hat{\alpha}_i}$.

Estudiemos la relación entre los conjuntos

$$\{q^{(n-1)\mu_{\hat{\alpha}_1}}/\Gamma(\hat{\alpha}_1), q^{(n-1)\mu_{\hat{\alpha}_2}}/\Gamma(\hat{\alpha}_2), \ \ldots, q^{(n-1)\mu_{\hat{\alpha}_k}}/\Gamma(\hat{\alpha}_k)\} \quad \text{y} \quad \{\Gamma(\hat{\alpha}_1), \Gamma(\hat{\alpha}_2), \ldots, \Gamma(\hat{\alpha}_k)\}$$

donde cada $\hat{\alpha}_i \in P$ *y si* $i \neq j$, *entonces* $\hat{\alpha}_j \notin \Theta(\hat{\alpha}_i)$ (recordemos que $\Theta(\hat{\alpha})$ es la órbita de $\hat{\alpha}$ bajo la acción del grupo $< \sigma >\subset \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ en P (ver notación 4.3.28 en la página 95)). También estudiemos al producto $\prod_{i=1}^{k} \Gamma(\hat{\alpha}_i)$

Notación 4.6.1. Denotemos por P/σ al conjunto $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots, \hat{\alpha}_k\}$ donde cada $\hat{\alpha}_i \in P$ es fijo y si $i \neq j$ entonces $\hat{\alpha}_j \notin \Theta(\hat{\alpha}_i)$. Este conjunto está formado por un representante, y sólo uno, de las clases de P bajo la acción de $< \sigma >$.

Notación 4.6.2. Si $\alpha = (\chi_1, \chi_1, \ldots, \chi_n) \in \Delta$, entonces denotemos por $\overline{\alpha}$ al elemento

$$\overline{\alpha} := (\overline{\chi}_1, \overline{\chi}_2, \ldots, \overline{\chi}_n).$$

Notemos que $\overline{\alpha} = \alpha^{-1}$ y que $\overline{\alpha} \in \Delta_{s_\alpha}$.

Lema 4.6.3. *Sea* P *el conjunto primitivo de* Δ. *Si* $\alpha \in P$, *entonces* $\overline{\alpha} = \alpha^{-1} \in P$.

Demostración. Si $\alpha = (\chi_1, \chi_1, \ldots, \chi_n)$, entonces $\overline{\chi}_i \neq \varepsilon$, ya que $\chi_i \neq \varepsilon$. Como $\prod_{i=0}^{n} \chi_i = \varepsilon$, *tenemos que* $\prod_{i=0}^{n} \overline{\chi}_i = \overline{\prod_{i=0}^{n} \chi_i} = \varepsilon$. *Como* α *y* $\alpha^{-1} = \overline{\alpha}$ *tienen el mismo orden, entonces si* $\alpha^{d_s} = \varepsilon$ también $\overline{\alpha}^{d_s} = \varepsilon$. Con esto hemos demostrado que $\overline{\alpha} \in \Delta$; ahora tenemos que demostrar que $\overline{\alpha} \in P$

Observación 4.6.4. Observemos que si $\beta \in \Delta$ es tal que $\beta \in \Delta_{\mu_\beta}$, entonces $\beta \in P$. En efecto, como $\hat{\beta} \in \Delta_{\mu_\beta}$ y $\hat{\beta}' = \beta$, es inmediato que $\beta = \hat{\beta}$ y por lo tanto $\beta \in P$.

Mostremos que $\overline{\alpha} \in \Delta_{\mu_{\overline{\alpha}}}$. Como α y $\overline{\alpha}$ tienen el mismo orden, i.e., $\rho_\alpha = \rho_{\overline{\alpha}}$ (uno es el inverso de otro) entonces $\mu_\alpha = \mu_{\overline{\alpha}}$, pero como $\overline{\alpha} \in \Delta_{\mu_\alpha} = \Delta_{\mu_{\overline{\alpha}}}$, el resultado se sigue. □

Teorema 4.6.5. Sea $\alpha \in \Delta$. Entonces $\Gamma(\overline{\alpha}) = \overline{\Gamma(\alpha)}$.

Demostración. Si $\alpha = (\chi_0, \chi_1, \ldots, \chi_n) \in \Delta_s$, entonces $\Gamma(\overline{\alpha}) = 1/q^s \prod_{i=0}^{n} \overline{\chi}_i(a_i^{-1}) g(\overline{\chi}_i)$. Como por el teorema 2.4.6 en la página 50 sabemos que $g(\overline{\chi}_i) = \chi_i(-1)\overline{g(\chi_i)}$ y como $\prod_i \chi_i = \varepsilon$,

tenemos que

$$\begin{aligned}\Gamma(\overline{\alpha}) &= \frac{1}{q^s}\prod_{i=0}^{n}\chi_i(-1)\prod_{i=0}^{n}\overline{\chi_i(a_i^{-1})g(\chi_i)} \\ &= \overline{\frac{1}{q^s}\prod_{i=0}^{n}\chi_i(a_i^{-1})g(\chi_1)} \\ &= \overline{\Gamma(\alpha)}.\end{aligned}$$

□

Observación 4.6.6. Si $\alpha \in P$, sabemos que $\overline{\alpha} \in P$ por lo que $\overline{\alpha} \in \Theta(\hat{\alpha}_j)$ para algún $\hat{\alpha}_j \in P/\sigma$. Con lo que $\Gamma(\overline{\alpha}) = \Gamma(\hat{\alpha}_j)$.

Proposición 4.6.7. *El mapeo de* $\{\Gamma(\hat{\alpha}_1), \Gamma(\hat{\alpha}_2), \ldots, \Gamma(\hat{\alpha}_k)\}$ *en si mismo dado por* $\Gamma(\hat{\alpha}_i) \longmapsto \overline{\Gamma(\hat{\alpha}_i)}$ *es biyectivo.*

Demostración. La observación anterior nos dice que el mapeo está bien definido. Para ver que es biyectivo, notemos que el mapeo en P dado por $\alpha \longmapsto \overline{\alpha}$ es biyectivo, por lo que nos induce una biyección entre $\{\Gamma(\alpha) : \alpha \in P\}$ dado por $\Gamma(\alpha) \longmapsto \Gamma(\overline{\alpha}) = \overline{\Gamma(\alpha)}$. La parte final de la observación anterior nos permite asegurar que está biyección nos induce una biyección entre $\{\Gamma(\hat{\alpha}_i) : \hat{\alpha} \in P/\sigma\}$ dado por $\Gamma(\hat{\alpha}_i) \longmapsto \overline{\Gamma(\hat{\alpha}_i)}$. □

Observación 4.6.8. Como $\Gamma(\hat{\alpha}_i)\overline{\Gamma(\hat{\alpha}_i)} = |\Gamma(\hat{\alpha}_i)|^2 = q^{\mu_{\hat{\alpha}_i}(n-1)}$, encontramos que la biyección de la proposición anterior puede ser descrita como:

$$\Gamma(\hat{\alpha}_i) \longmapsto q^{\mu_{\hat{\alpha}_i}(n-1)}/\Gamma(\hat{\alpha}_i)$$

por lo que, reordenando en el producto de la ecuación 4.23, tenemos la igualdad

$$\prod_{i=1}^{k}\left[1-(-1)^{n+1}(q^{(n-1)\mu_{\hat{\alpha}_i}}/\Gamma(\hat{\alpha}_i))t^{\mu_{\hat{\alpha}_i}}\right] = \prod_{i=1}^{k}\left[1-(-1)^{n+1}\Gamma(\hat{\alpha}_i)t^{\mu_{\hat{\alpha}_i}}\right] = P(t).$$

Lema 4.6.9. *Sea* $M = \sum_{i=1}^{k}\mu_{\hat{\alpha}_i}$ *con* $\hat{\alpha}_i \in P/\sigma$. *Entonces:*

$$\prod_{i=1}^{k}\Gamma(\hat{\alpha}_i) = \pm q^{M(n-1)/2}.$$

Demostración. Como

$$\begin{aligned}\left[\prod_{i=1}^{k}\Gamma(\hat{\alpha}_i)\right]^2 &= \prod_{i=1}^{k}\Gamma(\hat{\alpha}_i)\prod_{i=1}^{k}\overline{\Gamma(\hat{\alpha}_i)} \text{ (proposición 4.6.7)}\\ &= \prod_{i=1}^{k}\Gamma(\hat{\alpha}_i)\overline{\Gamma(\hat{\alpha}_i)}\\ &= \prod_{i=1}^{k} q^{\mu_{\hat{\alpha}_i}(n-1)} \text{ (observación 4.6.8)}\\ &= q^{M(n-1)},\end{aligned}$$

sacamos raíz cuadrada a ambos lados de la igualdad y obtenemos el resultado deseado. □

Juntando los resultados recién probados, tenemos el siguiente teorema.

Teorema 4.6.10. Sea P(t) como en 4.22, entonces:

$$P(1/q^{n-1}t)^{(-1)^n} = \pm q^{-(-1)^n M(n-1)/2} t^{-(-1)^n M} P(t)^{(-1)^n}.$$

Para la demostración basta substituir los resultados anteriores en 4.23. Finalmente notemos que si $Q(t)$ es como en 4.22, entonces:

$$Q(1/q^{n-1}t) = (-1)^n q^{-n(n-1)/2} t^{-n} Q(t)$$

(para ver está igualdad basta hacer la substitución), por lo que tenemos el teorema más importante de la sección.

Teorema 4.6.11 (La ecuación funcional). La función zeta asociada a la hipersuperficie de de Fermat determinada por $f = a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$, satisface la siguiente ecuación funcional:

$$\mathcal{Z}_f(1/q^{n-1}t) = \pm q^{(n-1)E/2} t^E \mathcal{Z}_f(t),$$

donde $E = n - (-1)^n M$ y $M = \deg P = \sum_{i=1}^{k} \mu_{\hat{\alpha}_i}$.

Ejemplo 4.6.12. En el ejemplo 4.20 vimos que

$$\mathcal{Z}_f(t) = \frac{(1+2t)^2}{(1-t)(1-4t)}.$$

Haciendo la substitución encontramos que

$$\begin{aligned}\mathcal{Z}_f(1/4t) &= \frac{(1+(2/4t))^2}{(1-(1/4t))(1-(4/4t))} \\ &= \frac{(2/4t)^2((4t/2)+1)^2}{(-1/4t)(1-4t)(-4/4t)(1-(4t/4))} \\ &= \frac{(1/4t^2)(1+2t)^2}{(1/4t^2)(1-4t)(1-t)} \\ &= \mathcal{Z}_f(t).\end{aligned}$$

En este caso encontramos que $E = 0$, lo cual coincide con el calculo $E = n - (-1)^n M$ ya que para este caso $n = 2$ y $M = \deg(1+2t)^2 = 2$.

4.7 Grados

Como mencionamos en la sección 4.2, en está sección no demostraremos la conjetura de los "números de Betti" ya que el estudio de los números de Betti escapa de los objetivos de la tesis. Sin embargo, daremos algunos resultados que tienen que ver con lo que esta conjetura expresa.

Escribamos a la fusión zeta asociada a la hipersuperficie de Fermat determinada por f en la forma 4.19. Es decir,

$$\mathcal{Z}_f(t) = \frac{P_1(t)P_3(t)\cdots P_{2(n-1)-1}(t)}{P_2(t)P_2(t)\cdots P_{2(n-1)}(t)}.$$

Denotemos por B_h al grado de $P_h(t)$ (En su articulo [Wei49], Weil llama a cada B_h el h-ésimo número de Betti de $\overline{H}_f(\overline{\mathbb{F}}_q)$). Entonces, si E es como en el teorema 4.6.11, i.e., $E := n - (-1)^n M$ donde $M := \deg P = \sum_{i=1}^{k} \mu_{\hat{a}_i}$, encontramos que:

$$E = \sum_h (-1)^h B_h$$

tal y como establece W4. Esto es gracias a la forma en que se definieron los polinomios $P_h(t)$ (ver página 4.19).

Observación 4.7.1. Si $f = a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$, y suponemos que $q \equiv 1 (\mathrm{mod}\, l)$, entonces $d_s = (l, q^s - 1) = l$ para todo entero positivo s (en particular

$(l, q-1) = l$), por lo que dado $\alpha \in \Delta$, ρ_α divide a $q-1$ y, por lo tanto, $\mu_\alpha = 1$. Esto nos dice que el conjunto primitivo P es subconjunto de Δ_1, más aún, como cada elemento de Δ_1 es su propio primitivo tenemos que $P = \Delta_1$. Esto nos da el siguiente teorema[2].

Como una aplicación inmediata del teorema de la racionalidad (teorema 4.3.32) y la observación anterior, tenemos el siguiente:

Teorema 4.7.2. *Si $f = a_0x_0^l + a_1x_1^l + \cdots + a_nx_n^l \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$, entonces la función zeta asociada a la hipersuperficie determinada por f tiene la forma:*

$$Z_f(t) = \frac{\prod_{(\chi_0,\chi_1,\ \ldots,\chi_n)} \left[1 - (-1)^{n+1}\frac{1}{q}\chi_0(a_0^{-1})\chi_1(a_1^{-1})\cdots\chi_n(a_n^{-1})g(\chi_0)g(\chi_1)\cdots g(\chi_n)t\right]}{(1-t)(1-qt)\cdots(1-q^{n-1}t)},$$

donde los χ_i $i = 0 \ldots n$ son caracteres multiplicativos de $\mathbb{F}_q$ sujetos a las condiciones de que $\chi_i \neq \varepsilon$, $\prod_i \chi_i = \varepsilon$ y $\chi_i^l = \varepsilon$.

Aplicado ahora la proposición 4.3.5 y tomando en cuanta que

$$P(t) = \prod_{(\chi_0,\chi_1,\ \ldots,\chi_n)} \left[1 - (-1)^{n+1}\frac{1}{q}\chi_0(a_0^{-1})\chi_1(a_1^{-1})\cdots\chi_n(a_n^{-1})g(\chi_0)g(\chi_1)\cdots g(\chi_n)t\right],$$

tenemos el siguiente corolario

Corolario 4.7.3. *El grado del polinomio $P(t)$ es igual a $l^{-1}[(l-1)^{n+1} + (-1)^{n+1}(l-1)]$.*

Ejemplo 4.7.4. Para la función zeta

$$Z_f(t) = \frac{(1+2t)^2}{(1-t)(1-4t)}$$

comentada en el ejemplo 4.20 (de hecho al final de cada sección de este capítulo), tenemos que $B_0 = 1$, $B_1 = 2$ y $B_2 = 1$. Además, el ejemplo 4.6.12 nos dice que $E = 0$ lo que coincide totalmente con el calculo $E = \sum_h (-1)^h B_h = 1 - 2 + 1 = 0$. Además, el polinomio $f = x_0^3 + x_1^3 + x_2^3 \in \mathbb{F}_4[x_0, x_1, x_2]$ tal que $4 \equiv 1 (\mathrm{mod}\, 3)$ por lo que, según el corolario anterior, su grado debería de ser $3^{-1}(3-1)^2 + (-1)^2(3-1) = 2$, lo que coincide perfectamente con la realidad

[2]El caso particular $q \equiv 1(\mathrm{mod}\, l)$ lo trabaja Ireland en su libro [IR90] pero lo deduce directamente de las propiedades de las sumas de Gauss y la forma que tienen los números $\overline{N}_s$

Bibliografía

[AK99] N. Anuradha and S.A. Kate Number of points on the projective curves $ay^l = bx^{2l} + cz^{2l}$ defined over finite fields, l an old prime. *Jurnal of Number Theory*, 77:288–313, 1999.

[AP95] I.R. Shafarevich A.N. Parshin, editor. *Number Theory I*, volume 49 of *Encyclopaedia of Mathematical Sciences*. Springer, 1995.

[Dwo60] Bernard Dwork. On te rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 81:631–648, 1960.

[FK88] Eberhard Freitag and Reinhardt Kiehl. *Etale Cohomology and the Weil Conjecture*. Number 13 in A Series of Modern Surveys in Mathematics. Springer-Verlag, Berling Heidelberg, Germany, 1988.

[Har77] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Number 84 in Graduate Text in Mathematics. Springer, 2th edition, 1990.

[LN94] Rudolf Lidl and Harald Niederreiter *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1994.

[Lor96] Dino Lorenzini. *An invitation to Arithmetic Geometry*, volume 9. American Mathematical Socity, 1996.

[Mor96] Patrick Morandi. *Field and Galois Theory*, volume 167 of *Graduate Text in Mahtematics* Springer-Verlag, New York, 1996.

[Rem91] R. Remmert. *Theroy of Complex Functions*, volume 122 of *Graduate Text in Mathematics*. Srpinger-Verlag, New York, 1991.

[Rot94] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Number 148 in Graduate Text in Mathematics. Springer-Verlag, New York, 4th edition, 1994.

[Sil85] Joseog H. Silverman. *The Arithmetic of Eliptic Curves*, volume 106. Springer-Verlag, 1985.

[Ste94] Serguei A. Stepanov. *Arithmetic of Algebraic Curves*. Monographs in Contemporary Mathematics. Consultants Bureau, Moscow, Russia, 1994.

[Wei49] A. Weil. Number of solutions of ecuations over finite fields. *Bull. American Mathematical Society*, 55:497–495, 1949.

Instituto de Matemáticas
Ciudad Universitaria, UNAM
México D.F. 04510
México

buendia@math.unam.mx