Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Licenciatura en Matemática

La función zeta en la geometría algebraica

Tesina Licenciatura en Matemática

LUIS EMILIO BELLO VALVERDE
2017

Profesor Guía: Antonio Laface
Departamento de Matemática,
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Índice general

Agradecimientos

Quiero empezar agradeciendo a mi profesor guía, Antonio Laface, por la gran entrega, apoyo y el conocimiento compartido a mi durante el transcurso de la realización de esta tesina en la cual me generó una gran motivación en los temas que se trabajaron.

También agradezco al profesor Andrea Tironi por su dedicación en revisar esta tesina y sugerir correcciones para una mejor presentación de este documento.

También, quiero agradecer a cada uno de los profesores que me ayudaron en mi formación académica durante los años en el que permanecí en la carrera.

También, quiero agradecer a mi familia por el apoyo que me otorgaron constantemente en estos años que permanecí en la Universidad.

Y a mis amigos, compañeros de la carrera, por su gran cariño y constante apoyo que me ofrecieron en estos años, con lo cual me ayudaron en mi formación académica.

Se agradecen el proyecto FONDECYT Regular N. 1150732 y el proyecto Anillo ACT 1415 PIA Conicyt.

Introducción

En esta tesina se estudia la función zeta local, cuya definición es la siguiente. Sea X una variedad proyectiva suave definida sobre un campo finito $\mathbb{F}_q$, sea $\mathbb{F}_{q^r}$ la extensión de $\mathbb{F}_q$ de grado r y sea $X(\mathbb{F}_{q^r})$ el conjunto de los puntos racionales de X sobre $\mathbb{F}_{q^r}$, es decir los puntos cuyas coordenadas están en $\mathbb{F}_{q^r}$. Denotamos por $N_r(X)$ la cardinalidad de $X(\mathbb{F}_{q^r})$. La función zeta local es

$$Z(X,t) = \exp\left(\sum_{r\geq 1} N_r(X)\frac{t^r}{r}\right).$$

Lo más importante sobre la función zeta son las conjeturas de Weil y su demostración por parte de Deligne, así como están enunciadas en el Teorema 3.1.2. Más precisamente, Weil observó [6] que el número $N_r(X)$ es el numero de punto fijos por la potencia r-esima del homomorfismo de Frobenius, ver Definición 1.3.4. Por esta razón el propuso expresar dicho numero por medio de una formula de punto fijo a la Lefschetz y consecuentemente formuló una serie de conjeturas sobre la función zeta. Dichas conjeturas dicen que $Z(X,t)$ es una fracción de polinomios en t con coeficientes racionales, cuyo grado es dado y cuyos módulos de las raíces son ciertas potencias de q. El camino a la demostración de dichas conjeturas necesitó el desarrollo de la cohomología l-ádica por parte de A. Grothendieck [9], donde posteriormente fueron finalmente probadas por su estudiante P. Deligne [5].

En esta tesina se ha estudiado con más profundidad la función zeta local de curvas algebraicas proyectivas y de hipersupercies cúbicas de dimensión tres. Se ha mostrado que ocupando las conjeturas de Weil, la función zeta de cualquier curva algebraica proyectiva de genero g definida sobre $\mathbb{F}_q$ es de la forma $P_1(t)/(1-t)(1-qt)$. Ocupando la ecuación funcional se prueba que $P_1(t)$ es un polinomio de grado $2g$ cuyos coeficientes tienen una simetría. Esto permite expresar dicho polinomio en función de otro polinomio $Q_1(t)$, con coeficientes racionales, y de grado g. Se mostró que el polinomio $Q_1(t)$ tiene todas sus raíces reales, con módulo acotado por $2\sqrt{q}$. Esto permite encontrar todas las posibles funciones zeta para pares (g,q) pequeñas. Con respecto a la función zeta de una hipersuperficie cubica suave de dimensión tres X se ha estudiado el método de Bombieri y Swinnerton-Dyer. Dicho método permite determinar $N_r(X)$ por medio de un algoritmo cuando X contiene por lo menos una recta L definida sobre $\mathbb{F}_q$. Dicho método ocupa la resolución de la proyección $\phi_L\colon X \dashrightarrow \mathbb{P}^2$ de X por la recta L para reducir el cálculo de $N_r(X)$ al cálculo de los puntos racionales de la curva discriminante del morfismo

$\Gamma_L \subseteq \mathbb{P}^2$ y su cubrimiento doble natural $\tilde{\Gamma}_L$ (un punto de Γ_L representa una unión de dos rectas, mientras un punto de $\tilde{\Gamma}_L$ representa la elección de una de dichas rectas).

La tesina está organizada de la siguiente forma.

En el capítulo 1 se centra sobre el estudio de campos, sus extensiones y el teorema fundamental de la correspondencia de la teoría de Galois. El capítulo se enfoca sobre la teoría de los campos finitos $\mathbb{F}_q$ mostrando como el grupo de Galois de la extensión de campos finitos $\mathbb{F}_{q^r}/\mathbb{F}_q$ es generado por una potencia del homomorfismo de Frobenius. En el capítulo 2 se centra sobre el estudio de variedades algebraicas proyectivas, su definición, grado y morfismos entre ellas. Se desarrollan los conceptos geométricos necesarios para entender el algoritmo de Bombieri y Swinnerton-Dyer: teoría de las cónicas, resolución de la proyección ϕ_L por medio de una explosión de una variedad a lo largo de una recta, curva discriminante de un morfismo. Al final del capítulo se introduce el concepto de punto racional de una variedad. En el capítulo 3 se centra sobre el estudio de la función zeta local, su definición y las Conjeturas de Weil. Luego, se estudia la función zeta de una curva algebraica proyectiva de un género dado y la definición del polinomio $Q_1(t)$. El capítulo finaliza con todos los polinomios $Q_1(t)$ de las curvas proyectivas de genero $g \leq 2$ definidas sobre $\mathbb{F}_3$. Además se estudian dichos polinomios para curvas proyectivas de género $g = 3, 6$, complementando con ejemplos explícitos de computaciones hechas de Magma. En el capítulo 4 se centra sobre el estudio de la función zeta local de una hipersuperficie cúbica X de dimensión tres que contiene al menos una recta. Empezando con la definición de dichas hipersuperficies, la construcción de la curva discriminante Γ_L y su cubrimiento doble $\tilde{\Gamma}_L$. Para finalizar este capítulo, se estudia cómo calcular $N_r(X)$ ocupando el algoritmo de Bombieri y Swinnerton-Dyer. La tesina se concluye con una apéndice de programas Magma ocupados en los Capítulos 3 y 4.

1 Campos

Este capítulo se centra sobre el estudio de campos, sus extensiones y el teorema fundamental de la correspondencia de la teoría de Galois. El capítulo se enfoca sobre la teoría de los campos finitos $\mathbb{F}_q$ mostrando como el grupo de Galois de la extensión de campos finitos $\mathbb{F}_{q^r}/\mathbb{F}_q$ es generado por una potencia del homomorfismo de Frobenius.

1.1. Preliminares

En esta sección se explica el concepto de un campo, además de una de sus propiedades mas fundamentales, la característica, también se explica que es una extensión de campos y algunas de sus elementos mas fundamentales, para terminar se explica sobre los homomorfismos de campos.

Definición 1.1.1. Sea K un conjunto de elementos dotado de las siguientes operaciones binarias

$$+ : K \times K \to K, \qquad (x, y) \mapsto x + y.$$
$$\cdot : K \times K \to K, \qquad (x, y) \mapsto x \cdot y.$$

Se dice que $(K, +, \cdot)$ es un ***campo*** si

1. $\forall a, b, c \in K, (a + b) + c = a + (b + c)$.
2. $\forall a, b \in K, a + b = b + a$.
3. $\exists 0 \in K, \forall a \in K, a + 0 = a$.
4. $\forall a \in K, \exists e \in K, a + e = 0$.
5. $\forall a, b, c \in K, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6. $\forall a, b \in K, a \cdot b = b \cdot a$.
7. $\exists 1 \in K, \forall a - \{0\} \in K, a \cdot 1 = a$.
8. $\forall a - \{0\} \in K, \exists e \in K, a \cdot e = 1$.
9. $\forall a, b, c \in K, a \cdot (b + c) = a \cdot b + a \cdot c$.

Observación 1.1.2. La notación usual de un campo es K.

Ejemplo 1.1.3. El conjunto de los números reales, los números racionales, los números complejos, con las operaciones usuales, son campos.

Definición 1.1.4. Sea K un campo, se define la ***característica*** de K de la siguiente manera

$$\text{Char}(K) = \begin{cases} p, & \text{si p es el menor entero positivo tal que } 1 \cdot p = \underbrace{1 + \ldots + 1}_{\text{p veces.}} = 0. \\ 0, & \text{en otro caso.} \end{cases}$$

Definición 1.1.5. Sean K y k dos campos, una extensión de campos K/k es una inclusión del campo k al campo K. Sea $\alpha \in K$, decimos que α es ***algebraico*** sobre k si el nucleo del homomorfismo $k[x] \to K$ definido por $p(x) \mapsto p(\alpha)$ es no trivial. En este caso el polinomio mónico generador del nucleo se llama el ***polinomio mínimo*** de α, denotado por $p_\alpha(x) \in k[x]$. Se dice que K/k es una extensión ***algebraica*** si cada elemento de K es algebraico sobre k. En otro caso se dice que la extensión K/k es ***transcendental***.

Definición 1.1.6. Sean F, K campos y $\sigma : F \to K$ una aplicación. Decimos que σ es un ***homomorfismo de campos*** si para todo $a, b \in F$ se cumple

- $\sigma(a + b) = \sigma(a) + \sigma(b)$.
- $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

Si σ es inyectiva y sobreyectiva, entonces se dice que σ es un ***isomorfismo de campos***. Si $\sigma : K \to K$ es un isomorfismo de campos entonces se dice que σ es un ***automorfismo*** de K.

1.2. Campos Finitos

En esta sección se introducirá el concepto de un campo finito, como también algunos de sus teoremas mas fundamentales. Estos campos finitos poseen diversas aplicaciones que se trabajan en las secciones 2.4, 3.2, 3.1, 4.1, 4.2.

Definición 1.2.1. Sea K un campo, se dice que K es un *campo finito o campo de Galois* cuando el contiene un número finito de elementos. En particular, si K contiene q elementos, por el Teorema 1.2.3 dicho campo es único a menos de isomorfismos y se denota como $\mathbb{F}_q$.

Teorema 1.2.2. [3, Prop. 11.1.1, Thm. 11.1.4] *Si K es un campo finito de q elementos entonces $q = p^n$, para algún p primo y n entero positivo. Viceversa para cada potencia de primo $q = p^n$ existe un campo finito con esta cardinalidad.*

Demostración. Supongamos que K es un campo finito de q elementos, definimos el homomorfismo de anillos

$$\varphi : \mathbb{Z} \to K \qquad n \mapsto \underbrace{1 + \ldots + 1}_{\text{n veces}}.$$

Recordando la definición de la característica de un campo, notamos que $\operatorname{Ker}(\varphi) = \langle p \rangle$, el cual es un ideal principal de $\mathbb{Z}$, luego, por el teorema fundamental de homomorfismos de anillos, se tiene que φ induce un isomorfismo $\overline{\varphi} : \mathbb{Z}/\operatorname{Ker}(\varphi) \to \varphi(\mathbb{Z})$. Como $\varphi(\mathbb{Z})$ es isomorfo a $\mathbb{F}_p$ tenemos que K es un $\mathbb{F}_p-$espacio vectorial, y dado que K es finito, se tiene que $\dim_{\mathbb{F}_p} K = n$ para algún n entero positivo. Considerando una base $\{u_1, \ldots, u_n\}$ de K, se tiene el siguiente isomorfismo de $\mathbb{F}_p$-espacios vectoriales

$$f : \mathbb{F}_p^n \to K \qquad (\alpha_1, \ldots, \alpha_n) \mapsto \alpha_1 u_1 + \ldots + \alpha_n u_n.$$

Para cada α_i existen p valores distintos, en efecto $|K| = p^n$.

Por otro lado, sea p un número primo y sea $q = p^n$. Sea $L/\mathbb{F}_p$ una extensión de campos tal que el campo L contiene todas las raíces del polinomio $x^q - x$. Dado que la característica es p, la derivada de $x^q - x$ es -1, entonces se tiene que $\operatorname{mcd}(x^q - x, (x^q - x)') = 1$. Así $x^q - x$ es separable y por lo tanto tiene distintas raíces en L. Esto muestra que $K = \{\alpha \in L : \alpha^q = \alpha\}$ es un subconjunto de L que consiste de q elementos. Por el Lema 1.3.6 sigue que K es un subcampo de L, por lo tanto K es un campo finito con $q = p^n$ elementos. □

El siguiente teorema justifica el uso de la notación $\mathbb{F}_q$ para un campo de q elementos.

Teorema 1.2.3. [3, Cor. 11.1.3] *Dos campos finitos de la misma cardinalidad son isomorfos.*

Demostración. Sea K un campo finito con $q = p^n$ elementos. Como el grupo multiplicativo K^* tiene $q - 1$ elementos entonces $\alpha^{q-1} = 1$ para cada $\alpha \in K^*$. Luego todos los elementos de K son raíces del polinomio $x^q - x$. Por lo tanto K es un campo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$. Se concluye recordando que dos campos de descomposición de un mismo polinomio son isomorfos [3, Cor. 5.1.7]. □

1.3. Grupo de Galois

En esta sección se explica lo que es el grupo de Galois de una extensión de campos K/k y el teorema fundamental para luego enfatizar que ocurre en los grupos de Galois de extensiones de campos finitos explicando algunos de sus resultados mas importantes.

Definición 1.3.1. [3, Def. 6.1.1] Sea K/k una extensión de campos. El ***grupo de Galois*** asociado a K/k es

$$\operatorname{Gal}(K/k) = \{\sigma : K \to K : \sigma \text{ es un automorfismo, } \sigma(a) = a, \forall a \in k\}.$$

Definición 1.3.2. Sea K/k una extensión finita de campos, se dice que la extensión es de Galois si

$$|\operatorname{Gal}(K/k)| = [K : k].$$

Teorema 1.3.3. *Sea K/k una extensión de Galois, $\mathcal{F}$ el conjunto de los campos entremedios entre K y k y $\mathcal{H}$ el conjunto de los subgrupos $\operatorname{Gal}(K/k)$. Las siguientes aplicaciones son biyecciones, cada una inversa de la otra:*

$$\begin{aligned} \phi &: \mathcal{F} \to \mathcal{H} & F &\mapsto \operatorname{Gal}(K/F) \\ \psi &: \mathcal{H} \to \mathcal{F} & H &\mapsto K^H, \end{aligned}$$

donde $K^H = \{u \in K : \sigma(u) = u, \forall \sigma \in H\}$ es el subcampo fijo de K por H.

Considerando una extensión de campos finitos $\mathbb{F}_q/\mathbb{F}_p$, se muestran algunas de las propiedades fundamentales de los grupos de Galois de dichas extensiones.

Definición 1.3.4. Sea K un campo de característica $p > 0$. El ***homomorfismo de Frobenius*** es

$$\operatorname{Frob} : K \to K \qquad \alpha \mapsto \alpha^p.$$

La demostración de que Frob es un homomorfismo de campos, se realiza en el siguiente teorema, donde considera el Lema 1.3.6.

Teorema 1.3.5. [3, Thm. 11.1.7] *Si $\mathbb{F}_q$ es un campo finito con $q = p^n$ elementos, entonces*

1. *$\mathbb{F}_q/\mathbb{F}_p$ es una extensión de Galois de grado n.*
2. *El homomorfismo de Frobenius $\operatorname{Frob} : \mathbb{F}_q \to \mathbb{F}_q$ es un automorfismo de $\mathbb{F}_q$, y es la identidad en $\mathbb{F}_p$.*
3. *El homomorfismo de Frobenius Frob genera al grupo de Galois $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Así, existe un isomorfismo de grupos*

$$\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}.$$

Demostración. En la prueba del Teorema 1.2.2, notamos que $x^q - x$ es separable. Entonces [3, Thm. 11.1.2] implica que $\mathbb{F}_q$ es el campo de descomposición de un polinomio separable. Por lo tanto $\mathbb{F}_q/\mathbb{F}_p$ es de Galois. [3, Prop. 11.1.1] implica que $[\mathbb{F}_q : \mathbb{F}_p] = n$ dado que $q = p^n$.

Para la parte **2)**, observamos que por el Lema 1.3.6,

$$\operatorname{Frob}(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \operatorname{Frob}(\alpha) + \operatorname{Frob}(\beta).$$

Dado que tenemos que $\text{Frob}(1) = 1^p = 1$ y

$$\text{Frob}(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \text{Frob}(\alpha)\,\text{Frob}(\beta)$$

esto prueba que Frob es un homomorfismo de anillos. Por el Ejercicio 2 de [3, Section 3.1], Frob es también uno a uno y por lo tanto es sobreyectiva, dado que es una aplicación del campo finito $\mathbb{F}_q$ a sí mismo. Así, Frob es un automorfismo de $\mathbb{F}_q$. Dado que es la identidad en $\mathbb{F}_p$ por [3, Lemma 9.1.2], se concluye que $\text{Frob} \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Para la parte **3)**, notamos que dado que $\mathbb{F}_q/\mathbb{F}_p$ es de Galois, tenemos

$$|\,\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p] = n.$$

Se sigue que el orden de Frob divide a n. Supongamos que Frob^r es la identidad, donde $0 < r < n$. Aquí, Frob^r denota el la composición de Frob r veces consigo mismo, asi que

$$\text{Frob}^r(\alpha) = \underbrace{\text{Frob}(\cdots\text{Frob}(\text{Frob}(\alpha))\cdots)}_{\text{r veces.}} = \underbrace{(\cdots(\alpha^p)^p\cdots)^p}_{\text{r veces.}} = \alpha^{p^r}.$$

Así, si Frob^r es el elemento identidad de $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, entonces

$$\alpha^{p^r} = \alpha$$

para todo $\alpha \in \mathbb{F}_q$. Dado que $0 < r < n$, esto implica que el polinomio $x^{p^r} - x$ de grado $p^r < p^n = q$ tiene q raíces, lo cual es imposible. Por lo tanto Frob tiene orden n, que fácilmente da el isomorfismo deseado $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$. □

De la parte **2)** y **3)** del Teorema 1.3.5 y del Teorema 1.3.3 podemos deducir que el grupo de Galois de una extensión de campos finitos $\mathbb{F}_{p^b}/\mathbb{F}_{p^a}$, con a que divide b, es cíclico con generador Frob^a. Dicho generados es la potencia del homomorfismo de Frobenius que solo fija los elementos que pertenecen al campo $\mathbb{F}_{p^a}$.

Lema 1.3.6. [3, Lemma. 5.3.10] *Sea K un campo de característica $p > 0$ y $\alpha, \beta \in K$, entonces $(\alpha + \beta)^p = \alpha^p + \beta^p$.*

Demostración. Por el teorema del binomio, se tiene que

$$(\alpha+\beta)^p = \sum_{i=0}^{p} \binom{p}{i}\alpha^{p-i}\beta^i = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \ldots + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p$$

donde $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$, y considerando que p divide a $p! = 1 \cdot 2 \cdots p$, y K es un campo de característica p, se tiene que $\binom{p}{i} = 0$ para cada $i = 1, 2, \ldots, p-1$, por lo que prueba el lema. □

2 Variedades algebraicas proyectivas

Este capítulo se centra sobre el estudio de variedades algebraicas proyectivas, su definición, grado y morfismos entre ellas. Se desarrollan los conceptos geométricos necesarios para entender el algoritmo de Bombieri y Swinnerton-Dyer: teoría de las cónicas, resolución de la proyección ϕ_L por medio de una explosión de una variedad a lo largo de una recta, curva discriminante de un morfismo. Al final del capítulo se introduce el concepto de punto racional de una variedad.

En lo que sigue se denotará por $\mathbb{P}^n_K$ el espacio proyectivo de dimensión n sobre el campo K. Cuando el contexto es claro también se denotará simplemente con $\mathbb{P}^n$.

2.1. Preliminares

En esta sección se introducirá el concepto del objeto que estudiaremos en el texto, el de una variedad algebraica proyectiva. También se explica algunas de sus propiedades mas fundamentales y algunas de estas variedades que se estudia con mayor profundidad en las siguientes secciones, estas son las variedades lineales, cuadráticas, cúbicas y las hipersuperficies. Caso aparte será el estudio de las curvas hiperelípticas, donde solo se enfatiza su definición en un espacio afín.

Definición 2.1.1. Sea $P \in K[x_1, \ldots, x_{n+1}]$ un polinomio con coeficientes en el campo K, se dice que P es ***homogéneo*** de grado d si $P(\lambda x_1, \ldots, \lambda x_{n+1}) = \lambda^d P(x_1, \ldots, x_{n+1})$ para todo $\lambda \in K$.

Definición 2.1.2. Sea K un campo y sea $\bar{K}$ su clausura algebraica. Sea el conjunto $S \subset K[x_1, \ldots, x_{n+1}]$ formado por polinomios homogéneos de grado d. Se define el ***lugar de ceros de*** S como

$$V(S) := \{x \in \mathbb{P}^n_{\bar{K}} : f(x) = 0 \text{ } \textit{para todo} \text{ } f \in S\}.$$

Los subconjuntos de $\mathbb{P}^n_{\bar{K}}$ que son de esta forma se denominan ***variedad algebraica proyectiva definida sobre*** K o simplemente ***variedad proyectiva***. Si $S = \{f_1, f_2, \ldots, f_k\}$, la variedad algebraica proyectiva asociada a S se denota $V(S)$ o $V(f_1, f_2, \ldots, f_k)$.

Definición 2.1.3. Se dice que una variedad algebraica proyectiva X definida sobre K es ***irreducible*** si no existe una descomposición $X = X_1 \cup X_2$, con $X_1, X_2 \subset X$ variedades definidas sobre K no vacías.

Definición 2.1.4. Sea $X = V(f_1, f_2, \ldots, f_m) \subset \mathbb{P}^n$ una variedad algebraica proyectiva.

1. Si cada polinomio f_i es de grado 1, X se dice que es una ***variedad lineal***. Por ejemplo, $X = V(x_1 + x_2 + x_3)$ es una variedad lineal.

2. Las variedades proyectivas asociadas a un sólo polinomio homogéneo de grado d se llaman ***hipersuperficies***. En particular, si $d = 2$, se dice que es una hipersuperficie cuádrica y si $d = 3$, se dice que es una hipersuperficie cúbica.

Definición 2.1.5. Se dice que una variedad algebraica proyectiva $X \subset \mathbb{P}^n$ es una ***curva algebraica proyectiva*** de grado d si su dimensión es uno y la intersección de X con un hiperplano general de $\mathbb{P}^n$ es un conjunto finito de cardinalidad d. El ***género*** de una curva algebraica proyectiva $X \subseteq \mathbb{P}^2$ de grado d es

$$g(X) := \frac{(d-1)(d-2)}{2} - a$$

donde a es el número de singularidades de la curva (considerando las multiplicidades de cada una de ellas). Se puede definir también el genero de una curva no plana, pero esto necesita de más teoría así que su definición no va a aparecer aquí.

Definición 2.1.6. Dados tres números enteros positivos a_1, a_2, a_3 tales que cada par es coprimo, el ***plano proyectivo pesado*** $\mathbb{P}(a_1, a_2, a_3)$ es el cociente de $\mathbb{C}^3 \setminus \{(0,0,0)\}$ por la relación de equivalencia definida por $(x_1, x_2, x_3) \sim (\lambda^{a_1} x_1, \lambda^{a_2} x_2, \lambda^{a_3} x_3)$, donde $\lambda \in \mathbb{C}^*$. Un polinomio $f \in \mathbb{C}[x_1, x_2, x_3]$ define un lugar de ceros en $\mathbb{P}(a_1, a_2, a_3)$ si f es homogeneo con respecto a la gradación definida por $\deg(x_i) = a_i$ para cada i.

Definición 2.1.7. Una curva algebraica X se dice que es una ***curva hiperelíptica*** si está definida por una ecuación de la forma

$$y^2 = f(x)$$

donde f es un polinomio de grado $2g + 2$, donde g es el género de X. La clausura proyectiva está en el espacio proyectivo pesado $\mathbb{P}(1, 1, g + 1)$.

Observación 2.1.8. Toda curva de género 2 es hiperelíptica [10, Ex. IV.1.7].

2.2. Cónicas

En la sección anterior se mencionó que una hipersuperficie cuadrática está definida por un único polinomio homogéneo de grado 2. En esta sección, hablaremos de una en particular, la que está definida en el plano proyectivo $\mathbb{P}^2$, la cónica, una variedad algebraica proyectiva muy importante en la construcción del algortimo de Bombieri y Swinnerton-Dyer (ver Sección 4.2).

Definición 2.2.1. Una ***cónica*** es una hipersuperficie de grado dos de $\mathbb{P}^2$.

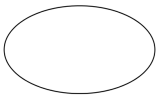
Sea K un campo tal que su característica es distinta de 2 y sea $X \subset \mathbb{P}^2_K$ una cónica. Podemos definir X mediante el polinomio $F(x_1, x_2, x_3) = a{x_1}^2 + 2bx_1x_2 + 2cx_1x_3 + d{x_2}^2 + 2ex_2x_3 + f{x_3}^2$, donde $a, b, c, d, e, f \in K$. Notamos que, por la hipotesis sobre la característica del campo, F puede ser escrito de la siguiente forma

$$F(x_1, x_2, x_3) = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x^t A x, \tag{2.2.1}$$

donde A es una matriz simétrica de orden 3. A partir de esto podemos clasificar las cónicas de la siguiente manera.

Definición 2.2.2. Sea X una cónica definida por el polinomio $x^t Ax$ con coeficientes en un campo K y sea r el rango de la matriz A.

1. X es una cónica irreducible si $r = 3$. Más abajo el dibujo de una cónica irreducible con $K = \mathbb{R}$.

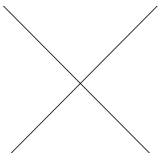


Ejemplo 2.2.3. Sea $X = V({x_1}^2 + {x_2}^2 + {x_3}^2)$ definido sobre el campo finito $\mathbb{F}_3$, se tiene que

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

luego $r = 3$, por lo tanto X es una cónica irreducible.

2. X es una unión de dos rectas distintas si $r = 2$. Más abajo el dibujo de una cónica de rango 2 con $K = \mathbb{R}$.

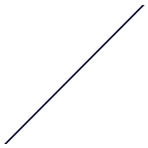


Ejemplo 2.2.4. Sea $X = V({x_1}^2 + {x_2}^2 + 2x_2x_3 + {x_3}^2)$ definido sobre el campo finito $\mathbb{F}_3$, se tiene que

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

donde el símbolo $\sim$ significa semejanza. Luego $r = 2$, por lo tanto X es una cónica formada por la unión de dos rectas distintas.

3. X es una recta doble si $r = 1$. Más abajo el dibujo de una cónica de rango 1 con $K = \mathbb{R}$.



Ejemplo 2.2.5. Sea $X = V({x_1}^2 + 2x_1x_3 + {x_3}^2)$ definido sobre el campo finito $\mathbb{F}_3$, se tiene que

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

donde el símbolo $\sim$ significa semejanza. Luego $r = 1$, por lo tanto X es una cónica formada por una recta doble.

2.3. Morfismos

En esta sección se explica lo que son los morfismos, que es una forma de relacionar distintas variedades proyectivas, para luego introducir dos conceptos que se aplican en nuestra sección principal 4.2, la explosión y la transformada estricta de una variedad.

Definición 2.3.1. [12, Def.3.4] Sean $X \subset \mathbb{P}^n$ y $Y \subset \mathbb{P}^m$ dos variedades algebraicas proyectivas definidas sobre un campo K, un morfismo entre X e Y es una función $F : X \to Y$ donde para cada $p \in X$, existen polinomios homogéneos de grado d $f_1, \ldots, f_{m+1} \in K[x_1, \ldots, x_{n+1}]$ tal que para alguna vecindad $U_p \subset X$ de p, la función $F|_{U_p} : U_p \to Y$ coincide con una función polinomial

$$U_p \to \mathbb{P}^m \qquad q \mapsto [f_1(q) : f_2(q) : \ldots : f_{m+1}(q)]$$

donde $X \not\subset V(f_1, \ldots, f_{m+1})$, o de dicho de otra forma, para cada $p \in X$, los polinomios f_i no se anulan simultáneamente en U_p.

Definición 2.3.2. Sea $X \subset \mathbb{P}^n$ una variedad algebraica proyectiva y $f_1, f_2, \ldots, f_{r+1}$ un conjunto de polinomios homogéneos que no se anulan simultáneamente en X. Entonces $U = X \setminus V(f_1, f_2, \ldots, f_{r+1})$ es un subconjunto abierto de X y se tiene que el siguiente morfismo está bien definido

$$f \colon U \to \mathbb{P}^r \qquad p \mapsto [f_1(p) : f_2(p) : \ldots : f_{r+1}(p)]$$

Considerando $\Gamma = \{(p, f(p)) : p \in U\} \subset X \times \mathbb{P}^r$, se define la ***explosión*** de X en $\{f_1, f_2, \ldots, f_{r+1}\}$ (o equivalentemente, la ***explosión*** de X a lo largo de $V(f_1, f_2, \ldots, f_{r+1})$) como la clausura de Γ, su notación usual es $\tilde{X}$. Las proyecciones del producto cartesiano sobre los dos factores inducen dos morfismos $\pi \colon \tilde{X} \to X$ y $\tilde{f} \colon \tilde{X} \to \mathbb{P}^r$. El morfismo π es el ***morfismo de la explosión*** de X en $\{f_1, f_2, \ldots, f_{r+1}\}$.

Ejemplo 2.3.3. El morfismo $f\colon K^2 \setminus \{(0,0)\} \to \mathbb{P}^1$ definido por $(x_1, x_2) \mapsto [x_1 : x_2]$ no se extiende a un morfismo en todo K^2. Observamos que la clausura del grafico Γ de f en $K^2 \times \mathbb{P}^1$ es

$$\bar{\Gamma} := \{((x_1, x_2), [y_1 : y_2]) \in K^2 \times \mathbb{P}^1 \ : \ x_1 y_2 - x_2 y_1 = 0\}.$$

Dicha variedad se llama la ***explosión*** de K^2 en el punto $(0,0)$. La restricción de la proyección sobre el primer factor define un morfismo $\pi\colon \bar{\Gamma} \to K^2$ que se llama el ***morfismo de explosión***. Observamos que para cada $p \in K^2 \setminus \{(0,0)\}$ el conjunto $\pi^{-1}(p)$ contiene solamente un punto, mientras $\pi^{-1}((0,0)) \simeq \mathbb{P}^1$. Este último subconjunto de $\bar{\Gamma}$ se llama el ***divisor excepcional*** de la explosión. Si lo denotamos con la letra E se puede probar que la restricción de π a su complemento induce un isomorfismo $\bar{\Gamma} \setminus E \to K^2 \setminus \{(0,0)\}$ (aquí solamente hemos mostrado que induce una biyección). Una figura que representa el morfismo π en el caso $K = \mathbb{R}$ es la siguiente.

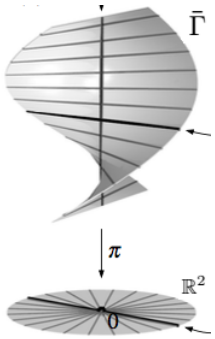


Figura 2.1: Figura tomada en [8, pag. 75].

Definición 2.3.4. Sea $Y \subset X$ una subvariedad cerrada tal que $Y \cap U \neq \phi$, donde $U = X \setminus V(f_1, \ldots, f_r)$, se define la ***transformada estricta*** de Y como la clausura de $Y \cap U$, de forma equivalente, representa la explosión de Y en $\{f_1, \ldots, f_r\}$.

En el ejemplo anterior, se tiene que la transformada estricta de una curva $C \subset K^2$ es la curva $\bar{C} \subseteq \bar{\Gamma}$ definida como la clausura de la curva $\pi^{-1}(C \setminus \{(0,0)\})$ en $\bar{\Gamma}$. Notar que si $p = (0,0)$ es un punto singular de C con multiplicidad d, hay d puntos de $\bar{C}$, contados con multiplicidad, que corresponden a p y que pertenecen al divisor excepcional $E := \pi^{-1}\{(0,0)\}$. En la siguiente imagen se ilustra la transformada estricta de una curva C con una singularidad con multiplicidad 2.

Definición 2.3.5. Sea X y Y variedades proyectivas y f un morfismo entre las variedades. Se define la ***diferencial*** de f en un punto $p \in X$ a la aplicación

$$df_p\colon T_pX \to T_{f(p)}Y \qquad q \mapsto df_p(q) = Jf(q) \cdot q$$

donde $Jf(q)$ es la ***matriz jacobiana de f*** en un punto $q \in T_pX$.

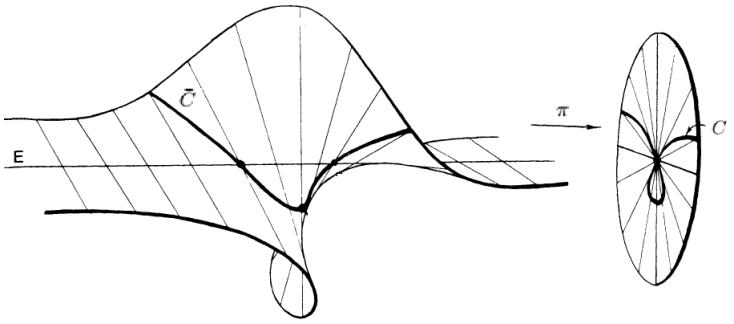


Figura 2.2: Figura tomada en [10, pag. 29].

Definición 2.3.6. Sean X, Y variedades proyectivas suaves definidas sobre un campo K y sea $f\colon X \to Y$ un morfismo sobreyectivo. Se dice que $q \in X$ es un ***punto crítico*** si

$$\mathrm{rk}(df_p) < \dim Y,$$

donde df_p es la diferencial de f en p. Decimos que $f(q) \in Y$ es un ***valor crítico*** si $f^{-1}(f(q))$ contiene un punto crítico. El conjunto de puntos $\{q \in Y : q \textit{ es un valor crítico}\}$ se llama ***variedad discriminante*** del morfismo f.

2.4. Puntos racionales

En esta sección se explica el concepto de un punto racional de una variedad algebraica proyectiva, para luego mostrar un teorema que nos dice la cantidad de puntos racionales de una curva algebraica proyectiva de grado 1 o 2, también se muestra que ocurre con los puntos racionales de algunas curvas proyectivas de grado mayor a 2.

Definición 2.4.1. Sea X una variedad algebraica proyectiva definida sobre un campo K y $p \in X$, se dice que p es un ***punto racional*** de X si todas sus coordenadas están en K. A el conjunto de los puntos racionales de la variedad algebraica proyectiva X se suele denotar por $X(K)$, donde K es el campo de definición.

Teorema 2.4.2. *Toda curva C proyectiva irreducible de grado 1 o 2 definida sobre $\mathbb{F}_q$ tiene $q+1$ puntos racionales.*

Cuando C es de grado mayor a 2, el teorema no es válido dado que existen curvas en donde no contienen puntos racionales. Con Magma [2] estudiamos algunas de estas curvas mediante el programa **NoPoints** descrito en el apéndice. En la siguiente tabla se describen algunas de esas curvas, donde d es el grado de la curva y q es la cardinalidad del campo finito $\mathbb{F}_q$ donde está definida la curva.

d	q	C
3	3	$x_1^3 + 2x_1^2x_2 + x_1x_2^2 + x_2^3 + 2x_1^2x_3 + 2x_2^2x_3 + x_1x_3^2 + x_3^3$
3	5	$x_1^3 + 2x_1^2x_2 + 3x_2^3 + 4x_1^2x_3 + 2x_1x_2x_3 + x_2^2x_3 + 3x_1x_3^2 + 3x_2x_3^2 + 4x_3^3$
3	7	$3x_1^3 + 6x_1^2x_2 + 4x_1x_2^2 + 2x_2^3 + 4x_1^2x_3 + 2x_1x_2x_3 + 6x_1x_3^2 + 6x_2x_3^2 + 3x_3^3$
4	3	$x_1^4 + x_1^2x_2^2 + 2x_2^4 + x_1^2x_2x_3 + x_2^3x_3 + x_1^2x_3^2 + 2x_1x_2x_3^2 + x_2^2x_3^2 + x_1x_3^3 + 2x_2x_3^3 + x_3^4$
5	5	$x_1^5 + 4x_1^4x_2 + 4x_1^2x_2^3 + 2x_1x_2^4 + 2x_2^5 + 2x_1^4x_3 + x_1^3x_2x_3 + 4x_1^2x_2^2x_3 + 3x_2^4x_3 + 4x_1^3x_3^2 + 2x_1^2x_2x_3^2 + x_1x_2^2x_3^2 + 3x_1^2x_3^3 + x_1x_2x_3^3 + 2x_2^2x_3^3 + 3x_1x_3^4 + x_2x_3^4 + 4x_3^5$

Lema 2.4.3. *Sea C una cónica definida sobre un campo finito $\mathbb{F}_q$ de característica impar. Entonces C tiene un punto racional.*

Demostración. (Ver https://goo.gl/DkGkvs) Mediante proyectividades se tiene que cualquier cónica C es proyectivamente equivalente a la cónica $a_0x_1^2 + b_0x_2^2 + c_0x_3^2$. Si algún a_0, b_0, c_0 es cero, en particular c_0, entonces $[0 : 0 : 1]$ es un punto racional de C. Entonces ahora asumimos que $a_0, b_0, c_0 \neq 0$. Por [3, Prop. A.5.3] el grupo multiplicativo $\mathbb{F}_q^*$ es cíclico y tiene orden par $q-1$, entonces contiene exactamente $\frac{q-1}{2}$ cuadrados. Por lo tanto el conjunto $S = \{y^2 : y \in \mathbb{F}_q\}$ tiene cardinalidad $\frac{q+1}{2}$, al igual que el conjunto $T = \{-b_0y^2 - c_0 : y \in \mathbb{F}_q\}$, esto dado que es una transformación lineal de S. Similarmente, el conjunto $U = \{a_0x^2 : x \in \mathbb{F}_q\}$ tiene cardinalidad $\frac{q+1}{2}$. Los conjuntos T y U no pueden ser disjuntos, dado que la suma de sus cardinalidades es mayor que $\mathbb{F}_q$, entonces debe existir algún $-b_0y_0^2 - c_0 \in T$ igual a algún $a_0x_0^2 \in U$, por lo tanto $[x_0 : y_0 : 1]$ es un punto racional de C. □

Demostración del Teorema 2.4.2. Sea $\mathbb{P}^1$ la recta proyectiva definida sobre un campo finito $\mathbb{F}_q$, se tiene que $\mathbb{P}^1 = \mathbb{A}^1 \cup \{p\}$, donde $\mathbb{A}^1$ es la recta afín y p es el punto al infinito, ambos definidos sobre $\mathbb{F}_q$, luego $\mathbb{A}^1$ tiene q puntos racionales y además considerando p se tiene que la recta proyectiva $\mathbb{P}^1$ tiene $q+1$ puntos racionales.

Sea C una curva algebraica proyectiva de grado 1, su ecuación es de la forma $ax_1 + bx_2 + cx_3 = 0$, con $a, b, c \in \mathbb{F}_q$. Por simplicidad supongamos que el punto $[0 : 0 : 1]$ no pertenece a la curva C, es decir $c \neq 0$. Definimos el siguiente morfismo

$$f : C \to \mathbb{P}^1, [x_1 : x_2 : x_3] \mapsto [x_1 : x_2]$$

Considerando la ecuación de C se tiene que $x_3 = -(ax_1 + bx_2)/c$, luego se tiene los siguientes resultados:

- Para cada $Q = [x_1 : x_2] \in \mathbb{P}^1$, existe un punto $P = [x_1 : x_2 : -ax_1/c - bx_2/c] \in C$, por lo tanto f es sobreyectiva.
- Para cada $P = [x_1 : x_2 : x_3] \in C$, la componente x_3 está unicamente determinado por las componentes x_1 y x_2, luego si $f(P_1) = f(P_2)$ entonces $P_1 = P_2$, por lo tanto f es inyectiva.

Luego f define un isomorfismo entre C y $\mathbb{P}^1$, por lo tanto C tiene $q+1$ puntos racionales. Ahora supongamos que C es una curva algebraica proyectiva de grado 2, consideramos $P = [x_1 : x_2 : 1]$ el punto racional de C demostrado en el Lema 2.4.3 y la carta afín $U_3 = \{[x_1 : x_2 : x_3] : x_3 \neq 0\}$, P se corresponde con (x_1, x_2), además, considerando un punto de la recta proyectiva $\mathbb{P}^1$ definido como $Q = [y_1 : y_2 : 1]$ que se corresponde con (y_1, y_2), con estos dos puntos formamos una recta L definida por la ecuación $y - y_2 = \frac{y_2 - x_2}{y_1 - x_1}(x - x_1)$.

Dado que ambos puntos están definidos en $\mathbb{F}_q$, la recta está definida en $\mathbb{F}_q$, además, la intersección entre la cónica C y la recta L está definida por el siguiente sistema de ecuaciones

$$y - y_2 = \frac{y_2 - x_2}{y_1 - x_1}(x - x_1), \quad ax^2 + 2bxy + 2cx + dy^2 + 2ey + f = 0$$

despejando la variable y en la ecuación de L y reemplazando lo obtenido en la ecuación de C, se obtiene una ecuación cuadrática de la forma $s(x) = a_0x^2 + a_1x + a_2 = 0$ de donde se obtienen los puntos P y R.

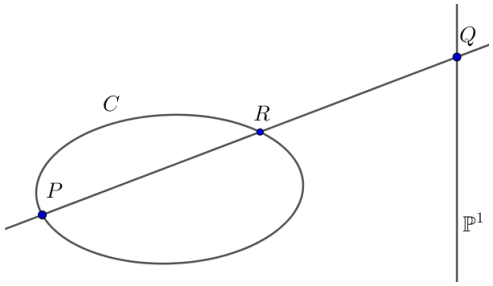


Figura 2.3: Intersección entre la cónica C y la recta L

De las fórmulas de Vieté [13, Remark 3.14], considerando β_1, β_2 las raices de s, se tiene que $\beta_1\beta_2 = \frac{a_2}{a_0}$, y dado que el punto P es unos de los puntos de intersección, unas de las raíces de s (supongamos que β_1) está definido en $\mathbb{F}_q$, esto último y dado que $a_0, a_2 \in \mathbb{F}_q$, se tiene que la otra raíz, es decir el punto R, también está definida en $\mathbb{F}_q$, por lo tanto R también es un punto racional de C. De manera general, considerando P, para cada punto de $\mathbb{P}^1$ se puede formar una recta donde la intersección de esta con la cónica es P y algún punto racional R, es decir, para cada punto de $\mathbb{P}^1$ se corresponde con un punto racional de C, y por otro lado, para cada punto racional $R \neq P$ de C, se puede formar una recta L que pase por P y R y se haga corresponder con un punto Q, un punto de la recta proyectiva $\mathbb{P}^1$. Por lo tanto se puede formar una biyección entre cada punto de $\mathbb{P}^1$ y un punto racional de C y considerando que $\mathbb{P}^1$ tiene $q + 1$ puntos racionales, se tiene que C tiene $q + 1$ puntos racionales. □

Ejemplo 2.4.4. Sea $X = V({x_1}^2 + {x_2}^2 - {x_3}^2)$ la variedad algebraica proyectiva definida sobre el campo finito $\mathbb{F}_3$. Por el Teorema 2.4.2, se tiene que X tiene 4 puntos racionales. Estos son $[0 : 1 : 1], [0 : 2 : 2], [1 : 0 : 1], [2 : 0 : 2]$.

3 La función zeta local

Este capítulo se centra sobre el estudio de la función zeta local, su definición y las Conjeturas de Weil. Luego, se estudia la función zeta de una curva algebraica proyectiva de un género dado y la definición del polinomio $Q_1(t)$. El capítulo finaliza con todos los polinomios $Q_1(t)$ de las curvas proyectivas de genero $g \leq 2$ definidas sobre $\mathbb{F}_3$. Además se estudian dichos polinomios para curvas proyectivas de género $g = 3, 6$, complementando con ejemplos explícitos de computaciones hechas con Magma.

3.1. Preliminares

En esta sección se introducirá lo que es la función zeta de una variedad algebraica proyectiva sobre un campo finito, lo que nos permitirá contar los puntos racionales de dicha variedad sobre el campo finito y de las extensiones finitas de dicho campo. Luego se enuncia las conjeturas de A. Weil que nos entrega diversas propiedades que cumple la función zeta.

Definición 3.1.1. [4, Pág. 21] Sea X una variedad algebraica proyectiva sobre un campo finito $\mathbb{F}_q$. Para cada $r \geq 1$, definimos $N_r(X) = \mathrm{Card}(X(\mathbb{F}_{q^r}))$. La ***función zeta local*** de X es la siguiente serie formal

$$Z(X,t) = \exp\left(\sum_{r\geq 1} N_r(X)\frac{t^r}{r}\right). \tag{3.1.1}$$

Recordamos aquí las conjeturas de Weil, probadas por Deligne [5], sobre la función zeta de una variedad algebraica proyectiva definida sobre un campo finito.

Teorema 3.1.2. [11, Thm. 2.2] *Sea $\mathbb{F}_q$ un campo finito con q elementos y X una variedad algebraica proyectiva suave de dimensión n definida sobre $\mathbb{F}_q$.*

- *(**Racionalidad**)*
$$Z(X,t) \in \mathbb{Q}(t).$$
- *(**Ecuación funcional**) Existe un entero ε (la característica de Euler de X) tal que*
$$Z(X, q^{-n}t^{-1}) = \pm q^{n\varepsilon/2}t^{\varepsilon}Z(X,t)$$

- *(**Hipótesis de Riemann**) Existe una factorización*

$$Z(X,t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}.$$

donde cada $P_i(t) \in \mathbb{Z}[t]$. Además $P_0(t) = 1-t, P_{2n}(t) = 1-q^n t$, y para cada $1 \leq i \leq 2n-1$, los factores de $P_i(t)$ (sobre $\mathbb{C}$) son

$$P_i(t) = \prod_j (1-\alpha_{ij}t) \text{ con } |\alpha_{ij}| = q^{i/2}.$$

3.2. Curvas

En esta sección se muestra, ocupando las conjeturas de Weil, la función zeta de una curva algebraica proyectiva suave de género g. También, se muestra la construcción de un polinomio que llamaremos Q_1, su relación con la función zeta de una curva algebraica proyectiva, y algunas de sus propiedades.

Proposición 3.2.1. *Sea X una curva algebraica proyectiva suave de género g definida sobre un campo finito $\mathbb{F}_q$. Luego la función zeta de X está dada por*

$$Z(X,t) = \frac{P_1(t)}{(1-t)(1-qt)}$$

donde $P_1(t) = \sum_{i=0}^{2g} a_i t^i$ es un polinomio con coeficientes enteros de grado $2g$ tales que $a_0 = 1$ y

$$a_{2g-i}q^{i-g} = a_i \qquad \text{para cada } i = 0,\ldots,g.$$

Observación 3.2.2. Esta Proposición fue mostrada en 1931 por el matemático F.K.Schmidt [7], años antes de que A. Weil enunciara las conjeturas mencionadas anteriormente.

Observación 3.2.3. Notar que si X es una curva algebraica proyectiva de género 0 se tiene que el polinomio $P_1(t)$ es de grado 0, luego $P_1(t) = 1$. Por lo tanto se tiene que la función zeta de X es

$$Z(X,t) = \frac{1}{(1-t)(1-qt)}.$$

Proposición 3.2.4. *Existe un polinomio $Q_1(x) = \sum_{i=0}^{g} b_i x^i$ de grado g con coeficientes racionales tal que la siguiente igualdad es cierta:*

$$Q_1\left(\frac{1}{t} + qt\right) = \frac{1}{t^g}P_1(t).$$

Además las raíces de Q_1 son todas reales de la forma $\dfrac{1}{\alpha} + q\alpha$, donde α es una raíz de P_1, con valor absoluto acotado por $2\sqrt{q}$.

Demostración de la Proposición 3.2.1. Considerando que $n = \dim(X) = 1$ y por [8, Ex. 13.16] tenemos $\varepsilon = 2-2g$. Sea d el grado de $P_1(t)$ es decir $P_1(t) = \sum_{i=0}^{d} a_i t^i$. Luego, por la ecuación funcional se obtiene lo siguiente

$$\begin{aligned} Z(X, q^{-1}t^{-1}) = \pm(qt^2)^{1-g} Z(X,t) &\Leftrightarrow \frac{P_1(q^{-1}t^{-1})}{P_0(q^{-1}t^{-1})P_2(q^{-1}t^{-1})} = \pm(qt^2)^{1-g}\frac{P_1(t)}{P_0(t)P_2(t)} \\ &\Leftrightarrow \frac{P_1(q^{-1}t^{-1})}{(1-qt)(1-t)/(qt^2)} = \pm(qt^2)^{1-g}\frac{P_1(t)}{(1-t)(1-qt)} \\ &\Leftrightarrow q^g t^{2g} P_1(q^{-1}t^{-1}) = \pm P_1(t) \\ &\Leftrightarrow q^g t^{2g} \sum_{i=0}^{d} a_i (q^{-1}t^{-1})^i = \pm \sum_{i=0}^{d} a_i t^i \\ &\Leftrightarrow \sum_{i=0}^{d} a_i q^{g-i} t^{2g-i} = \pm \sum_{i=0}^{d} a_i t^i. \end{aligned}$$

De lo anterior, igualando los grados de los dos polinomios, se deduce la igualdad $d = 2g$. Cambiando el indice de sumación de i hacia $2g - i$ el primer polinomio se cambia con $\sum_{i=0}^{2g} a_{2g-i} q^{i-g} t^i$. Se deduce que se cumplen las siguientes igualdades

$$a_{2g-i} q^{i-g} = a_i \qquad \text{para cada } i = 0, \ldots, g.$$

Finalmente $a_0 = P_1(0) = Z(X,0) = \exp\left(\sum_{r\geq 1} 0\right) = 1$. □

Demostración de la Proposición 3.2.4. Por la Proposición 3.2.1 tenemos la siguiente igualdad entre polinomios de Laurent $P_1(t)/t^g = t^{-g} + a_1 t^{1-g} + a_2 t^{2-g} + \ldots + a_g + a_{g-1}qt + \ldots + q^g t^g$. Vamos a probar que existe un polinomio $Q_1(x) = \sum_{i=0}^{g} b_i x^i$ tal que

$$Q_1\left(\frac{1}{t} + qt\right) = \frac{1}{t^g} P_1(t).$$

Se tiene que

$$\begin{aligned} Q_1\left(\frac{1}{t} + qt\right) &= \sum_{i=0}^{g} b_i \left(\frac{1}{t} + qt\right)^i \\ &= \sum_{i=0}^{g}\sum_{j=0}^{i} b_i \binom{i}{j} \left(\frac{1}{t}\right)^j (qt)^{i-j} \qquad \text{(por el teorema del binomio)} \\ &= \sum_{i=0}^{g}\sum_{j=0}^{i} b_i \binom{i}{j} q^{i-j} t^{i-2j}. \end{aligned}$$

Sea $l \geq 0$ entero tal que $i-2j=l$, se tiene que $j=\dfrac{i-l}{2}$, y dado que $0 \leq i \leq g, 0 \leq j \leq i$ se obtiene $0 \leq j \leq \lfloor \frac{g-l}{2} \rfloor$. Luego igualando los terminos de $Q_1(t^{-1}+qt)$ y $t^{-g}P_1(t)$ con potencias positivas obtenemos

$$\sum_{l=0}^{g} \left(\sum_{j=0}^{\lfloor \frac{g-l}{2} \rfloor} b_{l+2j} \binom{l+2j}{j} q^{l+j} \right) t^l = \sum_{l=0}^{g} a_{g-l} q^l t^l.$$

Por lo tanto obtenemos lo siguiente

$$a_{g-l} = \sum_{j=0}^{\lfloor \frac{g-l}{2} \rfloor} b_{l+2j} \binom{l+2j}{j} q^j.$$

La matriz que multiplica las variables b_i en las ecuaciones lineales de arriba es triangular superior con entradas igual a 1 en la diagonal principal (ver Ejemplos 3.3.3 y 3.3.4). Por lo tanto las variables b_i se pueden expresar de manera única como combinaciones lineales de las variables a_j con coeficientes enteros. Terminamos observando que si $\alpha \in \mathbb{C}$ es una raíz de P_1 entonces

$$Q_1\left(\frac{1}{\alpha}+q\alpha\right) = \frac{1}{\alpha^g} P_1(\alpha) = 0$$

Por lo tanto $\frac{1}{\alpha}+q\alpha$ es una raíz de Q_1. Considerando que $\overline{\alpha}$ también es una raíz de P_1, de las conjeturas de Weil se tiene que $|\alpha| = \frac{1}{q^{1/2}}$, luego $\alpha\overline{\alpha} = |\alpha|^2 = \frac{1}{q}$, en efecto

$$\begin{aligned} \overline{\frac{1}{\alpha}+q\alpha} &= \frac{1}{\overline{\alpha}} + q\overline{\alpha} \\ &= q\alpha + \frac{q}{q\alpha} \\ &= \frac{1}{\alpha} + q\alpha \end{aligned}$$

Por lo tanto $\frac{1}{\alpha}+q\alpha$ es una raíz real de Q_1. El valor absoluto de dicha raíz es

$$\begin{aligned} \left|\frac{1}{\alpha}+q\alpha\right| &= \left|\frac{1+q\alpha^2}{\alpha}\right| \\ &= \frac{|1+q\alpha^2|}{|\alpha|} \\ &= \sqrt{q}|1+q\alpha^2| \\ &\leq \sqrt{q}(1+|q\alpha^2|) \\ &\leq 2\sqrt{q}. \end{aligned}$$

□

Observación 3.2.5. Notar que si $l = g$, se obtiene que

$$a_0 = \sum_{j=0}^{\lfloor 0 \rfloor} b_{g+2j} \binom{g+2j}{j} q^j = b_g$$

y considerando que $a_0 = 1$, se obtiene que $b_g = 1$.

De la observación anterior se omitirá el cálculo del término b_g.

3.3. Ejemplos

En esta sección, ocupando los programas de Magma **PolQ1**, **Hyper**, **FuncZeta** descritos en el apéndice y además de los teoremas relacionados a Q_1 de la sección anterior, se muestran ejemplos de los polinomios Q_1 y de la función zeta de ciertas curvas proyectivas suaves de género g.

Ejemplo 3.3.1. Sea X una curva algebraica proyectiva suave de género $g = 1$, considerando la proposición anterior se tiene

$$a_1 = \sum_{j=0}^{\lfloor \frac{1}{2} \rfloor} b_{2j} \binom{2j}{j} q^j = b_0$$

Por lo tanto el polinomio Q_1 es

$$Q_1(x) = a_1 + x$$

Notar que la raíz de Q_1 es $-a_1$ y de la Proposición 3.2.4, se tiene que $|a_1| \leq 2\sqrt{q}$, considerando el campo finito $\mathbb{F}_3$, se tiene que $|a_1| \leq 2\sqrt{3} \approx 3,46$ y dado que Q_1 tiene coeficientes enteros, se tiene que $a_1 \in [-3, 3]$, luego los posibles polinomios Q_1 son $\{t, t \pm 1, t \pm 2, t \pm 3\}$. Por [10, Prop. IV.4.6] todas las curvas elípticas sobre un campo de característica impar son de la forma $y^2 = x^3 + Ax + B$. Ocupando el programa **Hyper** y **PolQ1**, se deduce que todos los posibles polinomios Q_1 descritos anteriormente se cumplen para ciertas curvas elípticas.

```
{PolQ1(f,3) : f in Hyper(1,3)};
{ t - 3, t + 3, t, t - 1, t + 1, t - 2, t + 2 }
```

Ejemplo 3.3.2. Sea X una curva algebraica proyectiva suave de género $g = 2$, considerando la proposición anterior se tiene

$$a_2 = \sum_{j=0}^{\lfloor \frac{2}{2} \rfloor} b_{2j} \binom{2j}{j} q^j = b_0 + 2b_2 q = b_0 + 2q \qquad a_1 = \sum_{j=0}^{\lfloor \frac{1}{2} \rfloor} b_{1+2j} \binom{1+2j}{j} q^j = b_1$$

Por lo tanto el polinomio Q_1 es $Q_1(x) = (a_2 - 2q) + a_1x + x^2$. De la Observación 2.1.8 se tiene que toda curva de género 2 es una curva hiperelíptica definida por $y^2 = f(x)$ donde f es un polinomio de grado 6. Con Magma, usando el programa **Hyper** y **PolQ1** descritos en el apéndice, determinamos los polinomios Q_1 de cada curva algebraica proyectiva de género 2 sobre el campo finito $\mathbb{F}_3$.

```
{PolQ1(f,3) : f in Hyper(2,3)};
```

Ejemplo 3.3.3. Sea X una curva algebraica proyectiva suave de género $g = 3$, se tiene

$$a_3 = \sum_{j=0}^{\lfloor \frac{3}{2} \rfloor} b_{2j} \binom{2j}{j} q^j = b_0 + 2b_2q \qquad a_2 = \sum_{j=0}^{\lfloor \frac{2}{2} \rfloor} b_{1+2j} \binom{1+2j}{j} q^j = b_1 + 3b_3q$$

$$a_1 = \sum_{j=0}^{\lfloor \frac{1}{2} \rfloor} b_{2+2j} \binom{2+2j}{j} q^j = b_2$$

Con lo cual se obtiene el sistema lineal $Mb = a$ con

$$M = \begin{pmatrix} 1 & 0 & 2q & 0 \\ 0 & 1 & 0 & 3q \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}, \qquad a = \begin{pmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix}$$

Como el determinante de la matriz M es 1 luego el sistema tiene una única solución. Se tiene que

$$M^{-1} = \begin{pmatrix} 1 & 0 & -2q & 0 \\ 0 & 1 & 0 & -3q \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

luego la solución esta dada por $b = M^{-1}a$, donde

$$b = (a_3 - 2a_1q, a_2 - 3q, a_1, 1)^t$$

Por lo tanto el polinomio Q_1 es

$$Q_1(x) = a_3 - 2a_1q + (a_2 - 3q)x + a_1x^2 + x^3$$

Consideramos una curva algebraica proyectiva C de género 3 definida sobre el campo finito $\mathbb{F}_3$. De las fórmulas de Vieté [13, Remark 3.14], considerando $\beta_1, \beta_2, \beta_3$ las raices del polinomio Q_1 asociado a C, se tiene que

$$\beta_1 + \beta_2 + \beta_3 = -b_2, \quad \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = b_1, \quad \beta_1\beta_2\beta_3 = -b_0$$

Luego considerando la Proposición 3.2.4,

$$|b_2| = |\beta_1+\beta_2+\beta_3| \leq 6\sqrt{q}, \quad |b_1| = |\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3| \leq 12q, \quad |b_0| = |\beta_1\beta_2\beta_3| \leq 8\sqrt{q^3}$$

En particular, con $q = 3$, se tiene que,

$$|b_2| \leq 6\sqrt{3} \approx 10,4, \quad |b_1| \leq 36, \quad |b_0| \leq 24\sqrt{3} \approx 41,5$$

Considerando que el polinomio Q_1 tiene coeficientes enteros, se tiene que $b_0 \in [-41, 41]$, $b_1 \in [-36, 36]$ y $b_2 \in [-10, 10]$. Luego hay 127,239 polinomios que satisfacen las desigualdades dadas. Con Magma, ocupando el programa **CandidatosQ1** descrito en el apéndice, se analizan cuales de éstos polinomios, las 3 raíces sean reales y satisfacen las condiciones descritas en la Proposición 3.2.4.

```
#CandidatosQ1(3,3);
677
```

Se concluye que hay 677 polinomios.

Ejemplo 3.3.4. Sea X una curva algebraica proyectiva suave de género $g = 6$, se tiene

$$a_6 = \sum_{j=0}^{\lfloor \frac{6}{2} \rfloor} b_{2j}\binom{2j}{j}q^j = b_0 + 2b_2q + 6b_4q^2 + 20b_6q^3, \quad a_3 = \sum_{j=0}^{\lfloor \frac{3}{2} \rfloor} b_{3+2j}\binom{3+2j}{j}q^j = b_3 + 5b_5q$$

$$a_5 = \sum_{j=0}^{\lfloor \frac{5}{2} \rfloor} b_{1+2j}\binom{1+2j}{j}q^j = b_1 + 3b_3q + 10b_5q^2 \qquad a_2 = \sum_{j=0}^{\lfloor \frac{2}{2} \rfloor} b_{4+2j}\binom{4+2j}{j}q^j = b_4 + 6b_6q,$$

$$a_4 = \sum_{j=0}^{\lfloor \frac{4}{2} \rfloor} b_{2+2j}\binom{2+2j}{j}q^j = b_2 + 4b_4q + 15b_6q^2, \qquad a_1 = \sum_{j=0}^{\lfloor \frac{1}{2} \rfloor} b_{5+2j}\binom{5+2j}{j}q^j = b_5$$

Con lo cual se obtiene el sistema lineal $Mb = a$ con

$$M = \begin{pmatrix} 1 & 0 & 2q & 0 & 6q^2 & 0 & 20q^3 \\ 0 & 1 & 0 & 3q & 0 & 10q^2 & 0 \\ 0 & 0 & 1 & 0 & 4q & 0 & 15q^2 \\ 0 & 0 & 0 & 1 & 0 & 5q & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 6q \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \end{pmatrix}, \qquad a = \begin{pmatrix} a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix}$$

Como la determinante de la matriz M es 1 luego el sistema tiene una única solución. Se

tiene que

$$M^{-1} = \begin{pmatrix} 1 & 0 & -2q & 0 & 2q^2 & 0 & -2q^3 \\ 0 & 1 & 0 & -3q & 0 & 5q^2 & 0 \\ 0 & 0 & 1 & 0 & -4q & 0 & 9q^2 \\ 0 & 0 & 0 & 1 & 0 & -5q & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -6q \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Luego la solución esta dada por $b = M^{-1}a$, donde

$$b = (a_6 - 2a_4q + 2a_2q^2 - 2q^3, a_5 - 3a_3q + 5a_1q^2, a_4 + 4a_2q + 15q^2, a_3 + 5a_1q, a_2 - 6q, a_1, 1)^t.$$

Por lo tanto el polinomio Q_1 es

$$\begin{aligned} Q_1(x) = {} & a_6 - 2a_4q + 2a_2q^2 - 2q^3 + (a_5 - 3a_3q + 5a_1q^2)x + (a_4 + 4a_2q + 15q^2)x^2 \\ & + (a_3 + 5a_1q)x^4 + (a_2 - 6q)x^5 + a_1x^5 + x^6. \end{aligned}$$

Ejemplo 3.3.5. Sea X la curva de Fermat definida por la variedad $X = V({x_1}^3 + {x_2}^3 + {x_3}^3)$ sobre el campo finito $\mathbb{F}_5$. Mediante el programa Magma podemos definir la variedad X, considerando en particular el campo finito $\mathbb{F}_5$.

```
K := GF(5);
P<[x]> := ProjectiveSpace(K,2);
X := Curve(P,x[1]^3+x[2]^3+x[3]^3);
```

Ocupando el programa **FuncZeta** descrito en el apéndice, podemos obtener los valores $N_1(X), N_2(X), \ldots, N_r(X)$ y la función zeta de X. En particular, con $r = 5$, se obtiene lo siguiente

```
FuncZeta(X,5);
[6, 36, 126, 576, 3126 ]
(5*t^2 + 1)/(5*t^2 - 6*t + 1)
```

En particular, se tiene que $N_4(X) = 576$, es decir, hay 576 puntos racionales de X en el campo $\mathbb{F}_{5^4}$. Mediante la función **PolQ1**, podemos obtener el polinomio Q_1.

```
_,Z := FuncZeta(X,5);
Q1 := PolQ1(Q!Numerator(Z));
t
```

Por lo tanto $Q_1(x) = x$.

Observación 3.3.6. Otra manera de determinar el valor de $N_r(X)$ para algunos valores de r es con el siguiente comando

```
[#Points(BaseChange(X,GF(5^r))) : r in [1..5]];
[ 6, 36, 126, 576, 3126 ]
```

4 El metodo de Bombieri y Swinnerton-Dyer

Este capítulo se centra sobre el estudio de la función zeta local de una hipersuperficie cúbica X de dimensión tres que contiene al menos una recta. Empezando con la definición de dichas hipersuperficies, la construcción de la curva discriminante Γ_L y su cubrimiento doble $\tilde{\Gamma}_L$. Para finalizar este capítulo, se estudia cómo calcular $N_r(X)$ ocupando el algoritmo de Bombieri y Swinnerton-Dyer.

4.1. Hipersuperficies cúbicas de dimensión tres

En esta sección se explica lo que es una hipersuperficie cúbica de dimensión tres, para luego introducir, la curva discriminante asociada a un fibrado de cónicas, junto con algunas de sus propiedades mas fundamentales. Se sigue la construcción hecha en [4].

Definición 4.1.1. Sea $X \subset \mathbb{P}^4_K$ una variedad algebraica proyectiva, se dice que X es una hipersuperficie cúbica si X está definido por un único polinomio homogéneo p de grado 3.

Sea $X \subset \mathbb{P}^4$ una hipersuperficie cúbica suave de dimensión tres definida sobre un campo K. Observamos que X no puede contener un plano. Para probarlo, a menos de cambios de coordenadas podemos suponer que las ecuaciones del plano sean $x_1 = x_2 = 0$. Entonces X estaría definido por un polinomio homogéneo $f = x_1 f_1 + x_2 f_2$, donde f_1, f_2 son formas cuadráticas. Como todas las derivadas parciales de f se anulan en el subconjunto no vacío $x_1 = x_2 = f_1 = f_2 = 0$ de $\mathbb{P}^4_{\bar{K}}$, luego X sería singular, una contradicción.

Supongamos ahora que la característica de K sea distinta de 2. Sea L la recta definida por el conjunto $\{[x_1 : x_2 : x_3 : x_4 : x_5] \in \mathbb{P}^4 : x_1 = x_2 = x_3 = 0\}$ y supongamos que L está contenida en X. Podemos escribir la ecuación de X de la siguiente manera:

$$f + 2q_1x_4 + 2q_2x_5 + \ell_1x_4^2 + 2\ell_2x_4x_5 + \ell_3x_5^2 = 0,$$

donde todos los coeficientes son polinomios homogéneos de $K[x_1, x_2, x_3]$. Además f es una forma cúbica, q_1, q_2 son formas cuadráticas y ℓ_1, ℓ_2, ℓ_3 son formas lineales. Consideramos el plano $\mathbb{P}^2 \subset \mathbb{P}^4$ definido por el conjunto $\{[x_1 : x_2 : x_3 : x_4 : x_5] \in \mathbb{P}^4 : x_4 = x_5 = 0\}$

para definir el siguiente ***fibrado de cónicas*** (es decir cualquier fibra de ϕ_L es una cónica):

$$\phi_L \colon X \setminus L \to \mathbb{P}^2 \qquad [x_1 : x_2 : x_3 : x_4 : x_5] \mapsto [x_1 : x_2 : x_3]. \tag{4.1.1}$$

Dado un punto $p = [x_1 : x_2 : x_3] \in \mathbb{P}^2$ la fibra $\phi_L^{-1}(p)$ genera un plano H_p que contiene a la recta L. Luego la intersección $X \cap H_p$ es igual a $L + C_p$, donde C_p es una cónica (no completa). Una ecuación homogénea de C_p es la siguiente

$$f y_1^2 + 2q_1 y_1 y_2 + 2q_2 y_1 y_3 + \ell_1 y_2^2 + 2\ell_2 y_2 y_3 + \ell_3 y_3^2 = 0.$$

Por 2.2.1 la ecuación de cualquier cónica puede ser expresada como $y^t A y = 0$, con $y \in \mathbb{P}^2$ y A una matriz simétrica de orden 3. Considerando la ecuación de la cónica C_p se tiene que

$$A = \begin{pmatrix} f & q_1 & q_2 \\ q_1 & \ell_1 & \ell_2 \\ q_2 & \ell_2 & \ell_3 \end{pmatrix}. \tag{4.1.2}$$

La curva discriminante Γ_L asociada al morfismo ϕ_L está definida por la ecuación $\det(A) = 0$, es decir, cuando el rango de A es menor a 3. Por lo que Γ_L es una curva formada por los puntos $p \in \mathbb{P}^2$ tales que C_p es una unión de dos rectas o una recta doble (ver 2.2.2). Además, notar que

$$\det(A) = f(\ell_1\ell_3 - {\ell_2}^2) - q_1(q_1\ell_3 - q_2\ell_2) + q_2(q_1\ell_2 - q_2\ell_1),$$

lo que muestra que Γ_L está definida por un polinomio homogéneo de grado 5. Además, por la Definición 2.1.5, su género es a lo máximo 6, por lo tanto Γ_L puede tener a lo más 6 singularidades. Bombieri y Swinnerton-Dyer en [1, Lemma 2] demuestran que si Γ_L tiene singularidades, estas son puntos dobles simples, es decir, puntos donde la curva se intersecta de tal manera que dos ramas de la curva tienen distintas rectas tangentes. En particular, cada uno de esos puntos baja el género de la curva de 1 y representa una de las rectas dobles de la fibración. Se tiene de forma natural el cubrimiento doble definido por el morfismo $\varrho : \tilde{\Gamma}_L \to \Gamma_L$ donde cada punto de $\tilde{\Gamma}_L$, representa una de las dos rectas sobre un punto de Γ_L. Es decir, si $p \in \tilde{\Gamma}_L$ entonces $\varrho(p)$ es un punto de Γ_L tal que si C_p es una unión de dos rectas, entonces p está asociado a una de esas dos rectas, o si C_p es una recta doble, p está asociado a esta recta.

4.2. Algoritmo de Bombieri y Swinnerton-Dyer

En esta sección se prueba el siguiente resultado de Bombieri y Swinnerton-Dyer que permite comparar el número de puntos racionales de una hipersuperficie cúbica X de $\mathbb{P}^4$ definida sobre un campo finito $\mathbb{F}_q$, con q impar, que contiene una recta L con el número de puntos de la curva discriminante y su cubrimiento doble.

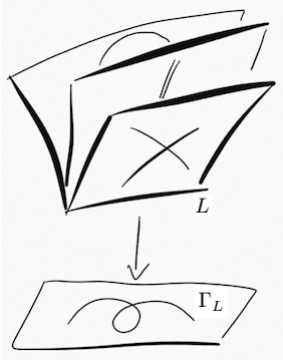


Figura 4.1: Construcción de la curva discriminante Γ_L.

Proposición 4.2.1 ([4, Prop.4.5]). *Sea $X \subset \mathbb{P}^4$ una variedad algebraica proyectiva de dimensión tres suave definida sobre $\mathbb{F}_q$, con q impar, y supongamos que X contiene una recta L definida en $\mathbb{F}_q$. Sean Γ_L y $\tilde{\Gamma}_L$ la curva discriminante de la proyección por L y su cubrimiento doble, así como definidas en la Sección 4.1). Luego para todo $r \geq 1$ se cumple lo siguiente*

$$N_r(X) = q^{3r} + q^{2r} + q^r + 1 + q^r(N_r(\tilde{\Gamma}_L) - N_r(\Gamma_L)).$$

Debido a la Proposición 4.2.1 se introduce la cantidad

$$M_r(X) := N_r(\tilde{\Gamma}_L) - N_r(\Gamma_L). \tag{4.2.1}$$

Observamos que para cada punto racional $p \in \Gamma_L$ el valor de $M_r(X)$ sube de 1 si $\tilde{\Gamma}_L$ tiene dos puntos racionales sobre p, viceversa baja de 1 si $\tilde{\Gamma}_L$ no tiene puntos racionales sobre p y finalmente $M_r(X)$ se maniene constante si p es un punto singular de Γ_L.

Recordamos la definición de la matriz A dada en (4.1.2). Para cada $p = [x_1 : x_2 : x_3] \in \mathbb{P}^2$ denotamos por $A(p)$ la evaluación de A en p, definida a menos de multiplicar por un escalar no nulo. Denotamos por $\delta_i(p)$ el determinante de la submatriz 2×2 de $A(p)$, obtenida eliminando la i-esima fila y la i-esima columna. Observamos que $\delta_i(p)$ está definido a menos de multiplicación por un elemento de $(\mathbb{F}_q^*)^2$. Por lo tanto la condición a evaluar en el siguiente algoritmo, que nos permite calcular $M_r(X)$, está bien definida.

Input : (X, L, r)
Output: M_r
Computar la matriz A, los tres menores $\delta_1, \delta_2, \delta_3$ y la curva Γ_L ;
$M_r := 0$;
while $p \in \{p : p \in \Gamma_L(\mathbb{F}_{q^r}) \mid \Gamma_L \text{ es suave en } p\}$ **do**
  if $-\delta_1(p) \in (\mathbb{F}_{q^r}^*)^2$ o $(\delta_1(p) = 0$ y $(-\delta_2(p) \in (\mathbb{F}_{q^r}^*)^2$ o $-\delta_3(p) \in (\mathbb{F}_{q^r}^*)^2))$
  then
    $M_r := M_r + 1$;
  else
    $M_r := M_r - 1$;
  end
end
return M_r

Algoritmo 1: Computando M_r

Este algoritmo está implementado en un programa Magma llamado **Mr** que está descrito en el apéndice. A partir de este programa, se construyó el programa Magma **Nr** que permite calcular $N_r(X)$ descrito en la proposición anterior. Considerando estos dos programas, se analiza el siguiente ejemplo.

Ejemplo 4.2.2. Con Magma, buscamos una hipersuperficie cúbica suave X de dimensión tres definida sobre $\mathbb{F}_5$, definida por un polinomio f, que contenga a la recta $L = \{[x_1 : x_2 : x_3 : x_4 : x_5] \in \mathbb{P}^4_{\mathbb{F}_5} : x_1 = x_2 = x_3 = 0\}$.

```
P<[x]> := ProjectiveSpace(GF(5),4);
L := Scheme(P,x[1..3]);
S := LinearSystem(P,3);
repeat
 f := Random(LinearSystem(S,L));
 X := Scheme(P,f);
until not IsSingular(X);
```

De donde se obtiene el X pedido definido por el siguiente polinomio f

```
f;
4*x[1]^3 + 3*x[1]*x[2]^2 + 4*x[1]^2*x[3] + x[1]*x[2]*x[3]
+ 2*x[2]^2*x[3] + x[1]*x[3]^2 + 2*x[2]*x[3]^2 + 4*x[3]^3
+ x[1]^2*x[4] + x[1]*x[2]*x[4] + 3*x[2]^2*x[4] + 3*x[1]*x[3]*x[4]
+ 3*x[2]*x[3]*x[4] + 2*x[3]^2*x[4] + 2*x[1]*x[4]^2 + 3*x[2]*x[4]^2
+ 2*x[3]*x[4]^2 + x[1]^2*x[5] + x[2]*x[3]*x[5] + 2*x[3]^2*x[5]
+ 2*x[1]*x[4]*x[5] + 3*x[3]*x[4]*x[5] + 4*x[2]*x[5]^2 + 2*x[3]*x[5]^2
```

Con el programa **Nr**, determinamos $N_1(X), N_2(X), \ldots, N_5(X)$.

```
[Nr(f,r) : r in [1..5]];
[ 161, 16201, 1966751, 244607501, 30527553126]
```

En particular, se puede observar que el tiempo que demora Magma en calcular $N_3(X)$ mediante **Mr** es mas rápido que si se calcula $N_3(X)$ de manera directa.

```
time Nr(f,3);
1966751
Time: 0.010

time #Points(BaseChange(Scheme(P,f),3));
1966751
Time: 29.140
```

Para probar el algortimo empezamos con introducir la construcción de la explosión de una hipersuperficie a lo largo de una recta.

Definición 4.2.3. Sea L una recta contenida en una hipersuperficie cúbica $X \subset \mathbb{P}^4$ de dimensión tres, cuya ecuación a menos de cambios de coordenadas, es $x_1 = x_2 = x_3 = 0$. Sea ϕ_L el morfismo definido en (4.1.1), considerando la definición 2.3.2, la ***explosión*** de X a lo largo de la recta L es

$$\tilde{X} = \overline{\{(p,q) \in X \setminus L \times \mathbb{P}^2 : \phi_L(p) = q\}} \in X \times \mathbb{P}^2$$

Las proyecciones del producto cartesiano sobre los dos factores inducen dos morfismos $\pi\colon \tilde{X} \to X$ y $\tilde{\phi}_L\colon \tilde{X} \to \mathbb{P}^2$. El morfismo π es el ***morfismo de la explosión*** de X a lo largo de L. Se puede probar que, como lo mostrado en el Ejemplo 2.3.3, el divisor excepcional $E := \pi^{-1}(L)$ es isomorfo con $\mathbb{P}^1 \times \mathbb{P}^1$ y que π induce un isomorfismo de variedades algebraicas proyectivas $\tilde{X} \setminus E \to X \setminus L$.

Demostración de la Proposición 4.2.1. De la definición anterior se obtiene el siguiente diagrama conmutativo de morfismos de variedades algebraicas

$$\begin{array}{ccccc} \tilde{X} \setminus E & \longrightarrow & \tilde{X} & & \\ \downarrow \simeq & & \downarrow \pi & \searrow^{\tilde{\phi}_L} & \\ X \setminus L & \longrightarrow & X & \overset{\phi_L}{\dashrightarrow} & \mathbb{P}^2 \end{array}$$

donde $E \simeq \mathbb{P}^1 \times \mathbb{P}^1$ es el divisor excepcional del morfismo de explosión π, con abuso de notación hemos identificado la función ϕ_L dada en (4.1.1) con la proyección por la recta

L, y el morfismo $\tilde{\phi}_L$ es una fibración en conicas. Lo cual obtenemos que Γ_L también es la curva discriminante de $\tilde{\phi}_L$. Sea $p \in \mathbb{P}^2(\mathbb{F}_q)$ que le corresponde a un plano $H_p \supset L$ definido en $\mathbb{F}_q$, la fibra $\tilde{C}_p := \tilde{\phi}_L^{-1}(p)$ es la transformada estricta de la cónica $C_p \subseteq X$ tal que $X \cap H_p = L + C_p$. Se tienen 4 casos:

1. C_p es geométricamente irreducible, es decir, $p \notin \Gamma_L(\mathbb{F}_q)$, en este caso, por el Teorema 2.4.2, la fibra $\tilde{C}_p(\mathbb{F}_q)$ consiste de $q+1$ puntos.

2. C_p es unión de dos diferentes rectas definidas en $\mathbb{F}_q$, es decir, p es un punto suave en Γ_L y los dos puntos de $\varrho^{-1}(x)$ están en $\tilde{\Gamma}_L(\mathbb{F}_q)$, en este caso $\tilde{C}_p(\mathbb{F}_q)$ consiste de $2q+1$ puntos.

3. C_p es la unión de dos diferentes $\mathbb{F}_{q^2}-$rectas conjugadas, es decir, p es un punto suave en Γ_L y los dos puntos de $\varrho^{-1}(p)$ no están en $\tilde{\Gamma}_L(\mathbb{F}_q)$, en este caso $\tilde{C}_p(\mathbb{F}_q)$ consiste de 1 punto.

4. C_p es una recta doble definida en $\mathbb{F}_q$, es decir, p es un punto singular en Γ_L, en este caso $\tilde{C}_p(\mathbb{F}_q)$ consiste de $q+1$ puntos.

De los últimos tres casos, se tiene que el número total de puntos de $\tilde{\Gamma}_L(\mathbb{F}_q)$ situado sobre una cónica reducible o no reducida C_p es $qN_1(\tilde{\Gamma}_L) + N_1(\Gamma_L)$. Del diagrama conmutativo se tiene que $N_1(\tilde{X})$ es la suma de los puntos que pertenecen a la transformada estricta de las cónicas. Luego

$$N_1(\tilde{X}) = (q+1)(N_1(\mathbb{P}^2) - N_1(\Gamma_L)) + qN_1(\tilde{\Gamma}_L) + N_1(\Gamma_L).$$

Además, del diagrama se obtiene que $\tilde{X} \setminus E \simeq X \setminus L$, en efecto,

$$N_1(\tilde{X} \setminus E) = N_1(X \setminus L).$$

Observamos que si Y es una variedad definida sobre un campo finito $\mathbb{F}_q$ y S es una subvariedad de Y definida sobre el mismo campo, luego $N_1(Y \setminus S) = N_1(Y) - N_1(S)$. También si W es otra variedad definida sobre K se cumple $N_1(Y \times W) = N_1(Y) \cdot N_1(W)$. Por lo tanto de lo anterior, de $N_1(E) = N_1(\mathbb{P}^1 \times \mathbb{P}^1)$ y del hecho que $N_1(\mathbb{P}^1) = q+1$ se deduce la igualdad

$$N_1(\tilde{X}) = N_1(X) - (q+1) + (q+1)^2.$$

Considerando los dos resultados anteriores, se tiene que

$$N_1(X) - (q+1) + (q+1)^2 = (q+1)(N_1(\mathbb{P}^2) - N_1(\Gamma_L)) + qN_1(\tilde{\Gamma}_L) + N_1(\Gamma_L).$$

considerando que $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$, se tiene que $N_1(\mathbb{P}^2) = q^2+q+1$, luego, despejando $N_1(X)$ y que al reemplazar q con q^r se obtiene la misma conclusión, esto prueba lo pedido. □

Sea C una cónica reducible definida por la ecuación $x^T Ax = 0$, donde $A = (a_{ij})$ es una matriz simétrica de orden 3 con $\det(A) = 0$ con $u = [u_1 : u_2 : u_3]$ el punto singular de la cónica. Recordamos la siguiente definición:

$$\delta_i = \ i\text{-ésimo menor de la matriz } A,$$

esto es el determinante de la matriz formada por la matriz A sin considerar la fila y columna i-ésima de la matriz A.

Lema 4.2.4. *Si $\delta_i \neq 0$ entonces $u_i \neq 0$.*

Demostración. Se demostra por el contra reciproco. Supongamos que $u_1 = 0$, entonces $[0 : u_2 : u_3]$ es el punto singular de la cónica C. Derivando la ecuación que define C con respecto a cada variable, se tiene que

$$\begin{aligned}\frac{\partial f}{\partial x_1} &= 2a_{11}x_1 + 2a_{12}x_2 + 2a_{13}x_3,\\ \frac{\partial f}{\partial x_2} &= 2a_{12}x_1 + 2a_{22}x_2 + 2a_{23}x_3,\\ \frac{\partial f}{\partial x_3} &= 2a_{13}x_1 + 2a_{23}x_2 + 2a_{33}x_3.\end{aligned}$$

Dado que $[0 : u_2 : u_3]$ es un punto singular de C, cada derivada parcial es igual a cero en el punto. Dado esta condición, se obtiene el siguiente sistema de ecuaciones,

$$a_{12}u_2 + a_{13}u_3 = 0, \quad a_{22}u_2 + a_{23}u_3 = 0, \quad a_{23}u_2 + a_{33}u_3 = 0$$

Considerando las últimas dos ecuaciones, se obtiene lo siguiente,

$$\begin{pmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Del último resultado se deduce que $(u_2, u_3)^t \in \mathrm{Ker}(T)$, donde T es la transformación lineal asociada a la matriz 2×2 del sistema anterior. Dado que una de las dos componentes de $(u_2, u_3)^t$ no son cero, $\mathrm{Ker}(T) \neq \{0\}$, por lo tanto T no puede ser inyectiva. En efecto, T no es invertible, por lo que la determinante δ_1 de la matriz es cero. Los otros casos se prueban de manera similar. □

Lema 4.2.5. *La conica C es una recta doble si y solo si $\delta_1 = \delta_2 = \delta_3 = 0$.*

Demostración. Supongamos que C es una recta doble, luego su ecuación está definida por $(ax_1 + bx_2 + cx_3)^2 = 0$, desarrollando el cuadrado anterior se tiene la ecuación de C es $a^2{x_1}^2 + 2abx_1x_2 + 2acx_1x_3 + b^2{x_2}^2 + 2bcx_2x_3 + c^2{x_3}^2 = 0$, de lo cual se deduce que la matriz A definida en 2.2.1 es

$$A = \begin{pmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix},$$

de donde se obtiene que $\delta_1 = b^2c^2 - (bc)^2 = 0$, $\delta_2 = a^2c^2 - (ac)^2 = 0$ y $\delta_3 = a^2b^2 - (ab)^2 = 0$. Supongamos ahora que $\delta_1 = \delta_2 = \delta_3 = 0$ y que C es una unión de dos rectas. La ecuación de C es de la forma $(ax_1 + bx_2 + cx_3)(dx_1 + ex_2 + fx_3) = 0$, desarrollando la

ecuación se obtiene que $adx_1{}^2 + aex_1x_2 + afx_1x_3 + bdx_1x_2 + bex_2{}^2 + bfx_2x_3 + cdx_1x_3 + cex_2x_3 + cfx_3{}^2 = 0$, de lo cual se deduce que la matriz A definida en 2.2.1 es

$$A = \begin{pmatrix} ad & \frac{ae+bd}{2} & \frac{af+cd}{2} \\ \frac{ae+bd}{2} & be & \frac{bf+ce}{2} \\ \frac{af+cd}{2} & \frac{bf+ce}{2} & cf \end{pmatrix},$$

de donde se obtiene que $\delta_1 = bcef - \frac{(bf+ce)^2}{4} = -\frac{1}{4}(bf - ce)^2$, y dado que $\delta_1 = 0$, se tiene que $bf = ce$, de manera análoga con δ_2 y δ_3 se obtiene que $af = cd$ y $ae = bd$. Supongamos que $f \neq 0$, luego $a = cd/f$ y $b = ce/f$, por lo que $ax_1 + bx_2 + cx_2 = cdx_1 + cex_2 + cfx_3 = c(dx_1 + ex_2 + fx_3)$, lo que muestra que la ecuación de una de las rectas es proporcional a la otra, por lo tanto ambas ecuaciones representan a la misma recta, por lo que C es una recta doble. □

Demostración del Algoritmo 1. Si $\delta_1 \neq 0$, por el Lema 4.2.4 se tiene que $u_1 \neq 0$. Al aplicar la transformación lineal $\varphi_1 \colon \mathbb{P}^2 \to \mathbb{P}^2$ definida por

$$[x_1 : x_2 : x_3] \mapsto [x_1, x_2 - u_2/u_1x_1, x_3 - u_3/u_1x_1]$$

el punto u se va a $[1 : 0 : 0]$. Por lo tanto el polinomio x^TBx que define la cónica $\varphi_1(C)$ no contiene la variable x_1 porque todas las derivadas parciales se anulan en el punto. Además, si ponemos $B = (b_{ij})$, por la forma que tiene φ_1 una matriz representativa es

$$\begin{pmatrix} 1 & 0 & 0 \\ -u_2/u_1 & 1 & 0 \\ -u_3/u_1 & 0 & 1 \end{pmatrix}.$$

Como la submatriz 2×2 obtenida eliminando la primera fila y primera columna es la identidad entonces se tiene $b_{22} = a_{22}$, $b_{23} = a_{23}$, $b_{33} = a_{33}$. Se concluye que $\varphi_1(C)$ tiene ecuación $a_{22}x_2{}^2 + 2a_{23}x_2x_3 + a_{33}x_3{}^2 = 0$ y por lo tanto el valor de δ_1 no cambia por este cambio de coordenadas. Dado que $\delta_1 \neq 0$ por el Lema 4.2.5 la cónica C es unión de dos rectas distintas y por lo tanto existe $[x_1 : x_2 : x_3] \in \varphi_1(C)$, con $x_3 \neq 0$. La ecuación de $\varphi_1(C)$ queda de la siguiente forma,

$$a_{22}(x_2/x_3)^2 + 2a_{23}x_2/x_3 + a_{33} = 0,$$

donde $\Delta/4 = a_{23}^2 - a_{22}a_{33} = -\delta_1$. Luego la ecuación cuadrática tiene exactamente dos soluciones si $-\delta_1 \in (\mathbb{F}_q^*)^2$. Si $\delta_1 = 0$, y C no es una recta doble, por el Lema 4.2.5 o bien $\delta_2 \neq 0$ o bien $\delta_3 \neq 0$. De forma análoga a la que se analizó δ_1, se prueba los 2 casos restantes.

□

Apéndice

Libreria de las funciones Magma [2] que se ocuparon en este texto.

- **CandidatosQ1**: Función Magma que dado el género g de una curva y el campo finito $\mathbb{F}_q$, determina los polinomios que satisfacen las propiedades del polinomio Q_1 definido en 3.2.4.

```
CandidatosQ1 := function(g,q)
 R<x> := PolynomialRing(Rationals());
 B := CartesianProduct([[-Floor(Binomial(g,k)*(2*Sqrt(q))^k)..
      Floor(Binomial(g,k)*(2*Sqrt(q))^k)] : k in [1..g]]);
 pol := [x^g+&+[x^(g-k)*b[k] : k in [1..g]] : b in B];
 pol2 := [];
 for f in pol do
 rr := Roots(f,RealField());
  if #rr ne 0 and &+[p[2] : p in rr] eq g
  and &and[Abs(p[1]) le 2*Sqrt(q) : p in rr]
   then Append(~pol2,f);
  end if;
 end for;
 return pol2;
end function;
```

- **FuncZeta**: Función Magma que determina a partir de una curva algebraica proyectiva C, los valores N_m definidos en (3.1.1) con $m \in [1, r]$ y además de la función zeta de C.

```
FuncZeta := function(C,r)
 Q<t> := PolynomialRing(Rationals());
 L<u> := LaurentSeriesRing(Q,r + 1);
 Z<t> := ZetaFunction(C);
 cf := [Integers()!(Coefficient(Log(L!ZetaFunction(C)),m)*m) : m in [1..r]];
 return cf,Z;
end function;
```

- **Hyper**: Función Magma que determina todos los polinomios P_1, definidos en 3.2.1, de una curva hiperelíptica de género g definida sobre $\mathbb{F}_q$.

```
Hyper := function(g,q)
 Sh := CartesianPower(GF(q),g+1);
 Sf := CartesianPower(GF(q),2*g+2);
 Q<t> := PolynomialRing(Rationals());
 R<x> := PolynomialRing(GF(q));
 Lh := {&+[a[i]*x^(i-1) : i in [1..g+1]] : a in Sh};
 Lf := {&+[a[i]*x^(i-1) : i in [1..2*g+2]] : a in Sf};
 lis := {};
 for h in Lh, f in Lf do
  if IsHyperellipticCurveOfGenus(g,[f, h]) then
   C := HyperellipticCurve(f, h);
   Include(~lis, Q!Numerator(ZetaFunction(C)));
  end if;
 end for;
 return lis;
end function;
```

- **MatrixA**: Función Magma que determina la matriz A que define a la cónica C_p descrita en (4.1.2).

```
MatrixA := function(g)
 R<[x]> := Parent(g);
 v := [x[1],x[2],x[3],0,0];
 f := Evaluate(g,v);
 l1 := Derivative(g,2,x[4])/2;
 l2 := Derivative(Derivative(g,x[5]),x[4])/2;
 l3 := Derivative(g,2,x[5])/2;
 q1 := Evaluate(Derivative(g,x[4]),v)/2;
 q2 := Evaluate(Derivative(g,x[5]),v)/2;
 A := Matrix(3,3,[f,q1,q2,q1,l1,l2,q2,l2,l3]);
 return A;
end function;
```

- **Mr**: Función Magma que representa el Algoritmo de Bombieri y Swinnerton-Dyer descrito en 1.

```
Mr := function(g,r)
 A := MatrixA(g);
 de := [Minor(A,i,i) : i in [1..3]];
 mr := 0;
 K := BaseRing(Parent(g));
 P := ProjectivePlane(K);
 C := Scheme(P,Evaluate(Determinant(A),[P.i : i in [1..3]] cat [0,0]));
 Cr := BaseChange(C,r);
 pts := Points(Cr) diff SingularPoints(Cr);
  for p in pts do
   dd := [Evaluate(v,Eltseq(p) cat [0,0]) : v in de];
    if (IsSquare(-dd[1]) and dd[1] ne 0) or (dd[1] eq 0 and
((IsSquare(-dd[2]) and dd[2] ne 0) or (IsSquare(-dd[3]) and dd[3] ne 0))) then
     mr := mr + 1;
    else
     mr := mr - 1;
    end if;
  end for;
 return mr;
end function;
```

- **NoPoints**: Función Magma que intenta encontrar una curva algebraica proyectiva definida por un polinomio de grado d sobre el campo finito $\mathbb{F}_q$ que no contiene puntos racionales.

```
NoPoints := function(d,q)
 K<u> := GF(q);
 P<[x]> := ProjectivePlane(K);
 L := LinearSystem(P,d);
 repeat
  f := Random(L);
  C := Scheme(P,f);
  n := #Points(C);
 until n eq 0 and IsIrreducible(C);
 return f;
end function;
```

- **Nr**: Función Magma que calcula el valor de $N_r(X)$ descrito en la Proposición 4.2.1 dado un entero $r > 0$ y un polinomio g que define a la hipersuperficie cúbica X.

```
Nr := function(g,r)
 K := BaseRing(Parent(g));
 q := #Set(K);
 return &+[q^(i*r) : i in [0..3]] + q^r*Mr(g,r);
end function;
```

- **PolQ1**: Función Magma que convierte un polinomio P_1, el numerador de una función zeta de una curva algebraica proyectiva, en un polinomio Q_1 definido en 3.2.4.

```
PolQ1 := function(f,q)
 R := Parent(f);
 t := R.1;
 g := 0;
 f := f/t^Quotrem(Degree(f),2);
 repeat
  d := Quotrem(Degree(Numerator(f)),2);
  h := (q*t+1/t)^d;
  c := LeadingCoefficient(Numerator(f))/LeadingCoefficient(Numerator(h));
  g := g + c*t^d;
  f := f - c*h;
 until f eq 0;
 return g;
end function;
```

Referencias

[1] E. Bombieri and H. P. F. Swinnerton-Dyer, *On the local zeta function of a cubic threefold*, Ann. Scuola Norm. Sup. Pisa (3) **21** (1967), 1–29. ↑29

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑16, 36

[3] David A. Cox, *Galois theory*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2012. ↑7, 8, 9, 10, 17

[4] Olivier Debarre, Antonio Laface, and Xavier Roulleau, *Lines on cubic hypersurfaces over finite fields*, Geometry over nonclosed fields, Simons Symp., Springer, Cham, 2017, pp. 19–51. ↑19, 28, 30

[5] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307 (French). MR0340258 ↑4, 19

[6] European Mathematical Society Springer Verlag GmbH, *Weil cohomology*, Encyclopedia of Mathematics. http://www.encyclopediaofmath.org/index.php?title=Weil_cohomology&oldid=24012. ↑4

[7] Eberhard Freitag and Reinhardt Kiehl, *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 13, Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse; With an historical introduction by J. A. Dieudonné. ↑20

[8] Andreas Gathmann, *Algebraic Geometry, Class Notes TU Kaiserslautern 2014*, available at http://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2014/alggeom-2014.pdf. ↑15, 21

[9] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, Vol. 9 (1995), Exp. No. 279, 41–55 (French). ↑4

[10] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. ↑12, 16, 23

[11] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. ↑19

[12] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves, *An invitation to algebraic geometry*, Universitext, Springer-Verlag, New York, 2000. ↑14

[13] E. B. Vinberg, *A course in algebra*, Graduate Studies in Mathematics, vol. 56, American Mathematical Society, Providence, RI, 2003. Translated from the 2001 Russian original by Alexander Retakh. ↑18, 24