Las conjeturas de Weil, cohomología étale y conjeturas de Tate

José Cuevas Barrientos

Resumen. En este artículo expositivo presentamos las conjeturas de Weil para curvas en lenguaje esquemático, motivando tópicos geométricos más avanzados como la cohomología étale y la(s) conjetura(s) de Tate.

Índice

1. Motivación para las conjeturas de Weil

En teoría de números, un objeto que resulta extremadamente útil son las funciones L en sus distintas formas (de Dedekind, de Dirichlet, de Artin, etc.). Ejemplos de sus repercusiones aritméticas incluyen el teorema de Dirichlet sobre primos en progresión aritmética, el teorema de los números

Fecha: 20 de noviembre de 2023.

primos y el teorema de densidad de Chebotarev. La función L por excelencia es la función dseta de Riemann que se define como la extensión analítica de

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots, \qquad \operatorname{Re} s > 1,$$

la cual puede reescribirse, mediante el producto de Euler, como

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}, \qquad \operatorname{Re} s > 1.$$

Donde p recorre los números primos de $\mathbb{Z}$. En álgebra uno aprende la definición de «elemento primo» en un anillo A arbitrario,[1] no obstante, el álgebra conmutativa hace la observación de que en lugar de trabajar con elementos primos, es mejor trabajar con ideales primos y, en este caso, uno podría escribir:

$$\zeta(s) = \prod_{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z} \setminus \{(0)\}} \frac{1}{1 - |\mathbb{Z}/\mathfrak{p}|^{-s}}.$$

Esta expresión revela que la definición clásica de Euler admite una extensión natural en contexto de anillos, donde, por comodidad, eliminaremos al (0) restringiéndonos a los ideales maximales:

$$\zeta(A, s) := \prod_{\mathfrak{m} \in \operatorname{mSpec} A} \frac{1}{1 - |A/\mathfrak{m}|^{-s}}.$$

La convergencia de este producto formal y otras propiedades depende claramente de la elección del anillo, pero hay casos bastante interesantes que se siguen. Por ejemplo, si elegimos un cuerpo numérico K (i.e., una extensión finita de $\mathbb{Q}$) y tomamos $A := \mathcal{O}_K$ su anillo de enteros (el cual es la clausura entera de $\mathbb{Z}$ en K), entonces la función $\zeta(\mathcal{O}_K, s) = \zeta_K(s)$ es la función dseta de Dedekind y goza de ciertas propiedades de la función dseta de Riemann (admite continuación analítica a todo $\mathbb{C}$ con un polo simple en $s = 1$, y hasta posee una ecuación funcional). No obstante, el análogo de la hipótesis de Riemann es un problema tan o más difícil en éste caso, de manera que no nos otorga «evidencia» para ella.

Si en característica 0, los anillos de la forma $\zeta(A, s)$ son «difíciles de estudiar», quizá tengamos mejor suerte en característica prima. El anillo más simple posible es $A = \mathbb{F}_p$, pero aquí $\zeta(\mathbb{F}_p, s) = 1/(1 - p^{-s})$, y esta función no nos da mucha información aritmética. El problema es claro, $\mathbb{F}_p$ siendo un cuerpo solo posee un primo, mientras que $\mathbb{Z}$ posee una variedad de primos. Por otro lado, geométricamente $\operatorname{Spec} \mathbb{F}_p$ es un punto, mientras que $\operatorname{Spec} \mathbb{Z}$ es una curva (absoluta), así que quizá la pregunta apropiada sería para *curvas de característica prima*.

[1] En éste texto, todos los anillos se asumen unitarios y conmutativos, a menos que se señale lo contrario.

Una razón para esto también se puede encontrar en el siguiente paralelo: las funciones dseta $\zeta(A, s)$ contienen información aritmética cuando $\operatorname{Frac} A$ era $\mathbb{Q}$ o un cuerpo numérico K, ambos ejemplos de *cuerpos globales*, por lo que sus similes en característica prima serían anillos como $\mathbb{F}_p[t]$ (de dimensión de Krull 1), ya que $\mathbb{F}_p(t)$ es un cuerpo global.

Así, la cuestión de si $\zeta(\operatorname{Spec}(\mathbb{F}_p[t]), s)$ posee las mismas propiedades que $\zeta(\operatorname{Spec}\mathbb{Z}, s)$ son parte de lo que se conocen como *conjeturas de Weil*. Pero antes de embancarnos de lleno, hagamos la última generalización:

Definición 1.1: Sea X un esquema. Denotamos por X^0 el conjunto de puntos cerrados de X. Para un punto $x \in X$ definimos su ***cuerpo de restos*** como

$$\Bbbk(x) := \mathscr{O}_{X,x}/\mathfrak{m}_{X,x},$$

(donde $\mathfrak{m}_{X,x}$ es el primo maximal del anillo local $\mathscr{O}_{X,x}$).

Definimos su ***función dseta de Hasse-Weil*** como

$$\zeta(X, s) := \prod_{x \in X^0} \frac{1}{1 - |\Bbbk(x)|^{-s}}.$$

Ahora sí, tenemos una definición lo suficientemente potente como para capturar todos los casos anteriores. No obstante, por lo general de esta definición, vamos a querer hacer reducciones a los esquemas a considerar. En particular, queremos que X sea un ***esquema algebraico*** sobre un cuerpo k base, es decir, que su morfismo estructural sea de tipo finito; aquí hay algo que tener en mente:

Proposición 1.2: Sea X un esquema algebraico sobre un cuerpo k. Un punto $x \in X$ es cerrado syss $\Bbbk(x)$ es una extensión finita de k. En particular, si k es algebraicamente cerrado, entonces $x \in X$ es cerrado syss $\Bbbk(x) = k$, es decir, si x es un punto k-racional.[2]

Demostración: Cfr. Liu [**5,** pág. 76], ex. 2.5.9. □

Definición 1.3: Sea X un esquema algebraico sobre un cuerpo k. Para un punto cerrado $x \in X^0$ se define $\deg x := [\Bbbk(x) : k]$.

Los esquemas permiten «buena geometría algebraica» sobre cuerpos que no son algebraicamente cerrados porque, entre otras cosas, los puntos cerrados de una variedad X son «órbitas de Galois» en lugar de meros puntos k-racionales. Esto es una hoja de doble filo, porque ahora los puntos cerrados poseen un «cuerpo de definición» que puede ser más grande.

[2]Dado un S-esquema X y otro S-esquema T, los *puntos T-valuados* de X, denotado $X(T)$, son los S-morfismos $T \to X$. Cuando $T = S$ hablamos de puntos *S-racionales* para ser enfáticos.

Ejemplo: Sea K un cuerpo numérico y sea $X := \operatorname{Spec}(\mathcal{O}_K)$. Si bien X es una curva absoluta, no es un esquema algebraico sobre ningún cuerpo, pero si tomamos un punto cerrado $x \in X^0$ correspondiente al primo $\mathfrak{p}$, y si p es el primo racional tal que $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}$, entonces el esquema local $\operatorname{Spec}(\mathscr{O}_{X,x})$ es un $\mathbb{F}_p$-esquema (aunque no es algebraico) y

$$\deg_{\mathbb{F}_p} x = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p] = f(\mathfrak{p}/\mathbb{Z})$$

es decir, es el grado de inercia.

El siguiente cambio de variables será útil:

Definición 1.4: Sea X un esquema algebraico sobre $\mathbb{F}_q$, se define:

$$Z(X,t) := Z(X, q^{-s}) = \zeta(X,s) = \prod_{x \in X^0} \frac{1}{1 - t^{\deg x}}.$$

2. Las conjeturas de Weil sobre curvas

Un cuento en cinco movimientos.

§2.1 *Preludio:* Racionalidad y ecuación funcional.

Proposición 2.1: Sea k una $\mathbb{Z}$-álgebra de tipo finito que también es un cuerpo, entonces k es finito.

Éste resultado admite dos posibles demostraciones. Primero una demostración algebraica:

Demostración: Es claro que $\mathbb{Z}$ es un anillo de Jacobson (cfr. Matsumura **[29,** pág. 34]) denotando $\varphi\colon \mathbb{Z} \to k$ el homomorfismo canónico, por el teorema de ceros de Hilbert general (cfr. **[29],** thm. 5.5) tenemos que $\varphi^{-1}[(0)]$ es maximal en $\mathbb{Z}$, luego es de la forma $p\mathbb{Z}$ para algún primo p y, por tanto, $\operatorname{car} k = p$. Ahora aplicamos el lema de Zariski usual (**[29],** thm. 5.6) para notar que $k/\mathbb{F}_p$ debe ser extensión finita y, así, k debe ser finito. □

Y una demostración geométrica:

Demostración: Si k tiene característica $p > 0$, entonces aplicamos el lema de Zariski para notar que $k/\mathbb{F}_p$ ha de ser una extensión finita y estamos listos. Si no, entonces el homomorfismo canónico $\mathbb{Z} \hookrightarrow k$ es inyectivo, luego k es un $\mathbb{Z}$-módulo plano, y así el morfismo $f\colon \operatorname{Spec} k \to \operatorname{Spec} \mathbb{Z}$ es plano. Claramente, $\operatorname{Spec} \mathbb{Z}, \operatorname{Spec} k$ son esquemas noetherianos y el morfismo f es de tipo finito, luego f es abierto (cfr. Liu **[5,** pág. 145], ex. 4.3.9); pero ningún punto es abierto en $\operatorname{Spec} \mathbb{Z}$. □

Lema 2.2: Sea X un esquema algebraico sobre $\mathbb{F}_q$. Entonces $|X(\mathbb{F}_{q^n})| = O(q^{n \dim X})$ y, por ende, para todo $N \in \mathbb{N}$ hay solo finitos $x \in X$ tales que $\deg x \leq N$.

Demostración: Podemos suponer que X es una variedad. Por el teorema de normalización de Noether, existe un morfismo finito $f\colon U \to \mathbb{A}^{\dim X}_{\mathbb{F}_q}$ para algún abierto $U \subseteq X$ denso, y claramente

$$|U(\mathbb{F}_{q^n})| \leq (\deg f) \cdot q^{n \dim X},$$

podemos concluir aplicando inducción sobre $\dim X$. □

Proposición 2.3: Sea X un esquema algebraico sobre $\mathbb{F}_q$, entonces

$$t \cdot \frac{\mathrm{d}}{\mathrm{d}t} \log Z(X,t) = \sum_{n=1}^{\infty} |X(\mathbb{F}_{q^n})| \cdot t^n \in \mathbb{Q}[[t]].$$

Demostración: Basta hacer el cálculo:

$$\begin{aligned} t \cdot \frac{\mathrm{d}}{\mathrm{d}t} \log Z(X,t) &= t \cdot \sum_{x \in X^0} \frac{\mathrm{d}}{\mathrm{d}t} \log\left((1 - t^{\deg x})^{-1}\right) = \sum_{x \in X^0} (\deg x) \cdot \frac{t^{\deg x}}{1 - t^{\deg x}} \\ &= \sum_{x \in X^0} (\deg x) \cdot \sum_{j \geq 1} t^{j \cdot \deg x} = \sum_{x \in X^0} \sum_{\deg x \mid n} (\deg x) t^n, \end{aligned}$$

finalmente, los puntos $\mathbb{F}_{q^n}$-valuados de X son precisamente los pares (x, σ) donde x es un punto cerrado de $\deg x \mid n$ y por un monomorfismo $\sigma\colon \Bbbk(x) \to \mathbb{F}_{q^n}$, luego es cada punto x de grado $\deg x \mid n$ contado $\deg x$ veces; así concluimos el enunciado. □

Proposición 2.4: Sea $X/\mathbb{F}_q$ un esquema algebraico. El producto formal de $\zeta(X,s)$ converge uniforme y absolutamente sobre compactos de $U := \{s \in \mathbb{C} : \operatorname{Re} s > \dim X\}$. Por tanto, determina una función analítica.

Demostración: Sin perdida de generalidad, supongamos que X es reducido. Si $X = X_1 \cup X_2$, donde X_1, X_2 son cerrados irreducibles, entonces se puede comprobar que

$$\zeta(X,s) = \frac{\zeta(X_1,s) \cdot \zeta(X_2,s)}{\zeta(X_1 \cap X_2, s)},$$

así que podemos suponer que X es variedad.

Para demostrar la convergencia de $\zeta(X,s)$ con $\operatorname{Re} s > \dim X$, basta probar la convergencia de la serie de potencias de $t \cdot \frac{\mathrm{d}}{\mathrm{d}t} \log Z(X,t)$ con $0 < t < q^{-\dim X}$, lo cual se deduce de que

$$t \cdot \frac{\mathrm{d}}{\mathrm{d}t} \log Z(X,t) = \sum_{n \geq 1} |X(\mathbb{F}_{q^n})| t^n \leq M \cdot \sum_{n \geq 1} q^{n \dim X} t^n$$

$$= M \cdot \sum_{n \geq 1} (q^{\dim X} t)^n. \qquad \square$$

Finalmente, requerimos el último lema:

Lema 2.5: Sea X una curva geométricamente íntegra, proyectiva y suave sobre un cuerpo finito k. Entonces $\mathrm{Pic}^0(X)$ es finito.

Haremos dos demostraciones. Una demostración más elemental:

Demostración: Sea D un divisor de grado $\deg D > 2g - 2$. Entonces por Riemann-Roch, vemos que $h^0(D) = \deg D + 1 - g > 0$, por lo que sea $f \in \Gamma(X, \mathscr{O}_X(D))$ no nulo. Por la proposición 2.9 (ver más adelante), se sigue que $D \sim D + \deg f \geq 0$ y $D + \deg f$ es efectivo, así que, hay una clase lateral de $\mathrm{Pic}^0(X)$ visto como subgrupo de $\mathrm{Pic}\, X$ cuyos representantes son divisores efectivos.

Así nos reducimos a contar divisores efectivos de grado fijo n, pero hay finitos puntos cerrados de grado $\leq n$ (lema 2.2) y por tanto hay finitas sumas formales con ellos. $\square$

Y una más geométrica:

Demostración: Recuérdese que, asociado a X, existe la variedad jacobiana J sobre k (cfr. Milne **[6],** thm. 1.1) tal que para toda extensión K/k de cuerpos que satisfaga $X(K) \neq \varnothing$ se cumple que $J(K)$ está en biyección canónica con el grupo $\mathrm{Pic}^0(X_K)$. Más aún, esta variedad es abeliana, aunque no utilizaremos éste hecho. Así, para una extensión finita suficientemente grande K/k tenemos que $|\mathrm{Pic}^0(X_K)| = |J(K)|$, el cual es finito por ser los puntos de una variedad proyectiva sobre un cuerpo finito. $\square$

Teorema 2.6: Sea X una curva suave, proyectiva, geométricamente conexa sobre $\mathbb{F}_q$ de género g. Entonces:

CW1. $Z(X, t)$ es una función racional, de hecho:

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

donde $f(t) \in \mathbb{Q}[t]$ tiene $\deg f \leq 2g$ y coeficiente libre 1.

CW2. **Ecuación funcional:**

- $Z(X, q^{-1}t^{-1}) = q^{1-g}t^{2-2g}Z(X, t)$.
- $f(t)$ en (1) tiene $\deg f = 2g$.
- $f(t) = \prod_{i=1}^{2g}(1 - \omega_i t) \in \mathbb{C}[t]$, donde $\omega_i \cdot \omega_{2g+1-i} = q$ para cada i.

Como X es suave, entonces los divisores de Weil y de Cartier están en correspondencia canónica (en particular, $\mathrm{Pic}\, X \cong \mathrm{Cl}\, X$), así que nos daremos la libertad de hablar de «divisores de Weil» cuando ciertos pasos estén mejor justificados en términos de haces inversibles.

Demostración: Calculemos:

$$Z(X,t) = \prod_{x\in X^0} \frac{1}{1-t^{\deg x}} = \prod_{x\in X^0}\sum_{j=0}^{\infty} t^{j\deg x} = \sum t^{\sum j_i \deg x_i},$$

donde nótese que $\sum_{i=1}^n j_i \deg x_i = \deg\left(\sum_{i=1}^n j_i \cdot x_i\right)$ el cual es un divisor efectivo de Weil. Así, vemos que

$$Z(X,t) = \sum_{\substack{D\in \operatorname{Div} X\\ D\geq 0}} t^{\deg D}.$$

Fijemos un $D \in \operatorname{Div} X$, entonces los divisores efectivos linealmente equivalentes a D conforman el sistema lineal completo $|D|$, el cual está en biyección con los conjuntos:

$$\frac{\Gamma(X, \mathscr{O}_X(D)) \setminus \{0\}}{\mathbb{F}_q^\times} = \mathbb{P}(D),$$

de modo que

$$Z(X,t) = \sum_{\substack{D\in \operatorname{Pic} X\\ D\geq 0}} \frac{q^{h_0(D)}-1}{q-1}\cdot t^{\deg D},$$

por el teorema de Riemann-Roch (cfr. Liu [**5,** pág. 281], thm. 7.3.26)[3] podemos ver que

$$Z(X,t) = \underbrace{\sum_{0\leq \deg D\leq 2g-2} \frac{q^{h_0(D)}-1}{q-1}\cdot t^{\deg D}}_{g_1(t)} + \underbrace{\sum_{2g-2<\deg D} \frac{q^{\deg D+1-g}-1}{q-1}\cdot t^{\deg D}}_{g_2(t)}.$$

Claramente $g_1(t)$ ya es racional así que enfoquémonos en $g_2(t)$. El grupo $\operatorname{Pic}^0 X$ es finito y luego podemos expresarlo como:

$$\begin{aligned} g_2(t) &= |\operatorname{Pic}^0 X| \sum_{n=2g-1}^{\infty} \frac{q^{n-1+g}-1}{q-1}\cdot t^n \\ &= \frac{|\operatorname{Pic}^0 X|}{q-1}\left(\frac{q^{g-1}(qt)^{2g-1}}{1-qt} - \frac{t^{2g-1}}{1-t}\right) = \frac{h(t)}{(1-t)(1-qt)}. \end{aligned}$$

Finalmente, vemos que $g_1(t)$ tiene grado $\leq 2g-1$ y es claro que $h(t)$ tiene grado $\leq 2g$. Evaluando podemos corroborar la afirmación del coeficiente libre y así probamos el inciso 1.

Volvamos ahora a $g_1(t)$ y a cada haz invertible D asociémosle $K_X - D$ (donde K_X es el divisor asociado a un haz canónico), la cual es una biyección y, por Riemann-Roch, tendremos

$$\frac{q^{h^0(K_X-D)}-1}{q-1}\cdot t^{\deg(K_X-D)} = \frac{q^{h^0(D)-\deg D-1+g}-1}{q-1}\cdot t^{2g-2-\deg D}$$

[3]Nótese que, al contrario de las pruebas usuales de Riemann-Roch, en éste caso necesitamos la generalidad adicional que el cuerpo base no sea algebraicamente cerrado.

$$= \frac{q^{h^0(D)} - q^{\deg D+1-g}}{q-1} \cdot q^{-(\deg D+1-g)} t^{2g-2-\deg D}$$
$$= q^{g-1}t^{2g-2} \cdot \frac{q^{h^0(D)} - q^{\deg D+1-g}}{q-1} \cdot (q^{-1}t^{-1})^{\deg D}, \tag{2}$$

donde recordamos que

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

Así, podemos ver que $Z(X,t)$ se descompone como

$$Z(X,t) = \sum_{0\leq \deg D\leq g-1} \frac{q^{h^0(D)} - 1}{q-1} \cdot t^{\deg D}$$
$$+ \sum_{g\leq \deg D\leq 2g-2} \frac{q^{h^0(D)} - q^{\deg D+1-g}}{q-1} \cdot t^{\deg D} + \sum_{g\leq \deg D} \frac{q^{\deg D+1-g} - 1}{q-1} \cdot t^{\deg D}.$$

Por el cálculo (2) vemos que la primera línea satisface la ecuación funcional, mientras que la segunda línea:

$$\sum_{g\leq \deg D} \frac{q^{\deg D+1-g} - 1}{q-1} \cdot t^{\deg D} = |\operatorname{Pic}^0 X| \sum_{n=g}^{\infty} \frac{q^{n+1-g} - 1}{q-1} t^n$$
$$= \frac{|\operatorname{Pic}^0 X| t^g}{q-1} \left(\frac{q}{1-qt} - \frac{1}{1-t} \right)$$
$$= |\operatorname{Pic}^0 X| \cdot \frac{t^g}{(1-qt)(1-t)}.$$

Y es fácil verificar que satisface la ecuación funcional.

Finalmente, basta aplicar la ecuación funcional sobre (1):

$$\frac{f(q^{-1}t^{-1})}{(1-q^{-1}t^{-1})(1-t^{-1})} = \frac{t^{2-2g}q^{1-g}f(t)}{(1-t)(1-qt)},$$

lo que nos da que $f(t) = t^{2g}q^g f(q^{-1}t^{-1})$, por lo que, necesariamente, $\deg f = 2g$. Llamando ω_i's a las raíces de $f(t)$, vemos que la expresión del lado derecho tiene raíces $\left\{\frac{1}{q\omega_1}, \ldots, \frac{1}{q\omega_{2g}}\right\}$, es decir, que existe una permutación $\sigma \in S_{2g}$ tal que $\omega_i \cdot \omega_{\sigma(i)} = q$. □

§2.2 ***Moderato:*** **La prueba de Bombieri.** Finalmente queda la última de las conjeturas de Weil. Hay dos demostraciones que haremos, una aquí empleando únicamente el teorema de Riemann-Roch que sigue el artículo de Bombieri **[17],** basado en un argumento de Stepanov **[21]** (1969). Una exposición de la demostración se encuentra en el apéndice de Rosen **[30].**

Lema 2.7: Sean $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ tales que $\left|\sum_{i=1}^{m} \lambda_i^n\right|$ está acotado (como función de n), entonces cada $|\lambda_i| \leq 1$.

Demostración: De haber $\lambda_i = 0$ los borramos de la lista. Nótese que podemos encontrar algún N suficientemente grande tal que $\operatorname{Re}(\lambda_i^N) > 0$ y $|\operatorname{Im}(\lambda_i^N)| < \frac{1}{2}\operatorname{Re}(\lambda_i^N)$. Esto se logra escribiendo $\lambda_i = r_i e^{\mathrm{i}\alpha_i}$ con $r_i \in \mathbb{R}_{>0}$, y traduciendo la condición en que $N\alpha_i$ caiga en un intervalo conveniente de la forma:

$$\exists j \in \mathbb{Z} \quad N\alpha_i \in (2\pi j - \arctan(1/2), 2\pi j + \arctan(1/2)),$$

y luego concluir por principio del palomar. Por inducción sobre m la cantidad de sumandos, obtenemos que para dicho N se tiene que

$$\sum_{i=1}^{m} |\lambda_i|^N \leq \sqrt{2}^m \left| \sum_{i=1}^{m} \lambda_i^N \right|.$$

Por palomar de hecho encontramos infinitos N's que cumplen la condición, así que aplicando límites obtenemos el enunciado. □

Proposición 2.8: Sea X una curva suave, proyectiva, geométricamente conexa sobre $\mathbb{F}_q$. Son equivalentes:

1. **(Hipótesis de Riemann)** Los ω_i de $Z(X,t)$ tienen $|\omega_i| = q^{1/2}$.
2. $N_n := |X(\mathbb{F}_{q^n})| = q^n + O(q^{n/2})$.

Demostración: $1 \implies 2$. Por la proposición 2.3 podemos aplicar derivadas logarítmicas a

$$Z(X,t) = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)},$$

para obtener que

$$|X(\mathbb{F}_{q^n})| = 1 + q^n - \sum_{n=1}^{2g} \omega_i^n = q^n + O(q^{n/2}). \tag{3}$$

$2 \implies 1$. Recíprocamente, definiendo $\lambda_i := \omega_i q^{-1/2}$ tenemos que $|\omega_i| \leq q^{1/2}$ por (3). Por la ecuación funcional (teo. 2.6), sabemos también que

$$|\omega_i| = \frac{q}{|\omega_{2g+1-i}|} \geq q^{1/2},$$

concluimos por antisimetría. □

Nótese que si deshacemos los cambios de variables, notamos que el inciso 1 es equivalente a que los ceros de $\zeta(X,s)$ tengan $\operatorname{Re} s = 1/2$, pero como hemos visto, es más fácil trabajar con $Z(X,t)$.

Ahora recordemos la siguiente correspondencia:

Proposición 2.9: Sea X un esquema íntegro, y sea $\mathscr{L}$ un haz invertible sobre X. A cada $s \in \Gamma(X, \mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{K}_X)$ no nulo, podemos asignarle un divisor de Cartier $\operatorname{div} s \in \operatorname{CaDiv} X$ de manera análoga.[4] Entonces:

1. Para toda sección $s \in \Gamma(X, \mathscr{L})$ se tiene que $\operatorname{div} s \geq 0$.
2. Para todo divisor $D \in \operatorname{CaDiv}^+ X$ identificando $\mathscr{O}_X(D) \subseteq \mathscr{K}_X$, se satisface sobre un abierto $U \subseteq X$:

$$\Gamma(U, \mathscr{O}_X(D)) = \{f \in \Gamma(U, \mathscr{K}_X^\times) : \operatorname{div} f + D|_U \geq 0\} \cup \{0\}.$$

Demostración: Cfr. Liu [**5,** pág. 266], ex. 7.1.13. □

Ahora sí. Para los siguientes lemas fijamos un cuerpo finito $k = \mathbb{F}_q$ y una curva C proyectiva y suave sobre la clausura algebraica k^{alg}, y denotaremos por $\varphi\colon C \to C$ el endomorfismo de Frobenius. Denotaremos también por N_r la cantidad de puntos fijos por la composición φ^r. Fijamos también $x_0 \in C$ cerrado tal que $\varphi(x_0) = x_0$. Como C tiene dimensión 1, podemos ver a x_0 como divisor de C y tenemos la siguiente correspondencia

$$R_m := \Gamma(X, \mathscr{O}_X(D)) = \{f \in K(X)^\times : \operatorname{div} f \geq -m x_0\}.$$

Como aplicación del teorema de Riemann-Roch tenemos que

$$m + 1 - g \underset{(*)}{\leq} \dim_k R_m \leq m + 1, \qquad \dim_k R_{m+1} \leq \dim_k R_m + 1,$$

donde $(*)$ alcanza igualdad cuando $m > 2g - 2$.

Ahora aplicamos el homomorfismo φ^* y obtenemos que $\varphi^*[R_m] \subseteq R_{mq}$, y nótese que cada elemento $\varphi^* f$ (con $f \in R_m$) es una potencia q-ésima, y de hecho, considerando a los elementos de R_m como funciones racionales, tenemos la relación

$$\operatorname{div}(f \circ \varphi) = q\varphi_*(\operatorname{div} f).$$

Sean U, V un par de k-subespacios vectoriales de R_m, R_n resp., y denotemos $U \cdot V$ el subespacio de R_{m+n} generado por los elementos fg donde $f \in U, g \in V$. Denotemos $R_\ell^{(p^\mu)}$ como el subespacio de $R_{\ell p^\mu}$ cuyos elementos son funciones f^{p^μ} con $f \in R_\ell$. Entonces

$$\dim_k(R_\ell^{(p^\mu)}) = \dim_k(R_\ell), \qquad \dim_k(\varphi^* R_m) = \dim_k(R_m).$$

Así tenemos lo siguiente:

Lema 2.10: Si $\ell p^\mu < q$, entonces el homomorfismo canónico

$$R_\ell^{(p^\mu)} \otimes_{k^{\mathrm{alg}}} \varphi^*(R_m) \xrightarrow{\ \sim\ } R_\ell^{(p^\mu)} \cdot \varphi^*(R_m)$$

es un isomorfismo.

[4] Elegimos un cubrimiento $\{U_i\}_i$, tal que $\mathscr{L}|_{U_i} \simeq \mathscr{O}_{U_i}$ y, mediante dicho isomorfismo canónico, la familia $\{(U_i, f_i)\}_i$ (donde $s|_{U_i} = e_i f_i$, con e_i un generador global de $\mathscr{L}|_{U_i}$) es un divisor de Cartier.

Demostración: Sea $f \in K(X)$, recuérdese que $\mathrm{mult}_x(f)$ denota la valuación $\mathfrak{m}_{X,x}$-ádica de f en un punto cerrado x (intuitivamente, el orden de un cero de f en x), y que

$$f \in R_m \implies \mathrm{mult}_{x_0} f \geq -m.$$

De ahora en adelante, ya que x_0 está fijo, abreviaremos $\mathrm{mult} := \mathrm{mult}_{x_0}$. Sean $s_1, \ldots, s_r$ una base de R_m tal que $\mathrm{mult}(s_i) < \mathrm{mult}(s_{i+1})$ para cada $1 \leq i < r$; esto se puede pues $\dim R_{m+1} \leq \dim R_m + 1$. El enunciado equivale a ver que si

$$\sum_{i=1}^{r} \sigma_i^{p^\mu} \cdot (\varphi \circ s_i) = 0,$$

entonces cada $\sigma_i = 0$. Borrando los primeros índices donde $\sigma_i = 0$, supongamos, por contradicción, que

$$\sum_{i=\rho}^{r} \sigma_i^{p^\mu} \cdot (\varphi \circ s_i) = 0, \qquad \sigma_\rho \neq 0.$$

Entonces calculamos

$$\begin{aligned} \mathrm{mult}(\sigma_\rho^{p^\mu} \cdot (\varphi \circ s_\rho)) &= \mathrm{mult}(-\sum_{i=\rho+1}^{r} \sigma_i^{p^\mu} \cdot (\varphi \circ s_i)) \\ &\geq \mathrm{mín}\{\mathrm{mult}(\sigma_i^{p^\mu} \cdot (\varphi \circ s_i)) : i > \rho\} \\ &\geq -\ell p^\mu + q\,\mathrm{mult}(s_{\rho+1}), \end{aligned}$$

donde la primera desigualdad es la «desigualdad ultramétrica», y donde en la última línea empleamos que $\mathrm{mult}(s_i)$ es estrictamente creciente. Así

$$p^\mu \,\mathrm{mult}(\sigma_\rho) \geq -\ell p^\mu + q(\mathrm{mult}(s_{\rho+1}) - \mathrm{mult}(s_\rho)) \geq -\ell p^\mu + q > 0,$$

y, por lo tanto, σ_ρ se anula en x_0. Pero por definición, como $\sigma_\rho \in R_\ell$, entonces no posee polos fuera de x_0, y toda función racional no nula posee tantos polos (en este caso, cero) como ceros contando multiplicidad, por lo que $\sigma_\rho = 0$ como se quería probar. □

Corolario 2.11: Si $\ell p^\mu < q$, entonces:

$$\dim_k(R_\ell^{(p^\mu)} \cdot \varphi^*(R_m)) = \dim_k(R_\ell) \cdot \dim_k(R_m).$$

Proposición 2.12: Supongamos que $q = p^\alpha$ con α par, tal que $q > (g+1)^4$. Entonces tenemos que

$$N_1 < q + (2g+1)\sqrt{q} + 1.$$

Demostración: Mantenemos nuestra notación. Supongamos que $\ell p^\mu < q$, por el lema la siguiente aplicación está bien definida y determina un homomorfismo

$$\delta\colon R_\ell^{(p^\mu)} \cdot \varphi^*(R_m) \longrightarrow R_\ell^{(p^\mu)} \cdot R_m \subseteq R_{\ell p^\mu + m}$$

$$\sum_{i=1}^{r} \sigma_i^{p^\mu} \cdot (s_i \circ \varphi) \longmapsto \sum_{i=1}^{r} \sigma_i^{p^\mu} \cdot s_i.$$

Por el corolario anterior y el teorema de Riemann-Roch, obtenemos que

$$\begin{aligned} \dim_k \ker \delta &\geq (\dim R_\ell)(\dim R_m) - \dim(R_{\ell p^\mu + m}) \\ &\geq (\ell + 1 - g)(m + 1 - g) - (\ell p^\mu + m + 1 - g) \end{aligned}$$

cuando $\ell p^\mu + m > 2g - 2$, lo cual se satisface si $\ell, m \geq g$. Ahora bien, cada elemento $f \in \ker \delta$ se anula en cada punto fijo de φ con orden $\geq p^\mu$, excepto quizá en x_0 debido a que

$$f(x) = \sum_{i=1}^{r} \sigma_i^{p^\mu}(x) s_i(\varphi(x)) = \sum_{i=1}^{r} \sigma_i^{p^\mu}(x) s_i(x) = (\delta f)(x) = 0,$$

y a que cada elementos de $R_\ell^{(p^\mu)} \cdot \varphi^*(R_m)$ es una potencia p^μ-ésima. Así pues, $(\operatorname{div} f)_0$, el divisor de ceros, tiene

$$\deg(\operatorname{div} f)_0 \geq p^\mu(N_1 - 1).$$

Pero como $f \in R_\ell^{(p^\mu)} \cdot \varphi^*(R_m) \subseteq R_{\ell p^\mu + mq}$, entonces el divisor de polos $(\operatorname{div} f)_\infty$ tiene

$$\deg(\operatorname{div} f)_\infty \leq \ell p^\mu + mq.$$

En síntesis, eligiendo ℓ, m de modo que

$$\ell p^\mu < q, \qquad \ell, m \geq g, \qquad \dim \ker \delta > 0$$

se satisface que

$$N_1 \leq \ell + \frac{mq}{p^\mu} + 1.$$

Si $q = p^\alpha$ con α par y $q > (g+1)^4$ podemos elegir

$$\mu := \alpha/2, \qquad m := p^\mu + 2g, \qquad \ell := \frac{g}{g+1} p^\mu + g + 1,$$

lo que nos da la cota del enunciado. □

Teorema 2.13: La hipótesis de Riemann se satisface para curvas geométricamente irreducibles, proyectivas y suaves sobre cuerpos finitos.

Demostración: Sea X como en el enunciado sobre un cuerpo finito $k = \mathbb{F}_q$, donde podemos suponer que q es la potencia par de un primo p. Haciendo cambio de base, miramos a la extensión de cuerpos $K(\overline{X})/k^{\mathrm{alg}}$, la cual contiene un subcuerpo $k^{\mathrm{alg}}(t)$ puramente trascendente tal que $K(\overline{X})/k^{\mathrm{alg}}(t)$ es separable por el teorema de Lüroth (cfr. Jacobson [**27,** vol. 2, pág. 515]). Luego, podemos tomar la clausura normal de $K(\overline{X})$ sobre $k^{\mathrm{alg}}(t)$, lo cual por la correspondencia entre extensiones de tipo finito y trascendencia 1, y curvas proyectivas suaves (cfr. Görtz y Wedhorn [**2,** pág. 500], thm. 15.21), nos da los siguientes morfismos

$$C' \longrightarrow C \longrightarrow \mathbb{P}^1_{k^{\mathrm{alg}}}.$$

donde la extensión de cuerpos $K(C')/k^{\mathrm{alg}}(t)$ es de Galois finita con grupo de Galois G, de modo que $C' \to \mathbb{P}^1_{k^{\mathrm{alg}}}$ es un cubrimiento de Galois, y $C' \to C$ también, correspondiente a un subgrupo $H \leq G$. Podemos suponer que G actúa sobre C' fijando una extensión de k finita. Así, si $x \in \mathbb{P}^1(k)$ es no ramificado en $C' \to \mathbb{P}^1_{k^{\mathrm{alg}}}$, y si $y \in C'_x$, entonces

$$\varphi(y) = \sigma.y, \qquad \sigma \in G,$$

al cual llamaremos *sustitución de Frobenius* de y. Sean $N_1(C', \sigma)$ la cantidad de puntos de C' con sustitución de Frobenius σ. Empleando el mismo argumento de la proposición anterior, con el homomorfismo

$$\delta_\sigma \colon R_\ell^{(p^\mu)} \cdot \varphi^*(R_m) \to R_\ell^{(p^\mu)} \cdot \sigma^*(R_m),$$

obtenemos que $N_1(C', \sigma) \leq q + (2g' + 1)\sqrt{q} + 1$, donde g' es el género de C'. Por otro lado

$$\sum_{\sigma \in G} N_1(C', \sigma) = |G| N_1(\mathbb{P}^1) + O(1),$$

donde $O(1)$ representa los puntos ramificados de $C' \to \mathbb{P}^1_{k^{\mathrm{alg}}}$. Como $N_1(\mathbb{P}^1) = q + 1$, comparando las desigualdades anteriores, concluimos finalmente que

$$N_1(C', \sigma) = q + O(q^{1/2}),$$

para todo $\sigma \in G$, y empleando que

$$\sum_{\tau \in H} N_1(C', \tau) = |H| N_1(C) + O(1)$$

concluimos finalmente que $N_1(C) = q + O(q^{1/2})$. □

A corolario de la hipótesis de Riemann (cfr. demostración de prop. 2.8), tenemos lo siguiente:

Corolario 2.14 (cotas de Hasse-Weil): Sea $X/\mathbb{F}_q$ una curva suave, proyectiva y geométricamente íntegra de género g. Entonces

$$|X(\mathbb{F}_q)| = q + 1 - \epsilon,$$

con $|\epsilon| \leq 2g\sqrt{q}$.

Este es uno de los primeros resultados en un curso estándar sobre curvas elípticas (sabiendo que éstas son suaves, proyectivas, geométricamente íntegras y de género $g = 1$).

§2.3 ***Intermezzo:*** **Intersecciones.** Como preliminar vamos a hacer mención de las bases para la intersección en geometría algebraica (cfr. Kollár **[4],** §VI.2).

Teorema 2.15 (Snapper): Sea X un esquema propio (e.g., un esquema proyectivo) sobre un cuerpo k. Sean $\mathscr{L}_1, \ldots, \mathscr{L}_r$ haces invertibles sobre X y $\mathscr{F}$ un haz coherente. Existe un único polinomio, llamado ***de Hilbert-Samuel*** $P(t_1, \ldots, t_r) \in \mathbb{Q}[\boldsymbol{t}]$ tal que para toda tupla de enteros $n_1, \ldots, n_r$ se satisface que

$$P(n_1, \ldots, n_r) = \chi_k(X, \mathscr{L}_1^{n_1} \otimes \cdots \mathscr{L}_r^{n_r} \otimes \mathscr{F}).$$

Aquí $\chi_k(X, -)$ denota la característica de Euler-Poincaré de haces coherentes.

Bosquejo de demostración: Si X fuese proyectivo, tomamos un encaje cerrado hacia un espacio proyectivo y así vemos que podemos suponer que $X = \mathbb{P}_k^r$. Por el teorema de los *syzygies* de Hilbert, podemos dar una resolución libre finita para $\mathscr{F}$ y reducirnos al caso en que $\mathscr{F} \simeq \mathscr{O}_X^p(q)$ para algunos p, q. Este es un cálculo que sale de una combinatoria sencilla con dualidad de Serre.

Si X no es proyectivo, entonces empleamos una mezcla de inducción noetheriana con *dévissage*, y construimos sucesiones exactas apropiadas para emplear la hipótesis inductiva. Para probar la finitud de $\chi_k(X, -)$ hay que emplear el lema de Chow (cfr. Görtz y Wedhorn **[2,** pág. 418], thm. 13.100) para generalizar el teorema de coherencia de Grothendieck. □

Hay autores que emplean la expresión *polinomio de Hilbert* para el caso con $r = 1$, donde $\mathscr{L}_1 = \mathscr{O}_X(1)$ es un haz muy amplio y $\mathscr{F}$ arbitrario. En este contexto hay que tener ojo con que el esquema se asume proyectivo (para tener haz muy amplio), y en que la elección de un haz muy amplio equivale a elegir de antemano un encaje cerrado $X \hookrightarrow \mathbb{P}_k^n$, de modo que X no es una «variedad abstracta», sino que viene con información concreta. Esto será importante en las cotas débiles de Lang-Weil.

El polinomio de Hilbert-Samuel puede no tener coeficientes enteros, pero es un ***polinomio numérico***, vale decir, que al evaluarlo en enteros nos regresa valores enteros. Así obtenemos lo siguiente:

Corolario 2.16: Sea X un esquema propio sobre un cuerpo k. Sean $\mathscr{L}_1, \ldots, \mathscr{L}_d$ haces invertibles sobre X y $\mathscr{F}$ un haz coherente con $\dim \operatorname{Supp} \mathscr{F} = d$. El coeficiente e que acompaña a $n_1 \cdots n_d$ de $\chi(X, \mathscr{L}_1^{n_1} \otimes \cdots \mathscr{L}_d^{n_d} \otimes \mathscr{F})$ es entero, y definimos el ***símbolo de intersección***:

$$(\mathscr{L}_1 \ldots \mathscr{L}_d . \mathscr{F}) := e.$$

Geométricamente podemos cambiar los haces invertibles por divisores (de Cartier) y los haces coherentes $\mathscr{F}$ por haces estructurales $\mathscr{O}_Z$ de subesquemas cerrados $Z \subseteq X$.

Teorema 2.17: Sea k un cuerpo algebraicamente cerrado y X una superficie suave proyectiva sobre k. Existe una única forma ($\mathbb{Z}$-)bilineal

$$(-.-)\colon \operatorname{Div} X \times \operatorname{Div} X \to \mathbb{Z},$$

tal que:

1. Si C, D son ciclos primos que se intersectan transversalmente, entonces $(C.D) = |C \cap D|$.
2. $(-.-)$ es una forma $\mathbb{Z}$-bilineal simétrica.
3. $(-.-)$ se preserva salvo equivalencia lineal, es decir, si $C_1 \sim C_2$ entonces $(C_1.D) = (C_2.D)$.

Demostración: Hartshorne [**3,** págs. 357-360], thm. V.1.1. □

Lo especial es que es relativamente sencillo verificar que el símbolo de intersección satisface 2. y 3.; la propiedad 1. es más laboriosa, pero también lograble. El teorema anterior es especial puesto que va en la misma línea que otros teoremas que caracterizan determinados cálculos (como los grupos de cohomología con los axiomas de Eilenberg-Steenrod) que uno debe interpretar como que «todo se *debe* calcular puramente empleando las propiedades anteriores».

Definición 2.18: Sea X un esquema propio sobre un cuerpo k. Se dice que un divisor D es ***numéricamente trivial*** si para toda curva íntegra $C \subseteq X$ se cumple que $(C.D) = 0$. Se dice que dos divisores D_1, D_2 son ***numéricamente equivalentes*** (denotado «$D_1 \equiv D_2$») si $D_1 - D_2$ es numéricamente trivial.

Denotamos por $\operatorname{Num} X$ al grupo cociente de los divisores de Cartier por el subgrupo de divisores numéricamente triviales.

Nótese que por los axiomas del número de intersección vemos que el conjunto de divisores numéricamente triviales es efectivamente un subgrupo, y también vemos que $\operatorname{Num} X$ es un cociente de $\operatorname{Pic} X$. El lector puede preguntarse porque hacemos la verificación de $(-.C) = 0$ sobre curvas íntegras $C \subseteq X$ y no sobre subvariedades cerradas; la razón yace en los lemas para los criterios de Nakai-Moishezon y de Seshadri en el cual se verifica que las curvas íntegras suelen captar casi toda la información relevante.

Teorema 2.19 (del índice de Hodge): Sea k un cuerpo algebraicamente cerrado y X una superficie suave proyectiva sobre k. Entonces:

1. Sea $H \in \operatorname{Div} X$ un divisor amplio y sea $D \in \operatorname{Div} X$ tal que $D \not\equiv 0$ pero $D.H = 0$. Entonces $D^2 < 0$.

2. $\mathrm{Num}(X) \otimes_{\mathbb{Z}} \mathbb{R}$ es un $\mathbb{R}$-espacio de forma bilineal (con la multiplicidad de intersección) que, al diagonalizar, tiene un único $+1$ en la diagonal.
3. $\mathrm{Num}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ es un $\mathbb{Q}$-espacio de forma bilineal con descomposición ortogonal $V \otimes W$, donde V es $\mathbb{Q}$-subespacio invariante de $\dim_{\mathbb{Q}} V = 1$ donde la forma es definida positiva y en W es definida negativa.

Demostración: Hartshorne **[3,** pág. 364], thm. V.1.9. □

§2.4 ***Adagio sostenuto:*** **La prueba de Weil.** Ésta es una traducción de la demostración original de Weil **[24]** (1948) en lenguaje esquemático. Seguimos a Hartshorne **[3,** pág. 368], ex. V.1.10.

Nuevamente, fijemos $k := \mathbb{F}_q$ un cuerpo finito, X una curva geométricamente conexa, proyectiva, suave sobre k y $\overline{X} := X_{k^{\mathrm{alg}}}$. Sobre $\overline{X}$ tenemos dos endomorfismos de Frobenius:

$$\mathrm{Frob}_{\overline{X}/k} := \mathrm{Frob}_{X/k} \times_{k^{\mathrm{alg}}} \mathrm{Id}_{k^{\mathrm{alg}}}, \qquad \psi := \mathrm{Id}_X \times_{k^{\mathrm{alg}}} \mathrm{Frob}_{k^{\mathrm{alg}}/k}\,.$$

Sea $Y := \overline{X} \times_{k^{\mathrm{alg}}} \overline{X}$. Denótese $\Delta := \mathrm{Img}\,\Delta_{\overline{X}/k^{\mathrm{alg}}}$ y F_n la imagen del gráfico de $\mathrm{Frob}^n_{\overline{X}/k}$; ambos son ciclos primos de Y (¿por qué?).

Lema 2.20: Se tiene que $[F_n] = ((\mathrm{Frob}_{\overline{X}/k} \times \mathrm{Id}_{\overline{X}})^*)^n[\Delta]$.

Demostración: Es claro que $((\mathrm{Frob}_{\overline{X}/k} \times \mathrm{Id}_{\overline{X}})^*)^n = (\mathrm{Frob}_{\overline{X}/k} \times \mathrm{Id}_{\overline{X}})^*$, así que bastará probar en general que para todo endomorfismo $g\colon \overline{X} \to \overline{X}$ se cumple que $[\mathrm{Img}(\Gamma_g)] = (g \times \mathrm{Id}_{\overline{X}})^*[\Delta]$. □

Lema 2.21: Para todo $n \in \mathbb{N}$ tenemos que $|X(\mathbb{F}_{q^n})| = ([F_n].[\Delta])$.

Demostración: Nótese que F_n, Δ se cruzan transversalmente. Más aún, como F_n, Δ son irreducibles de dimensión 1, solo deben cortarse en puntos cerrados. Ahora bien, por el teorema de ceros de Hilbert, dado que $\overline{X}$ es un esquema de tipo finito sobre un cuerpo algebraicamente cerrado, tenemos que los puntos cerrados de Y están en correspondencia con pares ordenados en $\overline{X}$. Finalmente, $\mathrm{Frob}^n_{\overline{X}}(x) = x$ (es decir, x es un punto $\mathbb{F}_{q^n}$-valuado) syss está fijado por $\mathrm{Id}_{\overline{X}} \times \mathrm{Frob}^n_{k^{\mathrm{alg}}/k}$. □

Finalmente, estamos listos para probar la hipótesis de Riemann:

Demostración: Sea $W := \mathrm{Num}(Y) \otimes \mathbb{Q}$. Sean H, V las curvas horizontal y vertical en $Y = \overline{X} \times \overline{X}$. Nótese que $[H], [V]$ son distintos en $\mathrm{Num}(Y)$, puesto que $[H].[V] = 1$ y $[H].[H] = 0$. Sean $U := [H]\mathbb{Q} \oplus [V]\mathbb{Q} \leq W$, y sea U' el complemento ortogonal de U, de modo que $W = U \oplus U'$. La matriz de la forma bilineal sobre U, respecto a la base $[H], [V]$ es:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

y ésta matriz posee un valor propio positivo, luego el subespacio definido positivo está contenido en U y, como tiene dimensión 1, no está en U'. Luego la forma es definida negativa en U'.

Sea $\Gamma_F := \mathrm{Frob}_{\overline{X}} \times \mathrm{Id}_{\overline{X}} \colon \overline{X} \to Y$, y sea $T \colon W \to W$ la transformación lineal dada por $T(D) := (\Gamma_F)^* D$. Nótese que $\deg(\Gamma_F) = q$, luego, para divisores $D, E \in \mathrm{Num}(Y)$ se da

$$\big((\Gamma_F)^* D, (\Gamma_F)^* E\big) = \big(D, (\Gamma_F)_* (\Gamma_F)^* E\big) = (D, qE) = q(D, E).$$

Así, para $u, v \in W$, vemos que $(Tu, Tv) = q(u, v)$.

Ahora bien, por el lema 2.20, sabemos que $T^n[\Delta] = [F_n]$ Finalmente, es fácil verificar que $T[H] = q[H], T[V] = [V]$ y descomponer $[\Delta] = [H] + [V] + [w]$ donde $w \in U'$, luego calculamos:

$$\begin{aligned} |X(\mathbb{F}_{q^n})| &= ([F_n], [\Delta]) = (T^n[\Delta], [\Delta]) \\ &= \big(T^n([H] + [V] + w), ([H] + [V] + w)\big) = q^n + 1 + (T^n w, w). \end{aligned}$$

Aplicando la desigualdad de Cauchy-Schwarz sobre U', donde la forma es definida negativa, vemos que

$$|(T^n w, w)| \leq \sqrt{|(T^n w, T^n w)|\,|(w, w)|} = \sqrt{q^n\,|u, v|} = O(q^{n/2}).$$

La hipótesis de Riemann queda probada por la equivalencia 2.8. □

§2.5 ***Allegro vivace:*** **Aplicaciones.** La siguiente aplicación es inmediata:

Proposición 2.22: Sea k un cuerpo finito y C una curva sobre k. Entonces no existen k-morfismos $f \colon C \times_k C \to \mathbb{P}^1_k$ universalmente inyectivos; i.e., siempre existe una extensión finita suficientemente grande K/k tal que $(C \times_k C)(K) \to \mathbb{P}^1(K)$ no es inyectivo (cfr. Liu **[5,** pág. 208], ex. 5.3.8).

Una demostración esquemática de éste hecho (generalizada a un cuerpo base arbitrario) iría por las siguientes líneas. Sabemos que el morfismo $f \colon X \to Y$ es universalmente inyectivo syss f es inyectivo y para cada $x \in X$ la extensión de cuerpos $\Bbbk(x)/\,\Bbbk\big(f(x)\big)$ es puramente inseparable (cfr. **[5,** págs. 200, 208], def. 5.3.13 y ex. 5.3.8). Como f es continuo (a nivel de espacios topológicos), entonces no puede ser inyectivo, pues f respeta especializaciones: En particular, como $C \times_k C$ tiene dimensión 2, podremos encontrar una cadena de puntos $\bullet \rightsquigarrow \bullet \rightsquigarrow \bullet$ que se deba mandar a una cadena similar en $\mathbb{P}^1_k$, la cual no existe por dimensión. No obstante, las conjeturas de Weil dan un argumento combinatorio del por qué no puede suceder y, de hecho, predicen efectivamente hasta que grado falla.

Un contraejemplo para cuerpos finitos pequeños siempre se puede construir a mano. Fijando $k = \mathbb{F}_q$ entonces la curva afín dada por

$$C' \colon \quad x^q - x = y^2 - a,$$

donde $a \notin k^{\times 2}$ no es un cuadrado, no posee puntos k-racionales (el lado izquierdo siempre es nulo, y el derecho no). Si homogeneizamos la ecuación

obtenemos

$$C := \{[x : y : z] \in \mathbb{P}^2_k : x^q - xz^{q-1} = y^2z^{q-2} - az^q\} \subseteq \mathbb{P}^2_k,$$

la cual, si $q > 2$, solo consta del punto k-racional $[0 : 1 : 0]$. Luego componiendo $C \times_k C \twoheadrightarrow C \to \mathbb{P}^1_k$, donde el primer morfismo es una proyección (cualquiera), y el segundo está dado por $[x : y : z] \mapsto [x : y]$ (nótese que $[0 : 0 : 1] \notin C$). Así, el morfismo resultante es inyectivo, pues $C \times_k C$ solo tiene un punto k-racional.

La siguiente aplicación está inspirada en una cota de Lang-Weil, aunque es considerablemente más débil.

Teorema 2.23 (cotas débiles de Lang-Weil): Sea X una variedad proyectiva geométricamente irreducible de dimensión r sobre cuerpo finito k. Entonces, para toda extensión $\mathbb{F}_q/k$:

$$|X(\mathbb{F}_q)| = q^r + O(q^{r-1/2}).$$

Más aún, si existe un encaje cerrado $X \hookrightarrow \mathbb{P}^n_k$ entonces $|X(\mathbb{F}_q)| \leq q^r + Aq^{r-1/2}$, donde A depende exclusivamente polinomio de Hilbert-Samuel de X y la dimensión n del espacio proyectivo en el cual podemos encajarlo.

Demostración: Nótese que si X no es suave, entonces como el locus suave es abierto, sus singularidades forman un cerrado en X con componentes (geométricas) irreducibles $Z_1, \ldots, Z_n$, luego, por hipótesis inductiva,

$$|X_{\mathrm{reg}}(\mathbb{F}_q)| = |X(\mathbb{F}_q)| - \sum_{i=1}^{n} |Z_i(\mathbb{F}_q)| = |X(\mathbb{F}_q)| - \underbrace{nq^{r-1} + O(q^{r-1-1/2})}_{\ll q^{r-1/2}},$$

donde «$\ll$» es notación de Vinogradov y donde X_{reg} representa el conjunto (o *locus*) suave. Así que podemos suponer que X es suave.

Procedemos por inducción sobre la dimensión d. Si $d = 1$, entonces esto es la hipótesis de Riemann para curvas usual. Podemos suponer que $d \geq 2$, entonces podemos restringirnos a un abierto U que es, por tanto, denso, y por lo tanto, los puntos que no vamos a contar representan un cerrado $X \setminus U = \bigcup_{i=1}^m Y_i$, donde Y_i son sus componentes irreducibles de dimensiones $< r$:

$$|(X \setminus U)(\mathbb{F}_q)| = \sum_{i=1}^{m} |Y_i(\mathbb{F}_q)| \ll q^{r-1}.$$

Más precisamente, vamos a elegir un abierto afín U y el teorema de normalización de Noether nos da un morfismo suprayectivo finito $U \twoheadrightarrow \mathbb{A}^r_k$, que luego componemos con la proyección $\mathbb{A}^r_k \twoheadrightarrow \mathbb{A}^1_k$ (pues $r \geq 2$), y por tanto tenemos un morfismo suprayectivo $U \twoheadrightarrow \mathbb{A}^1_k$.

Ahora un pequeño argumento técnico: nótese que el cuerpo de funciones $L := K(U)$ es una extensión de k, de modo que podemos tomar un *modelo proyectivo suave* P de L, el cual existe y será birracional a X. Luego, por

factorización de Stein (cfr. HARTSHORNE [**3,** pág. 280], cor. III.11.5) tenemos una factorización:

$$\begin{array}{ccc} P & \xrightarrow{f} & C \\ \text{birracional}\,\vdots\uparrow & & \downarrow\,\text{finito} \\ X & \twoheadrightarrow & \mathbb{A}^1_k \end{array}$$

Como el conteo de puntos no cambia pasando a una variedad birracional vamos a sustuir X con P, y suponer que tenemos un morfismo dominante $f\colon X \twoheadrightarrow C$ con fibras geométricamente íntegras, donde C es una curva completa, geométricamente íntegra. Finalmente, como los puntos cerrados van a puntos cerrados, podemos contar:

$$\begin{aligned} |X(\mathbb{F}_q)| &= \sum_{y\in C(\mathbb{F}_q)} |X_y(\mathbb{F}_q)| = \sum_{y\in C(\mathbb{F}_q)} \left(q^{r-1} + a_y q^{r-1-1/2}\right) \\ &= q^r + \left(\sum_{y\in C(\mathbb{F}_q)} a_y\right) q^{r-1/2}, \end{aligned}$$

donde los a_y's dependen de las propiedades geométricas de la fibra X_y; en particular del polinomio de Hilbert-Samuel por hipótesis inductiva (¡respecto al encaje $X_y \hookrightarrow X \hookrightarrow \mathbb{P}^n_k$!). Nótese que todo morfismo desde un esquema íntegro una curva irreducible normal es plano (cfr. GÖRTZ y WEDHORN [**2,** pág. 492], prop. 15.4) y dado un morfismo plano, entonces las fibras comparten polinomio de Hilbert-Samuel (cfr. HARTSHORNE [**3,** pág. 261], thm. III.9.9); borrando los finitos puntos singulares de C vemos que los a_y están acotados por un solo valor B. Así $|X(\mathbb{F}_q)| \leq q^r + B' q^{r-1-1/2}$ (donde el B' es una modificación del B para contar los puntos sin contar fuera del X).

Finalmente, para ver que este B' solo depende del polinomio de Hilbert-Samuel y de la dimensión del encaje, notamos que en $\mathbb{P}^n_k$ hay finitas subvariedades de dimensión r y polinomio de Hilbert-Samuel $Q := Q_X(t)$ fijo definidas sobre k. Esto es puesto que corresponden a puntos k-racionales del esquema de Hilbert $\mathrm{Hilb}_Q(\mathbb{P}^n/k)$, el cual es proyectivo (cfr. KOLLÁR [**4,** pág. 10], thm. I.1.4). Así que definimos la constante A del enunciado como el máximo de los $B'(X)$. □

Más generalmente, si X es una variedad completa geométricamente equidimensional sobre un cuerpo finito k, entonces vemos su cambio de base $X_{k^{\mathrm{alg}}}$ y, como es un esquema algebraico, es compacto y posee finitas componentes irreducibles (geométricas) c. Entonces para toda extensión $\mathbb{F}_q/k$ tenemos:

$$|X(\mathbb{F}_q)| = cq^r + O(q^{r-1/2}), \qquad r = \dim X.$$

El trabajo original de Lang-Weil da la siguiente cota mucho más aguda (cuando X es geométricamente irreducible, de grado d, cfr. **[20],** thm. 1):

$$|X(\mathbb{F}_q)| \leq q^r + (d-1)(d-2)q^{r-1-1/2} + O(q^{r-1}).$$

Nuestra demostración, empleando las cotas de Hasse-Weil, da el mismo resultado para superficies, pero para poder demostrar la cota aguda por inducción habría que controlar el grado de las fibras en función del grado del dominio.

Las cotas de Lang-Weil tienen consecuencias en la reducción de variedades sobre un cuerpo global a sus cuerpos locales (en particular, las cotas débiles bastan). Para ello, hagamos el siguiente recuerdo:

Definición 2.24: Sea K un cuerpo global (i.e., o bien es una extensión finita de $\mathbb{Q}$ (característica 0), o bien una extensión finita de $\mathbb{F}_p(t)$ (característica p)). Se denota por M_K el conjunto de lugares de K (i.e., clases de equivalencia de valores absolutos no triviales). Un lugar v se dice ***arquimediano*** o «al infinito» si un valor absoluto que le representa satisface la propiedad arquimediana (equivalentemente, si la compleción respecto a v, denotada K_v, admite un monomorfismo de cuerpos topológicos hacia $\mathbb{C}$). Se denota por S_∞ al conjunto de lugares arquimedianos.

Dado un lugar no arquimediano v representado por un valor absoluto $||$, definimos los siguientes conjuntos:

$$\mathfrak{o}_v := \{\alpha \in k : |\alpha| \leq 1\}, \qquad \mathfrak{p}_v := \{\alpha \in \mathfrak{o}_k : |\alpha| < 1\}, \qquad \Bbbk(v) := \mathfrak{o}_v/\mathfrak{p}_v.$$

Dado un conjunto finito S de lugares tal que $S_\infty \subseteq S \subseteq M_K$, se llama el ***anillo de S-enteros*** al subanillo

$$\mathcal{O}_{K,S} := \{\alpha \in K : \forall v \notin S \quad \alpha \in \mathfrak{o}_v\} \subseteq K.$$

Por ejemplo, si $S = \{2, 3, \infty\} \subseteq M_{\mathbb{Q}}$, entonces $\mathcal{O}_{\mathbb{Q},S}$ es el conjunto de números racionales cuyo denominador solo puede tener por factores primos al 2 o al 3. Si $S := S_\infty$, entonces $\mathcal{O}_{K,S} = \mathcal{O}_K$.

Lema 2.25: Sea $f\colon X \to Y$ un morfismo entre esquemas de tipo finito (sobre $\mathbb{Z}$). Sea q una potencia de un primo, sea $y \in Y(\mathbb{F}_q)$ y sea $X_y := X \times_Y \operatorname{Spec} \Bbbk(y)$ la fibra. Si X_y es geométricamente íntegra y q es suficientemente grande, entonces X_y posee un punto $\mathbb{F}_q$-racional suave (sobre $\mathbb{F}_q$).

Demostración: Empleando las cotas fuertes de Lang-Weil, vemos que, si $r := \dim(X_y)$, entonces $|X_y| = q^r + O(q^{r-1/2})$, donde las constantes implicadas no dependen tampoco de la característica de $\mathbb{F}_q$. Así pues, todo punto «geométrico», es decir, todo punto cerrado de $(X_y)_{\mathbb{F}_q^{\mathrm{alg}}}$, es un punto $\mathbb{F}_q$-racional para un q suficientemente grande. Sea U el locus suave del morfismo $f\colon X \to Y$, el cual es abierto y, como la fibra X_y es geométricamente íntegra, entonces su locus suave (como variedad sobre $\mathbb{F}_q$) es U_y. Así, reemplazando X por U, basta probar que la fibra X_y tiene puntos $\mathbb{F}_q$-racionales para q suficientemente grande, pero esto se sigue de las cotas fuertes de Lang-Weil. □

Teorema 2.26: Sea X una variedad geométricamente irreducible sobre un cuerpo global K. Entonces $X(K_v)$ es no vacío para todos salvo finitos lugares $v \in M_K$.

Demostración: La teoría de aproximación noetheriana absoluta (cfr. Poonen [**13,** pág. 60], thm. 3.2.1) nos dice que, mirando a X como un esquema sobre $K = \mathscr{O}_{A,\eta}$, donde η es el punto genérico del espectro de $A := \mathcal{O}_K$, entonces existe un esquema $\mathcal{X}$ de tipo finito sobre un abierto de $\mathrm{Spec}(\mathcal{O}_K)$ tal que $\mathcal{X}_\eta = X$ y cuyas fibras sean geométricamente íntegras. En nuestro caso, ese abierto puede elegirse de la forma $\mathrm{Spec}(\mathcal{O}_{K,S})$ donde $S_\infty \subseteq S \subseteq M_K$ es un conjunto finito de lugares.

Finalmente, aplicando el lema anterior al morfismo $\mathcal{X} \to \mathrm{Spec}(\mathcal{O}_{K,S}) =: Y$ y recordando que los puntos cerrados $y \in Y$ tienen cuerpo de restos $\Bbbk(y)$ finito (y que solo finitos y's comparten característica), vemos que para todo salvo finitos y's se cumple que $\mathcal{X}_y$ posee puntos racionales suaves. Finalmente, sea $y \in Y$ cerrado, lo que corresponde a un lugar v de $\mathcal{O}_K$, entonces el anillo local $\mathscr{O}_{Y,y} = \mathfrak{o}_v =: A$ es henseliano (por el lema de Hensel ya que es completo, cfr. Milne [**12,** pág. 35], prop. I.4.5), y el morfismo $\mathcal{X}_y \to \mathrm{Spec}\, A$ es suave, por lo que, el morfismo $\mathcal{X}_y(A) \twoheadrightarrow \mathcal{X}_y(\Bbbk(y))$ es suprayectivo (cfr. [**12,** pág. 39], ex. I.4.13). Así que $\mathcal{X}_y(\mathfrak{o}_v) \subseteq \mathcal{X}_y(K_v) = X_y(K_v)$ es no vacío. □

3. Teorías de cohomología de Weil

> A decir verdad, mis reflexiones sobre las conjeturas de Weil mismas, en vista a demostrarlas, fueron esporádicas. El panorama que comenzaba a abrirse ante mí, y que me esforzaba en escrutar y captar, sobrepasaba en mucho la amplitud y la profundidad de las hipotéticas necesidades de una demostración, e incluso de todo lo que esas famosas conjeturas habían dejado entrever. Con la aparición del tema esquemático y el de los topos, un mundo nuevo e insospechado se abrió de repente. En él «las conjeturas» ocupaban un lugar central, ciertamente, un poco como la capital de un vasto imperio o continente de innumerables provincias, donde la mayoría no tiene más que relaciones lejanas con ese lugar brillante y prestigioso. Sin habérmelo dicho jamás, sabía que en adelante sería el servidor de una gran tarea: explorar ese mundo inmenso y desconocido, descubrir sus límites hasta las fronteras más lejanas; y también recorrer en todos los sentidos e inventariar con un cuidado tenaz y metódico las provincias más cercanas y accesibles, y trazar planos con fidelidad y precisión escrupulosa, donde el menor caserío y la menor choza tuvieran su sitio...
>
> –Alexander Grothendieck [**25,** pág. 59].

Para ésta sección seguimos la exposición de Kleiman [**11**].

En primer lugar, conviene escribir las conjeturas de Weil en toda su generalidad. Sea X una variedad geométricamente íntegra, proyectiva y suave de dimensión d sobre un cuerpo finito $\mathbb{F}_q$.

CW1. **Racionalidad:** $Z(X,t)$ es una función racional y de hecho:

$$Z(X,t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)} \in \mathbb{Q}(t),$$

donde cada $P_i(t) \in \mathbb{Z}[t]$, donde $P_0(t) = 1-t, P_{2d}(t) = 1-q^d t$ y cada $P_i(t) = \prod_j (1-\alpha_{ij}t) \in \mathbb{Q}^{\mathrm{alg}}[t]$ con $0 < i < 2d$.

CW2. **Ecuación funcional:** Sea $\chi := (-1)^d(p_a+1)$, donde p_a denota el género aritmético de X.[5] Entonces

$$Z\left(X, \frac{1}{q^d t}\right) = \pm q^{d\chi/2} t^\chi Z(X,t). \tag{4}$$

CW3. **Hipótesis de Riemann:** Se cumple que $|\alpha_{ij}| = q^{i/2}$ para $0 < i < 2d$.

CW4. **Números de Betti:** Supongamos que X viene por reducción módulo $\mathfrak{p}$ de una variedad X_0 sobre un cuerpo numérico K. Entonces $\deg P_i = \beta_i$, los números de Betti del cambio de base $X_0 \times_K \operatorname{Spec}\mathbb{C}$. (En particular, $\chi = \sum_{i=0}^{2d}(-1)^i\beta_i$.)

El formalismo de Weil es que, si por algún milagro las variedades sobre $\mathbb{F}_q$ se comportasen como complejos celulares en topología algebraica, entonces al menos la racionalidad y la ecuación funcional se seguirían de resultados estándar.

Para formular la definición de una teoría de cohomología de Weil, necesitamos hablar del ***anillo de Chow***. Recuérdese que $\mathcal{Z}^r(X)$ representa el grupo (aditivo) de ciclos de codimensión pura r, es decir, una suma finita formal de subvariedades (cerradas) de codimensión r. Si X es una variedad, entonces $\mathcal{Z}^0(X) = \mathbb{Z}\cdot[X]$, es decir, es el grupo cíclico generado por el símbolo $[X]$. Dos ciclos C_1, C_2 de dimensión pura d se dicen ***racionalmente equivalentes***, denotado $C_1 \sim C_2$, si existen finitas subvariedades $W_i \subseteq X$ de dimensión $d+1$ y $f_i \in K(W_i)^\times$ tales que

$$C_1 - C_2 = \sum_i [\mathrm{div}(f_i)].$$

Si C_1, C_2 son divisores de Weil (i.e., ciclos de codimensión pura 1), entonces la equivalencia racional es lo que se suele llamar *equivalencia lineal*. Los ciclos racionalmente equivalentes a 0 conforman un subgrupo $R^r(X)$ y, por tanto, definimos el cociente $\mathrm{CH}^r(X) := \mathcal{Z}^r(X)/\sim_{\mathrm{rat}} = \mathcal{Z}^r(X)/R^r(X)$.

Así, $\mathrm{CH}^*(X) := \bigoplus_{n\in\mathbb{N}} \mathrm{CH}^n(X)$ forma un grupo abeliano graduado y, de hecho, forma un anillo graduado (cfr. Fulton **[1,** págs. 93-94**]**).

Definición 3.1: Sea k un cuerpo (usualmente, algebraicamente cerrado) y sea F un cuerpo de característica 0, llamado ***cuerpo de coeficientes***. Denotaremos por PsVar_k a la (sub)categoría (plena) de variedades proyectivas suaves sobre k. También denotaremos por GAcAlg_F a la categoría de F-álgebras ($\mathbb{N}$-)graduadas anticonmutativas.

[5] Equivalentemente, $\chi = \chi_k(X, \mathscr{O}_X)$ es la característica de Euler-Poincaré (cfr. Hartshorne **[3,** pág. 230**]**, ex. III.5.4).

Una ***teoría de cohomología de Weil*** sobre k es un funtor contravariante $H^*\colon \mathsf{PsVar}_k \to \mathsf{GAcAlg}_F$ tal que, dada una variedad X de $\dim X =: d$ satisface:

TC1. **Finitud:** $\dim_F H^q(X) < \infty$ para todo $q \geq 0$ y $H^q(X) = 0$ cuando $q > 2d$.

TC2. **Dualidad de Poincaré:** Existe un isomorfismo F-lineal $\int_X\colon H^{2d}(X) \to F$ llamado la ***aplicación de traza***. El producto sobre $H^*(X)$, llamado ***producto copa***, hace que

$$\smile\colon H^i(X) \times H^{2d-i}(X) \longrightarrow H^{2d}(X) \cong F$$

sea un emparejamiento perfecto.

TC3. **Fórmula de Künneth:** Para todo par de variedades X, Y, las proyecciones inducen (mediante H^* como funtor) un isomorfismo

$$H^*(X) \otimes_F H^*(Y) \xrightarrow{\sim} H^*(X \times_k Y). \tag{5}$$

TC4. **Mapa de ciclos:** Existe un homomorfismo de anillos graduados $\gamma_X\colon \mathrm{CH}^*(X) \to H^{2*}(X) = \bigoplus_{n\in\mathbb{N}} H^{2n}(X)$ que determina una transformación natural $\mathrm{CH}^* \Rightarrow H^{2*}$, tal que dados $Z \in \mathcal{Z}^*(X), W \in \mathcal{Z}^*(Y)$ se cumple que $\gamma_{X\times_k Y}(Z \times_k W) = \gamma_X(Z) \otimes_F \gamma_Y(W)$, y tal que, con $P = \operatorname{Spec} k$ se cumple que $\gamma_P\colon \mathcal{Z}^0(P) = \mathbb{Z} \hookrightarrow H^0(P) = F$ coincide con el (único) homomorfismo de anillos.

TC5. **Teorema débil de Lefschetz:** Sea $h\colon W \hookrightarrow\!\!\!\!\rightarrow X$ la sección de un hiperplano suave. Entonces $H^q(h)\colon H^q(X) \to H^q(W)$ es un isomorfismo para $q \leq d-2$ y es un monomorfismo para $q = d-1$.

TC6. **Teorema fuerte de Lefschetz:** Sea W la sección de un hiperplano suave, y sea

$$\begin{aligned} L_W\colon H^q(X) &\longrightarrow H^{q+2}(X) \\ x &\longmapsto x \smile \gamma_X(W), \end{aligned}$$

un homomorfismo llamado ***operador de Lefschetz***. Para $q \leq d$, la composición de $d-i$ veces el operador da un isomorfismo

$$L_W^{d-i}\colon H^q(X) \xrightarrow{\sim} H^{2d-q}(X).$$

Fijemos una teoría de cohomología de Weil H^* con coeficientes en F. Sea $f\colon X \to Y$ un morfismo de variedades proyectivas suaves sobre k, entonces denotamos por $f^* := H^*(f)\colon H^*(Y) \to H^*(X)$ el homomorfismo de F-álgebras dado por funtorialidad contravariante de H^*. Por dualidad de Poincaré, si $d := \dim X$, sabemos que $H^i(X)^\vee \cong H^{2d-i}(X)$, así que dualizando f^* y definiendo $c := \dim X - \dim Y$ obtenemos un homomorfismo:

$$f_*\colon H^i(X) \longrightarrow H^{i-2c}(Y).$$

Lema 3.2: Sea $f\colon X \to Y$ un k-morfismo de variedades proyectivas suaves sobre k. Para todo $y \in H^*(Y)$ tenemos que

$$(\pi_1)_*\big(\gamma_{X\times_k Y}(\Gamma_f) \smile \pi_2^* y\big) = f^*(y),$$

donde π_1, π_2 son las proyecciones con dominio $X \times_k Y$.

En el enunciado, Γ_f es el ***gráfico*** de f, vale decir, la clausura de $(\mathrm{Id}_X, f)\colon X \to X \times_k X$; mientras que $\Delta_{X/k}$ es la clausura de la imagen del morfismo diagonal o, lo que es lo mismo, el gráfico de la identidad.

Demostración: Basta calcular:

$$\begin{aligned}(\pi_1)_*\big(\gamma_{X\times_k Y}(\Gamma_f) \smile \pi_2^* y\big) &= (\pi_1)_*\big((\mathrm{Id}_X, f)_*(1) \smile \pi_2^* y\big)\\ &= (\pi_1)_*(\mathrm{Id}_X, f)_*\big(1 \smile (\mathrm{Id}_X, f)^*\pi_2^* y\big)\\ &= (\mathrm{Id}_X)_*\big(1 \smile f^* y\big) = f^* y. \qquad \square\end{aligned}$$

Lema 3.3: Sea $\{\boldsymbol{e}_i\}_i$ una base para $H^*(X)$ y sea $\{\boldsymbol{f}_j\}_j$ una base dual de $H^*(X)$ (i.e., $\boldsymbol{e}_i \smile \boldsymbol{f}_j = \delta_{ij}\boldsymbol{e}^{2d}$, donde $\int_X \boldsymbol{e}^{2d} = 1$). Para todo morfismo $g\colon X \to X$ se satisface que

$$\gamma_{X\times_k X}(\Gamma_g) := \sum_{i,j} g^*(\boldsymbol{e}_i) \otimes \boldsymbol{f}_j.$$

Demostración: Por la fórmula de Künneth, tenemos que

$$\gamma_{X\times_k X}(\Gamma_g) = \sum_i \boldsymbol{v}_i \otimes \boldsymbol{f}_i, \qquad \boldsymbol{v}_i \in H^*(X).$$

Aplicando el lema anterior obtenemos

$$g^*(\boldsymbol{e}_j) = (\pi_1)_*\left((\textstyle\sum_i \boldsymbol{v}_i \otimes \boldsymbol{f}_i) \smile (1 \otimes \boldsymbol{e}_j)\right) = (\pi_1)_*(\boldsymbol{v}_j \otimes \boldsymbol{e}^{2d}) = \boldsymbol{v}_j. \qquad \square$$

Teorema 3.4 (de la traza de Lefschetz): Sea X una variedad proyectiva y suave sobre un cuerpo algebraicamente cerrado k, sea H^* una teoría de cohomología de Weil sobre k, y sea $g\colon X \to X$ un k-morfismo de variedades. Entonces

$$(\Gamma_g.\Delta_{X/k}) = \sum_{r=0}^{2d} (-1)^r \operatorname{tr} H^r(g).$$

Aquí «$H^r(g)$» en el enunciado, denota precisamente lo que denota, puesto que por hipótesis H^r era un funtor. Otros libros emplean $\operatorname{tr}(g; H^r(X))$ o $\operatorname{tr}(g|_{H^r(X)})$.

Demostración: Sea $\{\boldsymbol{e}_i^r\}_i$ una base de $H^r(X)$ y $\{\boldsymbol{f}_j^{2d-r}\}_j$ una base dual de $H^{2d-r}(X)$. Escribamos

$$\gamma(\Gamma_g) = \sum_{i,r} g(\boldsymbol{e}_i^r) \otimes \boldsymbol{f}_i^{2d-r},$$

$$\gamma(\Delta_{X/k}) = \sum_{i,r} \boldsymbol{e}_i^r \otimes \boldsymbol{f}_i^{2d-r} = \sum_{i,r} (-1)^{r(2d-r)} \boldsymbol{f}_i^{2d-r} \otimes \boldsymbol{e}_i^r = \sum_{i,r} (-1)^r \boldsymbol{f}_i^{2d-r} \otimes \boldsymbol{e}_i^r.$$

Aplicando productos, se obtiene que

$$\gamma(\Gamma_g \cdot \Delta_{X/k}) = \sum_{i,r} (-1)^r g^*(\boldsymbol{e}_i^r) \boldsymbol{f}_i^{2d-r} \otimes \boldsymbol{e}^{2d} = \sum_r (-1)^r \operatorname{tr}(H^r(g))(\boldsymbol{e}^{2d} \otimes \boldsymbol{e}^{2d}).$$

Concluimos aplicando la traza $\int_X$ (TC2). □

§3.1 Racionalidad y ecuación funcional. Desde aquí en adelante fijaremos X una variedad de $\dim X =: d$ geométricamente íntegra, proyectiva, suave sobre un cuerpo finito $k = \mathbb{F}_q$. Denotamos $\overline{X} := X_{k^{\mathrm{alg}}}$ el cambio de base. También, H denotará una teoría de cohomología de Weil sobre k^{alg}.

Definición 3.5: Sea $F\colon X \to Y$ un morfismo finito dominante entre esquemas íntegros, donde $\xi \in X$ es el punto genérico. Entonces induce una extensión finita de cuerpos $f := F_\xi^\sharp\colon K(Y) \to K(X)$ y se define el ***grado*** de f como $\deg f := \big[K(X) : f[K(Y)]\big]$ (cfr. Liu **[5,** págs. 67, 112**]**, ex. 2.4.11(iv) y ex. 3.3.15)

Lema 3.6: El endomorfismo de Frobenius $\mathrm{Frob}_{X/k}\colon X \to X^{(q)}$ tiene grado q^d.

Demostración: Fijemos notación, sea $\xi \in X$ el punto genérico y sea $f := (\mathrm{Frob}_{X/k})_\xi^\sharp\colon K(X^{(q)}) \to K(X)$. Haremos primero el caso de $X = \mathbb{A}_k^d$ (aunque no sea proyectivo). Así $K(X) = k(x_1, \ldots, x_d)$ y f está inducido por:

$$\begin{aligned} f|_{k[\boldsymbol{x}]}\colon k[\boldsymbol{x}] &\longrightarrow k[\boldsymbol{x}] \\ x_i &\longmapsto x_i^q. \end{aligned}$$

Es claro que $k[x_1, \ldots, x_d]$ es un $k[x_1^q, \ldots, x_d^q]$-módulo libre de rango q^d, de modo que al tensorizar por $\mathrm{Frac}(k[\boldsymbol{x}]) = k(\boldsymbol{x})$, vemos que induce una extensión de grado q^d.

Ahora sigamos con X en general. Sea $t_1, \ldots, t_d$ una base de trascendencia de $K(X)$ sobre $\mathbb{F}_q = k$, de modo que $K(X)/k(\boldsymbol{t})$ es una extensión finita. Entonces nótese que f satisface que $f[K(X)] \cap k(\boldsymbol{t}) = f[k(\boldsymbol{t})]$ (donde $f[K(X)] =$). Además $K(X^{(q)}) := f[K(X)] \vee k(\boldsymbol{t})$, de modo que tenemos que

$$[K(X) : K(X^{(q)})] = \big[k(\boldsymbol{t}) : f[k(\boldsymbol{t})]\big] = q^d$$

por el caso anterior. □

Proposición 3.7: Para todo $m \geq 1$ se cumple

$$N_m := |X(\mathbb{F}_{q^m})| = \sum_r (-1)^r \operatorname{tr} H^r(\mathrm{Frob}_{X/k}^m).$$

Demostración: Esto se sigue del teorema de la traza de Lefschetz aplicado al morfismo de Frobenius $F\colon \overline{X} \to \overline{X}$, en cuyo caso la expresión del enunciado iguala al símbolo de intersección $(\Gamma_F.\Delta_{\overline{X}/k^{\mathrm{alg}}})$, pero los ciclos Γ_F, Δ se intersectan transversalmente puesto que sus espacios tangentes son ortogonales, así que cuenta $\Gamma_F \cap \Delta$ los cuales son los puntos $\mathbb{F}_{q^m}$-racionales de la diagonal. □

El siguiente lema es pura álgebra lineal:

Lema 3.8: Sea $\varphi\colon V \to V$ un endomorfismo de k-espacios vectoriales de dimensión finita y sea $P_\varphi(t) = \prod_{i=1}^n (1 - \omega_i t)$ su polinomio característico. Entonces $\operatorname{tr}(\varphi^m) = \sum_{i=1}^n \omega_i^m$ y, por tanto,

$$\log(1/P_\varphi(t)) = \sum_{m=1}^{\infty} \operatorname{tr}(\varphi^m)\frac{t^m}{m}.$$

Demostración: Podemos tensorizar por k^{alg}. Basta notar que si $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ es una base por vectores propios tal que $\varphi(\boldsymbol{v}_i) = \omega_i \boldsymbol{v}_i$, entonces $\varphi^m(\boldsymbol{v}_i) = \omega_i^m \boldsymbol{v}_i$. El resto es un ejercicio. □

Agrupando todo, se prueba la racionalidad (CW1):

Teorema 3.9: Sea X una variedad geométricamente íntegra, proyectiva, suave sobre un cuerpo finito k de dimensión d. Entonces

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

es una función racional, donde cada

$$P_r(X,t) = \det(\mathrm{Id} - \mathrm{Frob}^*_{\overline{X}/k}\, t; H^r(X)) \in F^{\mathrm{alg}}[t].$$

Aquí F denota el cuerpo de coeficientes de la teoría de cohomología de Weil.

Demostración: Se calcula

$$\begin{aligned}
Z(X,t) &= \exp\left(\sum_{m=1}^{\infty} N_m \cdot \frac{t^m}{m}\right) && \text{(prop. 2.3)}\\
&= \exp\left(\sum_{m=1}^{\infty}\sum_{r=0}^{2d} (-1)^r \operatorname{tr} H^r(\mathrm{Frob}^m)\frac{t^m}{m}\right)\\
&= \prod_{r=0}^{2d} \exp\left(\sum_{m=1}^{\infty} \operatorname{tr} H^r(\mathrm{Frob}^m)\frac{t^m}{m}\right)^{(-1)^r}\\
&= \prod_{r=0}^{2d} P_r(X,t)^{(-1)^{r+1}}. && \text{(prop. anterior)}
\end{aligned}$$

□

Una ventaja curiosa es que $\deg P_r(X,t) = \dim_F H^r(X)$. Cabe destacar que, obviamente, la factorización anterior depende –al menos *a priori*– de la teoría de cohomología de Weil empleada. Más adelante, introduciremos varias teorías distintas y veremos que hay una familia para las cuales la factorización anterior coincide.

Comentario. En una carta a Grothendieck, Serre le explicó que no podía existir una teoría de cohomología de Weil con valores en $\mathbb{R}$ y, por tanto, tampoco con valores en $\mathbb{Q}$. Esto es dos veces perjudicial para nuestra prueba de la racionalidad, ya que el F ni siquiera puede ser $\mathbb{Q}$. No obstante, si existen sobre $\mathbb{Q}_\ell$, y tener muchas «teorías ℓ-ádicas» compatibles (en algún sentido) es como tener una teoría sobre $\mathbb{Q}$.

Lema 3.10: Sea $f(t) \in k[[t]]$ una serie formal tal que $f(t) \in K[t]$ es un polinomio en una extensión K/k. Entonces $f(t) \in k[t]$ es un polinomio.

Notando que, como $F \supseteq \mathbb{Q}$ (pues tiene característica 0), entonces:

Corolario 3.11: La función $Z(X,t)$ es racional con coeficientes en $\mathbb{Q}$.

Lema 3.12: Sea $f(t) = g(t)/h(t)$, donde

$$f(t) \in 1 + t \cdot \mathbb{Z}_\ell[[t]], \qquad g(t), h(t) \in 1 + t \cdot \mathbb{Q}_\ell[t].$$

Si g, h son polinomios coprimos, entonces tienen coeficientes en $\mathbb{Z}_\ell$.

Demostración: Pasando a una extensión finita de $\mathbb{Q}_\ell$, podemos suponer que h se descompone completamente como $h(t) = \prod_{i=1}^n (1 - \omega_i t) \in \mathbb{Q}_\ell[t]$. Si algún $|\omega_j|_\ell > 1$, entonces como $f(t)$ converge en el disco unitario y $|\omega_j|_\ell^{-1} < 1$, vemos que $f(\omega_j^{-1})$ converge, lo cual sería absurdo pues $h(\omega_j^{-1}) = 0 \neq g(\omega_j^{-1})$. Así que necesariamente cada $|\omega_i|_\ell \leq 1$ y, por desigualdad ultramétrica, $h(t) \in \mathbb{Z}_\ell[t]$.

Cambiando $f(t)$ por $f(t)^{-1}$, vemos que $g(t) \in \mathbb{Z}_\ell[t]$ también. □

Proposición 3.13: La función $Z(X,t) = P(t)/Q(t)$, donde $P, Q \in \mathbb{Z}[t]$.

Demostración: Aplicamos el lema anterior sobre todas las cohomologías ℓ-ádicas (incluyendo $\ell = p$) y así obtenemos que P, Q tienen coeficientes en cada $\mathbb{Z}_\ell$, por tanto, necesariamente sobre $\mathbb{Z}$. □

Teorema 3.14 (ecuación funcional, CW2): Sea X una variedad geométricamente íntegra, proyectiva, suave sobre un cuerpo finito $k = \mathbb{F}_q$. Se satisface la ecuación funcional (4).

Demostración: Por dualidad de Poincaré, tenemos el emparejamiento

$$H^{2d-r}(X) \times H^r(X) \xrightarrow{\smile} H^{2d}(X) \xrightarrow[\sim]{\int_X} F.$$

Y, por definición,

$$\int_X \mathrm{Frob}_*(x) \smile y = \int_X x \smile \mathrm{Frob}^*(y), \qquad x \in H^{2d-r}(X), y \in H^r(X).$$

Así pues, los valores propios de $\mathrm{Frob}^*|_{H^r}$ son los mismos que los de $\mathrm{Frob}_*|_{H^{2d-r}}$. Pero $\mathrm{Frob}^* = q^d/\mathrm{Frob}_*$, por lo que si $\alpha_1, \ldots, \alpha_s$ son los valores propios de $\mathrm{Frob}^*|_{H^r}$, entonces $q^d/\alpha_1, \ldots, q^d/\alpha_s$ son los valores propios de $\mathrm{Frob}^*|_{H^{2d-r}}$. De esto se deduce el enunciado. □

4. La cohomología étale

> De toda la obra de Grothendieck, la cohomología étale es sin lugar a dudas aquella que mayor influencia ha tenido en la geometría aritmética en los últimos cincuenta años.[6]
>
> –Luc Illusie

Definición 4.1: Un morfismo $f\colon X \to Y$ localmente de tipo finito se dice ***no ramificado*** en un punto $x \in X$ si $\mathscr{O}_{X,x}/\mathfrak{m}_{Y,y}\mathscr{O}_{X,x}$ es una extensión separable de $\Bbbk(y)$, donde $y := f(x)$. Se dice que f es un morfismo ***étale*** en un punto $x \in X$ si es plano y no ramificado en x. Se dice que f es ***no ramificado*** (resp. étale) si es no ramificado (resp. étale) en todo punto de X.

Proposición 4.2: Se cumplen:

1. Todo encaje cerrado de esquemas localmente noetherianos es no ramificado.
2. Todo encaje abierto de esquemas localmente noetherianos es étale.
3. Los morfismos no ramificados (reps. étale) son estables salvo composición, cambio de base y productos fibrados.

Demostración: Cfr. Liu [**5,** pág. 140], prop. 4.3.22. □

Proposición 4.3: Sean $f\colon X \to Y, g\colon Y \to Z$ morfismos tales que $g \circ f$ es no ramificado (resp. étale) y g es separado localmente de tipo finito (resp. no ramificado), entonces f es no ramificado (resp. étale).

[6] *De toute l'oeuvre de Grothendieck, c'est sans doute la cohomologie étale qui aura exercé l'influence la plus profonde sur l'évolution de la géométrie arithmétique dans les cinquante dernières années.*

Demostración: Cfr. [**5,** pág. 103], lemma 3.3.15 y Milne [**12,** pág. 24], cor. I.3.6. □

La siguiente noción la hemos empleado antes ya, pero conviene tener una definición clara:

Definición 4.4: Sea $f\colon X \to Y$ un morfismo de tipo finito entre esquemas localmente noetherianos. Se dice que f es ***suave*** en un punto $x \in X$ si es plano en x y si la fibra $X_y \to \operatorname{Spec} \Bbbk(y)$ es suave[7] en x, con $y := f(x)$. Se dice que f es ***suave de dimensión relativa*** n si es suave en todo punto (luego es un morfismo plano) y la dimensión de alguna fibra (en consecuente, de todas) es n.

Proposición 4.5: Un morfismo de tipo finito entre esquemas localmente noetherianos es étale syss es suave de dimensión relativa 0.

Demostración: Cfr. [**5,** pág. 142]. □

§4.1 La geometría de los morfismos étale. Ahora incluyo un par de resultados folclóricos para enfatizar el carácter geométrico de los morfismos étale y desmitificar su rol cohomológico. En primer lugar:

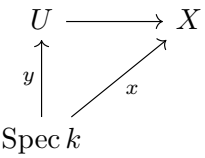
Teorema 4.6: Sea k un cuerpo. Un morfismo $X \to \operatorname{Spec} k$ de tipo finito es étale syss X es un esquema afín artiniano cuyas secciones globales $\Gamma(X, \mathscr{O}_X) \cong \prod_{i=1}^{n} K_i$ son un producto de extensiones de cuerpos K_i/k separables y finitas.

Demostración: Todo esquema es plano sobre un cuerpo, de modo que un morfismo es étale syss es no ramificado. Así aplicamos la equivalencia de la prop. I.3.2(e) de Milne [**12,** pág. 21]. □

Las siguientes definiciones son divertidas:

Definición 4.7: Sea X un esquema. Un ***punto geométrico*** de X es un punto k-valuado (i.e., un morfismo $\operatorname{Spec} k \to X$), donde k es un cuerpo separablemente cerrado.

Se dice que $U \to X$ es un ***entorno étale*** de un punto k-valuado $x \in X(k)$ si $U \to X$ es un morfismo étale y se tiene el siguiente diagrama conmutativo:



[7] Un esquema $X \to \operatorname{Spec} k$ se dice *suave* en un punto $x \in X$ si para toda extensión de cuerpos K/k se cumple que X_K es regular en toda preimagen de x.

La razón del adjetivo *geométrico* se debe a que, si X es un esquema algebraico sobre un cuerpo base perfecto k (que suele ser el caso), un punto geométrico es un punto en el cambio de base $X_{k^{\mathrm{alg}}}$.

Lo «divertido» en la definición es que pareciera tratar a los morfismos étale como si fueran abiertos, cuando uno sabe que todo abierto es un esquema étale pero el recíproco es falso.

Proposición 4.8: Sea Z un S-esquema conexo, y sean $f_1, f_2 \colon Z \to X$ un par de S-morfismos hacia un S-esquema étale finito X. Si existe un punto geométrico $\overline{z} \colon \operatorname{Spec} \Omega \to Z$ tal que $f_1 \circ \overline{z} = f_2 \circ \overline{z}_2$, entonces $f_1 = f_2$.

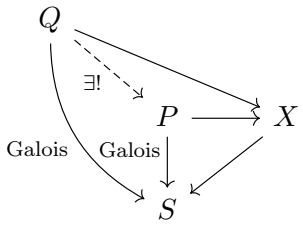
Demostración: Cfr. Szamuely [**31,** pág. 160], cor. 5.3.3. □

En consecuencia, vemos que ningún elemento de $\mathrm{Aut}_S(X)$, el grupo de S-automorfismos de X, no fija puntos geométricos.

Definición 4.9: Se dice que un morfismo $p \colon X \to S$ es un ***cubrimiento de Galois*** si X es conexo y p es un cubrimiento étale finito, tal que $\mathrm{Aut}_S(X)$ actúa transitivamente sobre las fibras geométricas.

Proposición 4.10: Sea $f \colon X \to S$ un cubrimiento étale finito conexo. Entonces existe un único X-esquema $\pi \colon P \to X$ tal que:

1. $f \circ \pi \colon P \to S$ es un cubrimiento de Galois.
2. Dado otro X-esquema $q \colon Q \to X$ tal que $f \circ q \colon Q \to S$ es un cubrimiento de Galois, entonces existe un único S-morfismo $Q \to P$ tal que el siguiente diagrama conmuta:



Demostración: Cfr. [**31,** pág. 163], prop. 5.3.9. □

La proposición anterior, debería considerarse un análogo algebraico de la clausura normal (nótese que el hecho de que X sea S-étale es un sustituto a la condición de ser una extensión separable), y un análogo geométrico del recubrimiento universal en topología algebraica.

Definición 4.11: Sea S un esquema conexo. Denotamos por $\mathscr{G}_S$ a la categoría cuyos objetos son cubrimientos de Galois $P \to S$ y cuyas flechas son S-morfismos entre ellos.

Lema 4.12: La categoría $\mathscr{G}_S$ es cofiltrada (i.e., es equivalente a la categoría opuesta de un conjunto ordenado dirigido).

Definición 4.13: Sea $(G, \cdot)$ un grupo, definimos su ***opuesto***, denotado G^{op}, al grupo cuyos elementos son los de G y cuyo producto $\odot$ está definido por $g \odot h := h \cdot g$.

Sea S un esquema conexo y sea $\overline{s}\colon \operatorname{Spec}\Omega \to S$ un punto geométrico. Se define su ***grupo fundamental algebraico*** basado en $\overline{s}$ como

$$\pi_1^{\mathrm{alg}}(S, \overline{s}) := \varprojlim_{P \in \mathscr{G}_S} \operatorname{Aut}_S(P)^{\mathrm{op}},$$

donde P recorre los entornos étale de $\overline{s}$ que son cubrimientos de Galois.

Así π_1^{alg} es un grupo profinito, y se relaciona con el grupo fundamental topológico π_1^{top} mediante:

Teorema 4.14: Sea X un esquema conexo algebraico sobre $\mathbb{C}$. El funtor de analitificación $(-)^{\mathrm{an}}\colon \mathsf{Sch}/\mathbb{C} \to \mathsf{Top}$ establece una equivalencia entre cubrimientos étale finitos de X y recubrimientos topológicos finitos de X^{an}. Más aún, para todo punto racional $\bar{x} \in X(\mathbb{C})$, tenemos un isomorfismo canónico

$$\widehat{\pi_1^{\mathrm{top}}(X^{\mathrm{an}}, x)} \xrightarrow{\ \sim\ } \pi_1^{\mathrm{alg}}(X, \bar{x}),$$

donde x denota la imagen de $\bar{x}$, y donde $\widehat{()}$ denota la completación profinita.

Demostración: Cfr. [**31,** pág. 184], thm. 5.7.4. □

§4.2 Haces sobre sitios *en una cáscara de nuez.* Cuando uno propone una generalización de un concepto matemático es importante tener en cuenta, ¿qué propiedad pretende obtener *a posteriori*? Por ejemplo, un espacio topológico generaliza un espacio métrico con el objetivo de tener también una noción de «función continua». Lo que Grothendieck y M. Artin querían era generalizar la noción de *haz*, para lo cual desarrollaron una generalización de una «topología»:

Definición 4.15 (M. Artin): Sea $\mathscr{C}$ una categoría pequeña con productos fibrados. Fijado un objeto $U \in \operatorname{Obj}\mathscr{C}$ y dado un par de conjuntos $\mathcal{S}_1 := \{U_i\}_{i\in I}, \mathcal{S}_2 := \{V_j\}_{j\in J}$ de objetos de $\mathscr{C}/U$, se dice que $\mathcal{S}_2$ es un ***refinamiento*** de $\mathcal{S}_1$ si para todo $i \in I$ existe un $j \in J$ y una flecha $U_i \to V_j$ (de $\mathscr{C}/U$).

Se le llama una ***(pre)topología de Grothendieck*** a una familia $J := \{\mathrm{Cov}_U\}_{U\in\operatorname{Obj}\mathscr{C}}$, tal que para cada objeto $U \in \operatorname{Obj}\mathscr{C}$, se cumple que Cov_U es una familia de conjuntos de flechas, llamados ***cubrimientos*** que satisface lo siguiente:

COV1. Para todo isomorfismo $V \to U$ se cumple que $\{V \to U\}$ es un cubrimiento.
COV2. El refinamiento de un cubrimiento es también un cubrimiento.
COV3. El cambio de base de un cubrimiento induce un cubrimiento. Vale decir, dado un cubrimiento $\mathcal{S} := \{U_i \to U\}_{i\in I} \in \mathrm{Cov}_U$ y una flecha $V \to U$, la familia $\mathcal{S} \times_U V := \{U_i \times_U V \to V\}_{i\in I} \in \mathrm{Cov}_V$.
COV4. Sea $\mathcal{S}_1 := \{U_i \to U\}_{i\in I} \in \mathrm{Cov}_U$ y $\mathcal{S}_2 := \{V_j \to U\}_{j\in J}$ una familia de flechas. Si para cada U_i se cumple que $\mathcal{S}_2 \times_U U_i \in \mathrm{Cov}_{U_i}$, entonces $\mathcal{S}_2 \in \mathrm{Cov}_U$.

Un ***sitio*** es un par $X := (\mathscr{C}, J)$, donde J es una (pre)topología de Grothendieck sobre $\mathscr{C}$. Denotamos $\mathrm{Cat}(X) := \mathscr{C}$.

La definición de una topología de Grothendieck es otra (cfr. KASHIWARA y SCHAPIRA **[28],** §16.1), pero uno puede probar que una pretopología induce de manera única una topología.

Ejemplo: Sea X un espacio topológico. Definimos el *sitio topológico* X_{top} como el sitio con $\mathrm{Cat}(X_{\mathrm{top}}) := \mathsf{Op}(X)$, la categoría de abiertos con inclusiones por flechas, y donde los cubrimientos coinciden con la definición topológica de «cubrimiento».

Definición 4.16: Un ***prehaz*** sobre un sitio X a valores en una categoría completa $\mathscr{D}$ no es más que un funtor $F\colon \mathrm{Cat}(X)^{\mathrm{op}} \to \mathscr{D}$. Se dice que F es un ***haz*** si para todo cubrimiento $\{U_i \xrightarrow{u_i} A\}_{i\in I}$ se cumple que el siguiente diagrama representa un ecualizador:

$$FA \xrightarrow{\prod_{i\in I} F(u_i)} \prod_{i\in I} FU_i \rightrightarrows \prod_{j,k} F(U_j \times_A U_k).$$

Sea X un espacio topológico. Un haz sobre el sitio topológico X_{top} es lo mismo que un haz (en sentido usual) sobre X.

Recuérdese que, como el funtor de secciones globales $\Gamma(X, -)$ es exacto por la izquierda y la categoría de haces abelianos $\mathsf{Sh}(X, \mathsf{Ab})$ tenía suficientes inyectivos, entonces concluíamos que existe (abstractamente) los grupos $H^p(X, -)$ de cohomología de haces. Ambas proposiciones son ciertas cambiando el esquema X por un sitio S, de modo que $H^p(S, -)$ también designará los grupos de cohomología, pero nuevamente construidos de forma abstracta.

Una manera más concreta es mediante la *cohomología de Čech*. No obstante, al igual que en el caso usual, hay que tener cuidado con que uno debe poner condiciones al esquema base para que el cálculo sea eficaz. La ventaja es que, el 0-ésimo grupo de cohomología de Čech es, de hecho, las secciones globales de la *hazificación* de un prehaz $\mathscr{F}$, así que conceptualmente mata dos pájaros de un tiro.

Definición 4.17: Sea $\mathcal{P}$ una propiedad de flechas en una categoría con coproductos $\mathscr{C}$ (e.g., «ser un morfismo de tipo finito» en la categoría de esquemas). Se dice que una familia $\{X_i \to Y\}_{i\in I}$ posee ***colectivamente*** $\mathcal{P}$ si la flecha $\coprod_{i\in I} X_i \to Y$ posee $\mathcal{P}$.

Se dice que una familia de morfismos de esquemas $\mathcal{U} := \{f_i \colon U_i \to X\}_{i\in I}$ es un ***cubrimiento de Zariski*** si es colectivamente suprayectiva y cada morfismo es un encaje abierto. Se dice que $\mathcal{U}$ es un ***cubrimiento étale*** si es colectivamente suprayectiva y étale.

Se dice que $\mathcal{U}$ es un ***cubrimiento fpqc***[8] si cada morfismo es plano, es colectivamente suprayectiva y para cada abierto compacto $K \subseteq X$ se cumple que existen finitos abiertos compactos $K_{i_j} \subseteq U_{i_j}$ tales que

$$K = \bigcup_{j=1}^{n} f_{i_j}[K_{i_j}].$$

Finalmente, sea X un esquema. Se le llama el ***sitio (pequeño) de Zariski*** al sitio que tiene por categoría Op/X (los encajes abiertos con codiminio X) y cuyos cubrimientos son los cubrimientos de Zariski. Se le llama el ***sitio (pequeño) étale-finito*** al sitio que tiene por categoría FEt/X (los morfismos finitos étale con codiminio X) y cuyos cubrimientos son los cubrimientos étale-finitos.[9] El ***sitio grande de Zariski*** (resp. ***sitio grande étale***, ***sitio fpqc***) tiene por categoría Sch/X y cuyos cubrimientos son los de Zariski (resp. étale, fpqc).

Así, fijando un esquema X y una topología $\tau \in \{\text{fpqc}, \text{ét}, \text{Zar}\}$, denotaremos $H^p_\tau(X, -)$ los grupos de cohomología sobre el sitio grande $(\mathsf{Sch}/X)_\tau$. La cohomología de haces usual es $H^p_{\text{Zar}}(X, -)$ y es de hecho un ejercicio estándar de un curso de geometría algebraica probar que coincide con $H^p(X_{\text{top}}, -)$ (cfr. HARTSHORNE [**3,** pág. 208], prop. III.2.6).

Una ventaja de trabajar con los sitios grandes es que en muchas situaciones nos encontramos con funtores $(\mathsf{Sch}/X)^{\text{op}} \to \mathscr{D}$, donde $\mathscr{D}$ es una categoría cualquiera (usualmente $\mathsf{Set}, \mathsf{Gr}, \mathsf{Ab}$) y la noción de *haz en la topología* τ puede ser útil.

La relación entre las tres topologías viene dada por:

Proposición 4.18: Se cumplen:

1. Todo cubrimiento por abiertos de Zariski es un cubrimiento étale-finito.
2. Todo cubrimiento étale es un cubrimiento fpqc.

Siguiendo un lenguaje clásico diríamos que la topología étale-finita es más *fina* o *fuerte* que la topología de Zariski. Como consecuencia, todo funtor

[8] Abrev. del fr. *fidèlement plat et quasi-compact*.

[9] Ojo, no decimos que los cubrimientos tengan finitos términos, sino que los *morfismos* son finitos.

$(\mathsf{Sch}/X)^{\mathrm{op}} \to \mathscr{C}$ que es un haz en la topología fpqc, es un haz en la topología étale y Zariski. El siguiente criterio es útil:

Proposición 4.19: Todo funtor $F\colon (\mathsf{Sch}/X)^{\mathrm{op}} \to \mathsf{Set}$ que es representable[10] es un haz en la topología fpqc.

Demostración: Cfr. **[Stacks],** Tag 023Q. □

Proposición 4.20: Sea $\mathscr{F}$ un haz cuasicoherente sobre un esquema X. Entonces el prehaz

$$\mathscr{F}^a(T \xrightarrow{f} X) := \Gamma(T, f^*\mathscr{F})$$

es un haz en la topología fpqc.

Demostración: Cfr. **[Stacks],** Tag 030G. □

Teorema 4.21: Sea $\mathscr{F}$ un haz cuasicoherente sobre un esquema X. Para toda topología $\tau \in \{\text{fpqc}, \text{ét}, \text{Zar}\}$ se cumple que

$$H^p(X, \mathscr{F}) \cong H^p_\tau(X, \mathscr{F}^a)$$

para todo $p \geq 0$. Donde el lado izquierdo designa la cohomología de haces usual y el lado derecho designa la cohomología de haces en el sitio $(\mathsf{Sch}/X)_\tau$.

Sea S un esquema base y τ una topología de Grothendieck. Tome el funtor $\mathscr{O}^\times_\tau(T \xrightarrow{f} S) := \Gamma(T, \mathscr{O}_T)^\times$. En la teoría de esquemas en grupos[11] que el funtor está representado por el esquema $\mathbb{G}_{m,S} := \mathrm{Spec}(\mathbb{Z}[t, t^{-1}]) \times_{\mathbb{Z}} S$, por lo que uno a veces denota por «$\mathbb{G}_m$» al haz. Así, $\mathbb{G}_m$ es un haz en la topología fpqc y:

Teorema 4.22 (de Hilbert 90): Para todo esquema S tenemos los siguientes isomorfismos canónicos:

$$H^1_{\text{ét}}(S, \mathbb{G}_m) \cong H^1_{\text{Zar}}(S, \mathbb{G}_m) \cong \mathrm{Pic}(S).$$

Definición 4.23: Sea X un esquema y G un grupo abeliano. Denotamos por $\underline{G}$ o $\underline{G}_S$ a la hazificación del prehaz $(\mathsf{FEt}/X)^{\mathrm{op}} \to \mathsf{Ab}$ constante $U \mapsto G$. Se dice un haz $\mathscr{F} \in \mathsf{Sh}(S, \mathsf{Ab})$ es ***localmente constante*** si existe un cubrimiento étale-finito $\{U_i \to X\}_i$ tal que $\mathscr{F}|_{U_i}$ es un haz constante (sobre el sitio étale pequeño $U_{\text{ét}}$). Se dice que $\mathscr{F}$ es además ***finito*** si para todo X-esquema étale finito U se cumple que $\mathscr{F}(U)$ es un grupo abeliano finito.

[10] Es decir que existe un X-esquema S tal que para todo X-esquema T, se cumple que $F(T) = S(T)$, donde aquí la igualdad designa una biyección de conjuntos que es natural en T.

[11] fr. *(pré)schémas en groupes*, eng. *group schemes*.

Definición 4.24: Sea X un esquema cuyo espacio topológico subyacente sea noetheriano (e.g., un esquema noetheriano).[12] Sea $\mathscr{F}$ un haz de grupos abelianos sobre el sitio étale $X_{\text{ét}}$. Se dice que $\mathscr{F}$ es ***constructible*** si existe una partición $X = \coprod_i X_i$, donde cada X_i es un subesquema localmente cerrado (i.e., un subesquema cerrado de un subesquema abierto) tal que cada $\mathscr{F}|_{X_i}$ es localmente constante finito.

Teorema 4.25: Sea X una variedad suave sobre $\mathbb{C}$. Para todo grupo abeliano finito G existen isomorfismos canónicos

$$H^i_{\text{sing}}(X^{\text{an}}; G) \cong H^i_{\text{ét}}(X, \underline{G}),$$

donde X^{an} denota la *analitificación*, es decir, al X visto con la topología de variedad analítica sobre $\mathbb{C}$, y el lado izquierdo representa cohomología singular a coeficientes en G.

Demostración: Cfr. Milne [**12,** pág. 117], thm. III.3.12. □

Cabe destacar que, si G no fuese finito, en particular, si fuese $\mathbb{Z}$, entonces el cálculo falla en general. Esto también demuestra que efectivamente la cohomología étale «tiene más abiertos», ya que $\underline{G}$ en la topología de Zariski es un haz flácido y, por tanto, no posee cohomología superior (cfr. Hartshorne [**3,** pág. 208], prop. III.2.5).

Al igual que en el caso clásico, si tenemos un morfismo $g\colon X \to Y$ entonces determina una aplicación a nivel de los sitios étale dado por el cambio de base:

$$\begin{array}{ccc} V_X & \longrightarrow & V \\ {\scriptstyle \text{étale finito}}\downarrow & \Leftarrow g_{\text{ét}} = & \downarrow{\scriptstyle \text{étale finito}} \\ X & \xrightarrow[g]{} & Y \end{array}$$

Así, dado un haz $\mathscr{F}$ sobre $X_{\text{ét}}$ podemos definir el ***haz imagen directa*** sobre $Y_{\text{ét}}$ por:

$$\Gamma(V, g_*\mathscr{F}) := \Gamma(V_X, \mathscr{F}).$$

Ahora bien, las categorías de haces abelianos sobre un sitio étale forman una categoría de Grothendieck (cfr. Kashiwara y Schapira [**28,** pág. 437], thm. 18.1.6(v)), y es fácil verificar que g_* preserva límites inversos puesto que es exacto por la izquierda ([**28,** pág. 82], prop. 3.3.3), por lo que prop. 8.3.27(iii) de [**28,** pág. 186] dice que admite una adjunta por la izquierda denotada g^*.

Para evitar confusión, desde ahora f_* siempre denotará el *pull-back* y f^* siempre denotará el *push-forward* sobre haces en la topología étale, nunca en la de Zariski.

Se destacan los siguientes resultados:

[12] Ésta condición atípica está para evitar la definición real de «conjunto constructible».

Teorema 4.26 (cambio de base propio): Sea $\pi\colon X \to Y$ un morfismo propio y sea $\mathscr{G}$ un haz sobre $Y_{\text{ét}}$. Se cumplen las siguientes:

1. Si $\mathscr{G}$ es constructible, entonces $\mathsf{R}^q\,\pi_*\mathscr{G}$ es constructible sobre X para cada $q \geq 0$.
2. Si $\mathscr{F}$ es un haz de pura torsión[13] sobre $X_{\text{ét}}$ y $g\colon Z \to Y$ es otro morfismo de esquemas (ver diagrama (6)), entonces el homomorfismo canónico
$$g^*(\mathsf{R}^q\,\pi_*\mathscr{F}) \xrightarrow{\ \sim\ } \mathsf{R}^q(\pi_Z)_*(g_X^*\mathscr{F})$$
de cambio de base es un isomorfismo para todo $q \geq 0$.

Demostración: Cfr. [**12,** págs. 223-224], thm. VI.2.1 y cor. VI.2.3. □

El diagrama de la situación del inciso 2 viene dada en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} X_Z = Z_X & \xrightarrow{g_X} & X \\ {\scriptstyle \pi_Z}\downarrow & \ulcorner & \downarrow{\scriptstyle \pi} \\ Z & \xrightarrow[g]{} & Y \end{array} \tag{6}$$

Y la fórmula involucrada debería considerarse un análogo de la «fórmula de proyección».

Definición 4.27: Sea Y un esquema. Llamamos su ***característica*** al conjunto $\operatorname{car} Y := \{\operatorname{car} \Bbbk(y) : y \in Y\}$.

Teorema 4.28 (cambio de base suave): Sea $\pi\colon X \to Y$ un morfismo compacto y $g\colon Z \to Y$ un morfismo suave. Dado un haz $\mathscr{F}$ de pura torsión en $X_{\text{ét}}$ con torsión coprima a $\operatorname{car} Y$. Entonces el homomorfismo canónico $g^*(\mathsf{R}^q\,\pi_*\mathscr{F}) \xrightarrow{\sim} \mathsf{R}^q(\pi_Z)_*(g_X^*\mathscr{F})$ de cambio de base es un isomorfismo para todo $q \geq 0$.

§4.3 La cohomología ℓ-ádica. Primero demos una descripción breve de la situación: en general, la cohomología étale puede «comportarse mal» con haces étale (de grupos abelianos) que no sean de pura torsión; así que una buena alternativa es mirar una sucesión de haces, similar a cuando uno presenta un grupo profinito como límite inverso de grupos finitos. No obstante, éste proceso también tiene consecuencias «desastrosas» si no se tiene el cuidado de que la torsión no coincida con la característica del cuerpo; de modo que si tenemos un esquema sobre un cuerpo de característica p, la cohomología ℓ-ádica resulta de mirar haces con torsión ℓ^n donde ℓ es un primo distinto de p.

Lo anterior se ejemplifica en el siguiente teorema:

[13]Las expresiones «haz de pura torsión» y «de torsión coprima a p» significan que $\mathscr{F}(U)$ es de pura torsión, o de torsión coprima a p para todo X-esquema compacto U.

Teorema 4.29: Sea k un cuerpo algebraicamente cerrado, sea X un esquema algebraico separado sobre k de dimensión ≤ 1, sea A un anillo noetheriao y sea $\mathscr{F}$ un haz constructible de A-módulos sobre $X_{\text{ét}}$ que es de pura torsión. Entonces $H^q_{\text{ét}}(X, \mathscr{F})$ es un A-módulo finitamente generado si $\mathscr{F}$ es de torsión coprima a $\operatorname{car} k$.

Demostración: Cfr. [**Stacks**], Tag 0GJJ. □

Son ésta clase de suposiciones las razones de hablar de cohomología ℓ-ádica en lugar de p-ádica.

Definición 4.30: Un ***haz (étale) ℓ-ádico*** es un sistema inverso $\mathscr{F} := (\mathscr{F}_n)_{n\in\mathbb{N}}$ de haces sobre $X_{\text{ét}}$ tales que el homomorfismo de haces $\mathscr{F}_{n+1} \to \mathscr{F}_n$ es isomorfo al homomorfismo $\mathscr{F}_{n+1} \to \mathscr{F}_{n+1} \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^n\mathbb{Z}$, o equivalentemente, tales que se induce un isomorfismo $\mathscr{F}_{n+1}/\ell^n\mathscr{F}_{n+1} \xrightarrow{\sim} \mathscr{F}_n$. Se dice que $\mathscr{F}$ es ***constructible*** (resp. ***localmente libre de rango finito*** r) si cada $\mathscr{F}_n$ lo es. Dado un haz ℓ-ádico $\mathscr{F}$, se define

$$H^q(X, \mathscr{F}) := \varprojlim_{n\in\mathbb{N}} H^q_{\text{ét}}(X, \mathscr{F}_n).$$

Corolario 4.31 (comparación de cohomologías ℓ-ádica y de Betti): Sea X una variedad suave sobre $\mathbb{C}$ y sea $\mathscr{F}$ un haz ℓ-ádico constante finito sobre X. Entonces para todo $q \geq 0$ tenemos los siguientes isomorfismos canónicos

$$H^q(X_{\text{ét}}, \mathscr{F}) \cong \varprojlim_{n} H^q_{\text{sing}}(X^{\text{an}}; \mathscr{F}_n) = H^q_{\text{sing}}(X^{\text{an}}; \mathscr{F}).$$

Más aún, basta que $\mathscr{F}$ sea constructible.

Lema 4.32: Sea X una variedad suave sobre un cuerpo k, y sea $\mathscr{F}$ un haz finito, localmente constante sobre X cuya torsión es coprima a $\operatorname{car} k$. Entonces $H^q_{\text{ét}}(X, \mathscr{F})$ es finito para todo $q \geq 0$.

Demostración: Cfr. [**12,** pág. 244], cor. VI.5.5. □

Definición 4.33: Sea k un cuerpo y sea $\ell \neq \operatorname{car} k$ un primo. La ***cohomología ℓ-ádica*** sobre PsVar_k es la cohomología dada por $H^*(-, \mathbb{Z}_\ell)$, donde $\mathbb{Z}_\ell := \left(\underline{\mathbb{Z}/\ell^n\mathbb{Z}}\right)_n$ es un haz ℓ-ádico.

Teorema 4.34 (Grothendieck, M. Artin, 1963; Deligne, 1980): La cohomología ℓ-ádica sobre un cuerpo algebraicamente cerrado de característica prima $p \neq \ell$ determina una teoría de cohomología de Weil.

Demostración: La finitud corresponde al lema anterior. La dualidad de Poincaré (cfr. **[12],** §VI.11), la fórmula de Künneth (cfr. **[12],** §VI.8), el mapa de ciclos (cfr. **[12,** págs. 243-244], cor. VI.5.3) y el teorema débil de Lefschetz (cfr. **[12],** §VI.7) fueron probados por Grothendieck y M. Artin. El teorema fuerte de Lefschetz fue probado por Deligne en **[10],** §4.1. □

5. Recuento histórico de las conjeturas de Weil

El siguiente recuento histórico está inspirado en el artículo de Milne **[26].**

En 1921, en la tesis de **Emil Artin [16]** (publ. 1924), él define el análogo de las funciones dseta de Dedekind para cuerpos globales de característica positiva. Técnicamente hablando lo hace empleando el concepto de *lugar*, que por un análogo del teorema de Ostrowski, se corresponden a los primos en un anillo de la forma $\mathbb{F}_p[t]$ o en la clausura entera de una extensión $K/\mathbb{F}_p[t]$ de tipo finito y de grado de trascendencia 1. Más específicamente, E. Artin trabajó con extensiones cuadráticas $K/\mathbb{F}_p[t]$ y, en estos casos, probó que la función $Z(K,s)$ aquí definida satisface la conjetura de racionalidad (CW1) y la ecuación funcional (CW2). Además, siguiendo los análogos para funciones L, también calculo el residuo del polo de $\zeta(K,s)$ en $s=1$. Artin no probó las hipótesis de Riemann en éste caso, aunque ciertamente formuló la conjetura apropiada.

Geométricamente, diríamos que Artin trató el caso de cónicas o de género 0, así que el siguiente caso lógico es el de curvas elípticas (género 1).[14] Éste fue desarrollado por **Edmund Hasse** en 1933 **[19]** y en su demostración hace un uso esencial del anillo de endomorfismos de la curva elíptica, de modo que su argumento no es generalizable. A diferencia de E. Artin, Hasse logra demostrar que las hipótesis de Riemann se satisfacen en éste caso. Cabe destacar que, si bien empleamos la terminología geométrica, la escuela alemana de teoría de números optaba por hablar de *cuerpos de funciones* e incluso el concepto geométrico del género estaba definido en ese lenguaje.

Finalmente, entre 1940 y 1941 el numerista francés **André Weil** anuncia la solución de las conjeturas de E. Artin para curvas de género arbitrario. Durante una visita de seis meses a Roma entre 1925 y 1926, Weil conoció a la escuela italiana de geometría algebraica, y en él tuvo gran influencia los trabajos de Francesco Severi y de Van der Waerden, especialmente enfocados en la teoría de intersección. El gran problema que retrasó a Weil fue notar que la teoría principalmente estaba desarrollada sobre $\mathbb{C}$ (incluyendo el teorema de Riemann-Roch), por lo que necesitó trabajar en los fundamentos de la geometría algebraica para obtener una teoría que funcionase sobre un cuerpo finito. En 1941 **[22]** y en 1948 **[24]** Weil otorgó dos pruebas distintas a las conjeturas de E. Artin, una usando teoría de intersección, y la otra empleando la variedad jacobiana de una curva. Esto sucedió durante la Segunda Guerra

[14]Técnicamente una curva elíptica es una curva proyectiva, suave de género 1 *con un punto racional*. En 1931, F.K. Schmidt demostró que toda curva proyectiva sobre un cuerpo finito posee puntos racionales.

Mundial, durante la cual Weil pasó un cierto tiempo encarcelado; al parecer, el cautiverio de Weil resultó tan fructífero que su amigo Hermann Weyl le propuso usar su influencia para volver a encarcelarlo.[15] En 1949 Weil formula las conjeturas que llevan su nombre, donde su trabajo pretende generalizarse a dimensión arbitraria.

Por aquel tiempo, Weil también habla con sus colegas de la heurística de emplear métodos de la topología algebraica para resolver las conjeturas; esto más adelante se vería reforzado por la correspondencia «GAGA» de Serre que señala que una cohomología (algebraica) de haces apropiada da los mismos cálculos que la homología singular (analítica) para variedades proyectivas suaves sobre $\mathbb{C}$; no obstante, esta cohomología no da suficiente información para variedades sobre cuerpos finitos. Señala Grothendieck [**25,** pág. 1066] al respecto:

> Nadie tenía entonces la menor idea de cómo definir tal cohomología, y no estoy seguro de que alguien además de Serre y yo, ni siquiera el mismo Weil, tuviera la íntima convicción de que eso debiera existir.

Tras la publicación de las hipótesis de Riemann para curvas varias aplicaciones se hicieron ver rápidamente, algunas que nosotros mismos exponemos en el presente artículo. En 1948, Weil [**23**] probó, basado en un artículo de 1935 de Davenport y Hasse, que todas las sumas exponenciales en una variable pueden escribirse como sumas de trazas de endomorfismos de Frobenius. En 1954, Serge Lang y Weil aplicaron las conjeturas de Weil para probar una cota sobre puntos racionales de variedades sobre cuerpos finitos (teo. 2.23). Es parte de las conjeturas de Weil generales el que estas cotas se satisfagan, así que es interesante el que estos resultados se hayan obtenido solo a partir del caso de las curvas.

Podría decirse que por los años siguientes, las conjeturas de Weil quedaron en «estado de hibernación». Algunos estudiantes (especialmente los de Weil y colegas) se encargaron de dar demostraciones alternativas a la hipótesis de Riemann para curvas. En 1956, un resultado de Zariski permitía extender la demostración de Riemann-Roch al caso de cuerpos finitos, dando implícitamente otra prueba a las hipótesis de Riemann para curvas. En privado, **Alexander Grothendieck** y **Jean-Pierre Serre** hablaban bastante de las conjeturas de Weil en su correspondencia. Ambos, habían demostrado su talento para trabajar con teorías cohomologías; y, tal y como muestra la cita previa, ambos confiaban en desarrollar una teoría que respondiese a la heurística de Weil. Resultó una sorpresa para ellos (y para muchos otros) cuando en 1959, Bernard Dwork logró probar la racionalidad (CW1) de las funciones dseta para variedades arbitrarias sobre cuerpos finitos empleando métodos p-ádicos; lo sorpresivo no era que no solo prescindía de una teoría de cohomología, sino que también optaba por un camino más analítico que geométrico.

[15] Kratz, S. G. *Mathematical Apocrypha Redux. More Stories and Anecdotes of Mathematicians and the Mathematical* (Mathematical Association of America, 2005), pág. 20.

No obstante, los métodos de Grothendieck comenzaron a dar frutos. Desde 1960, Grothendieck comenzaría a llevar a cabo los famosos Seminarios de Geometría Algebraica del Bosque Marie (SGA), y en la cuarta entrega publicada en 1964 sus estudiantes y él atacan el problema de la cohomología étale, y en la quinta entrega se dedican de lleno a la cohomología ℓ-ádica y las funciones L. Las principales líneas de investigación que llevaron a demostrar la racionalidad, la ecuación funcional (CW2) y los números de Betti (CW4) fueron logradas por Grothendieck junto a su alumno **Michael Artin**, hijo de E. Artin.

Así, solo una de las conjeturas de Weil se resistía, la hipótesis de Riemann (CW3). Hacia 1968, Grothendieck había trabajado principalmente en encontrar la reformulación apropiada para atacar éste problema; él mismo explica [**25,** pág. 56]:

> [H]abía extraído una versión más fuerte, y sobre todo más «geométrica», de las conjeturas de Weil. [...] Mi reformulación consistió, esencialmente, en desentrañar una especie de «quintaesencia» de lo que debía seguir siendo válido, en el cuadro de las variedades algebraicas llamadas «abstractas», de la clásica «teoría de Hodge», válida en las variedades algebraicas «ordinarias» [complejas]. Llamé «conjeturas estándar» (sobre los ciclos algebraicos) a esa nueva versión, totalmente geométrica, de las famosas conjeturas.

Grothendieck se habría inspirado en un artículo de Serre sobre los análogos kählerianos de las conjeturas de Weil. Durante un tiempo, las conjeturas estándar se propagaron sin estar explícitamente publicadas en el círculo de Grothendieck; años más tarde, finalmente las haría públicas y explicaría que, junto a la resolución de singularidades (o programa minimal de Mori), las conjeturas estándar corresponderían a uno de los problemas centrales para la geometría algebraica.

Entre los muchos estudiantes de Grothendieck, **Pierre Deligne** probó ser uno de los más talentosos («el más brillante de mis alumnos "cohomólogos"», señala [**25,** pág. 55]). Hacia 1970, diversas circunstancias desembocaron en la salida de Grothendieck de la escena matemática. Tres años más tarde, Grothendieck habría escuchado que Deligne había demostrado finalmente las hipótesis de Riemann (en [**9**]), lo que confesa que no le produjo sorpresa; lo que sí le sorprendió fue saber que sus conjeturas estándar seguían abiertas.

La demostración de Deligne estaba basada en técnicas aritméticas de funciones L y grupos de monodromía. En una entrevista, confiesa:[16]

> Gowers. [...] Ciertamente, [...] hubo una serie natural de pasos que eventualmente te llevaron a esta maravillosa demostración.
>
> Deligne. Sí, pero para poder divisar esos pasos, fue crucial que no sólo siguiera los cursos de geometría algebraica, sino también otras cosas que parecían bastante distintas como la teoría de formas automorfas (se verán menos distintas ahora). Era la discrepancia entre lo

[16] Milne, J. S. *Lectures on étale cohomology (v2.21)* `https://www.jmilne.org/math/CourseNotes/lec.html` (22 de mar. de 2013), pág. 200.

que uno podía hacer en ambas disciplinas lo que llevo al qué debía hacerse.

GOWERS. ¿Fue mera casualidad que estuvieses instruido en ambas?

DELIGNE. Sí.[17]

Años más tarde, Deligne dio una segunda demostración en términos de *haces perversos* (en **[10]**), y le siguieron otras demostraciones mediante el uso de transformaciones de Fourier ℓ-ádicas (Laumon), y cohomología rígida (Kedlaya). Algunas de las consecuencias de las conjeturas de Weil incluyen el teorema fuerte de Lefschetz (TC6), una conjetura de Ramanujan-Petersson y las conjeturas estándar de tipo Künneth (C) sobre cuerpos finitos.

6. Las conjeturas de Tate y algunos casos

Para esta sección seguimos la exposición de TATE **[15].**

Sea k un cuerpo de tipo finito sobre su cuerpo primo y fijemos $\ell \neq \operatorname{car} k$ primo. Entonces la cohomología ℓ-ádica es una teoría de cohomología de Weil, como hemos mencionado anteriormente, y denotaremos

$$H^i(X) := H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell), \qquad \overline{X} := X_{k^{\text{sep}}},$$

donde X es una variedad (geométricamente íntegra) sobre k, $\mathbb{Q}_\ell$ en realidad denota el haz étale a valores constantes en $\mathbb{Q}_\ell$ y k^{sep} denota la clausura separable de k. Sea $\mathfrak{G} := \operatorname{Gal}(k^{\text{sep}}/k)$ el grupo de Galois absoluto, entonces nótese que $\mathfrak{G}$ actúa sobre $H^i(X)$ visto como $\mathbb{Q}_\ell$-espacio vectorial, y denotamos $W := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} (\varprojlim_n \mu_{\ell^n})$, donde μ_m designa el grupo de raíces m-ésimas de la unidad. El W funciona como «torcimiento» y denotamos $V(m) := V \otimes_{\mathbb{Q}_\ell} W^{\otimes m}$, donde

$$W^{\otimes m} := (W^{\otimes |m|})^\vee = \operatorname{Hom}_{\mathbb{Q}_\ell}(W^{\otimes m}, \mathbb{Q}_\ell), \qquad m < 0.$$

Así, definimos $V^j(X) := H^{2j}(X)(j)$. Nótese que, como $\mathbb{Q}_\ell$-espacio vectorial, da igual torcer por W o no, pero esto dota al grupo de cohomología ℓ-ádica con una acción de Galois; estableciendo vínculos con la cohomología de Galois.

Finalmente la conjetura de Tate sobre ciclos algebraicos es:

Conjetura 6.1 (de Tate $T^i_k(X)$): El mapa de ciclos $\gamma_X \colon \operatorname{CH}^i(X) \to V^i(X)^{\mathfrak{G}}$ satisface que $\operatorname{Img}(\gamma_X) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = V^i(X)$.

[17] *GOWERS: Certainly, [that conveys the idea that] there was a certain natural sequence of steps that eventually led to this amazing proof.*

DELIGNE: Yes, but in order to be able to see those steps it was crucial that I was not only following lectures in algebraic geometry but some things that looked quite different (it would be less different now) the theory of automorphic forms. It was the discrepancy in what one could do in the two areas that gave the solution to what had to be done.

GOWERS: Was that just a piece of good luck that you happened to know about both things.

DELIGNE: Yes.

Diremos que se satisface $T^i(X)$ si el enunciado anterior es cierto para el i y X especificados. Nos interesará particularmente el caso $i = 1$ (llamada ***conjetura de Tate para divisores***) donde se traduce a que todo elemento en cohomología ℓ-ádica $y \in H^2_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell)$ viene como suma formal a coeficientes en $\mathbb{Q}_\ell$ de divisores de Weil.

Proposición 6.2: Fijemos X una variedad geométricamente íntegra, proyectiva, suave sobre un cuerpo k de tipo finito sobre su cuerpo primo. Son equivalentes:

1. $T^1_{k^{\text{sep}}}(X_{k^{\text{sep}}})$.
2. $T^1_K(X_K)$ para toda extensión K/k suficientemente grande.

Demostración: Cfr. Tate **[14,** pág. 98]. □

Teorema 6.3: Sean X, Y esquemas proyectivos equidimensionales sobre k. Se cumplen:

1. $T^1(X) + T^1(Y) \iff T^1(X \times_k Y)$.
2. $T^1(X)$ es invariante birracionalmente.
3. Sea $X \to Y$ una k-aplicación racional dominante, entonces $T^1(Y) \implies T^1(X)$.

Demostración: Cfr. Tate **[15],** (5.2). □

Lema 6.4: Sea X una variedad proyectiva sobre un cuerpo k, y sea $\mathscr{E}$ un $\mathscr{O}_X$-módulo localmente libre[18] de rango r. Entonces el fibrado proyectivo $\mathbb{P}_X(\mathscr{E})$ es birracional a $\mathbb{P}^{r-1}_X$.

Recuérdese que el fibrado proyectivo está definido como

$$\mathbb{P}_X(\mathscr{E}) := \operatorname{Grass}_1(\mathscr{E}) \cong \operatorname{Proj}_X(\operatorname{Sym} \mathscr{E}^\vee).$$

La definición de los símbolos a la derecha, las puede encontrar en Görtz y Wedhorn **[2,** págs. 213-218], §8.8.

Demostración: Basta notar que, por definición, existe un abierto (denso) U tal que $\mathscr{E}|_U \simeq \mathscr{O}^r_U$, luego

$$\mathbb{P}_X(\mathscr{E}) \times_X U = \mathbb{P}_U(\mathscr{E}|_U) \cong \mathbb{P}_U(\mathscr{O}^r_U|_U) \cong \mathbb{P}^{r-1}_U.$$

Así que son isomorfos en un abierto denso, luego birracionales. □

Corolario 6.5: Sea X una variedad proyectiva sobre un cuerpo k y sea $\mathscr{E}$ un $\mathscr{O}_X$-módulo localmente libre. Entonces se satisface $T^1(X)$ syss se satisface $T^1\big(\mathbb{P}_X(\mathscr{E})\big)$.

[18]Cuando digamos *$\mathscr{O}_X$-módulo localmente libre* siempre supondremos rango constante finito.

Veamos casos donde la conjetura de Tate es cierta:

1. Para curvas proyectivas: en efecto, $\dim_{\mathbb{Q}_\ell} H^2(X) = 1$ por dualidad de Poincaré y el mapa de ciclos es no trivial.
2. Para espacios proyectivos y, por tanto, para variedades unirracionales:[19] esto se debe a que $\mathrm{CH}^1(\mathbb{P}^n) = \mathrm{Pic}(\mathbb{P}^n) \cong \mathbb{Z}$, ya que está generado por un hiperplano. Empleando el teorema débil de Lefschetz (TC5) y un argumento inductivo, obtenemos que $V^1(\mathbb{P}^n) = H^2(\mathbb{P}^n, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$.
3. Para variedades abelianas sobre cuerpos numéricos: esto es un teorema profundo de Faltings y fue parte importante de su demostración de la conjetura de Mordell (cfr. [**18**]).

Proposición 6.6: Sea X una variedad geométricamente irreducible, completa, suave y racionalmente conexa[20] (e.g., Fano) sobre un cuerpo numérico k. Entonces se satisface $T^1(X)$.

Demostración: Como $\operatorname{car} k = 0$, entonces racionalmente conexa equivale a *separablemente* racionalmente conexa (cfr. Kollár [**4,** pág. 200], prop. IV.3.3.1) y, por tanto, $H^0(X, \Omega^m_{X/k}) = 0$ para todo $m > 0$ (cfr. [**4,** pág. 202], cor. IV.3.8). Así, pues por la comparación de cohomologías ℓ-ádica y de Betti tenemos que

$$H^2_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell) \cong H^2_{\text{sing}}(X^{\text{an}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong H^{1,1}(X) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell,$$

donde el último isomorfismo viene de la descomposición de Hodge (cfr. Voisin [**7,** pág. 142]). Así, basta probar que el homomorfismo de clases de Chern $\operatorname{Pic} X \to H^{1,1}(X^{\text{an}})$ es suprayectivo, y esto es precisamente el teorema de Lefschetz para clases $(1,1)$ (cfr. [**7,** pág. 280]).

El que las variedades Fano geométricamente íntegras sean racionalmente conexas, se sigue de que, al hacer cambio de base, la variedad $X_{k^{\text{alg}}}$ es racionalmente conexa en cadenas[21] (cfr. [**4,** pág. 254], thm. V.2.13) y por tanto es racionalmente conexa (cfr. [**4,** pág. 204], thm. IV.3.10). □

Comentario: Uno podría notar que en la demostración solo se emplea que la irregularidad $h^{0,j}(X) = 0$ para todo j y que, por tanto, el enunciado general sería para esta clase de variedades. No obstante, una conjetura folclórica de Mumford (cfr. [**4,** pág. 202], conj. IV.3.8.1) dice que esto es *equivalente* a ser racionalmente conexa en característica 0; Miyaoka comprobó esto para dimensión ≤ 3.

Ahora veamos casos particulares, gracias a una clasificación de Campana y Peternell [**8**]**:**

---

[19] Siguiendo a Kollár [**4,** pág. 199], decimos que una variedad X es *unirracional* si existe una k-aplicación racional dominante $\mathbb{P}^n_k \dashrightarrow X$. El mismo Kollár advierte que hay autores que emplean la palabra *unirracional* para «geométricamente unirracional».

[20] eng. *rationnally connected*.

[21] eng. *rationally chain connected*.

Teorema 6.7: La conjetura de Tate T^1 es válida para variedades geométricamente írreducibles, proyectivas, suaves de dimensión ≤ 3 con tangente nef sobre un cuerpo numérico k.

Demostración: Sea X una variedad como está descrita en el enunciado. Para poder usar la clasificación de variedades, nos gustaría hacer cambio de base a X sobre $\mathbb{Q}^{\text{alg}}$, pero en realidad, basta pasar a una extensión K/k suficientemente grande. Si X es una curva, entonces está listo por el ejemplo 1. Si $X_{K^{\text{alg}}}$ es una superficie, entonces es minimal (cfr. [**8,** pág. 176], thm. 3.1) y, por la clasificación de Kodaira-Enriques uno de los siguientes casos se cumple:

(a) X_K es una superficie abeliana: en cuyo caso se sigue del teorema de Faltings.
(b) X_K es una hiperelíptica, vale decir, es el cociente de producto de curvas elípticas: en cuyo caso, hay un morfismo suprayectivo $E_1 \times_K E_2 \to X$, luego basta verificar T^1 sobre el dominio, lo cual es cierto por ser un producto de curvas elípticas.
(c) $X_K \cong \mathbb{P}^2_K$: esto es el ejemplo 2.
(d) $X_K \cong \mathbb{P}^1_K \times_k \mathbb{P}^1_K$: esto es el ejemplo 2 junto con que Tate vale en un producto syss lo hace en factores.
(e) $X_K \cong \mathbb{P}_C(\mathscr{E})$, donde C es una curva elíptica y $\mathscr{E}$ es localmente libre de rango 2: esto se sigue del corolario anterior, pues Tate es cierto sobre curvas.

Si X_K es una 3-variedad (eng. *three-fold*), entonces posee un cubrimiento étale $\widetilde{X}$ que pertenece a la siguiente lista (cfr. [**8,** pág. 185], thm. 10.1):

(a) y (b). X_K es Fano.
(c) $\widetilde{X} \cong \mathbb{P}(\mathscr{E})$, donde $\mathscr{E}$ es localmente libre sobre una curva elíptica.
(d) $\widetilde{X} \cong \mathbb{P}(\mathscr{F}) \times_E \mathbb{P}(\mathscr{G})$, donde $\mathscr{F}, \mathscr{G}$ son localmente libres sobre una curva elíptica E.
(e) $\widetilde{X} \cong \mathbb{P}(\mathscr{E})$, donde $\mathscr{E}$ es localmente libre sobre una superficie abeliana.
(f) $\widetilde{X}$ es una variedad abeliana.

Para probar que X_K satisface T^1, veremos que $T^1(\widetilde{X})$. Por la proposición anterior concluimos que se satisfacen los casos (a) y (b). Por el teorema de Faltings, también se satisface el caso (f) y, por el corolario 6.5, también los casos (c) y (e).

El caso (d) es el único que tratamos de manera aislada, para lo cual empleamos la proposición 7.2 de [**8,** pág. 181], la cual nos dice que existe un morfismo suprayectivo y no ramificado $f\colon \widetilde{E} \to E$, donde E es una curva elíptica, tal que $X \times_E \widetilde{E} \cong \widetilde{S}_1 \times_{\widetilde{E}} \widetilde{S}_2$ (como $\widetilde{E}$-esquemas), y donde cada $\varrho_i\colon \widetilde{S}_i \to \widetilde{E}$ es una superficie eliptica reglada. Nótese que por la fórmula de

Hurwitz (cfr. Liu [**5,** pág. 290], thm. 7.4.16) tenemos que

$$2p_a(\widetilde{E}) - 2 = (\deg f)(2p_a(E) - 2) + \sum_{x \in X_K^0} (e_x - 1)[\Bbbk(x) : K],$$

donde e_x es el índice de ramificación de cada $f_x^\sharp \colon \mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X_K,x}$. Como f es no ramificado, entonces $p_a(\widetilde{E}) = p_a(E) = 1$. Más aún f, debe ser un morfismo suave puesto que es plano (porque el codominio es una curva íntegra normal, y el dominio es íntegro, cfr. Görtz y Wedhorn [**2,** pág. 492], prop. 15.4) con fibras de dimensión pura 0, es de tipo finito y $\Omega^1_{\tilde{E}/E} \simeq 0$ (cfr. [**5,** pág. 221], cor. 6.2.3). Así, necesariamente $\widetilde{E}$ es una curva íntegra, proyectiva y suave de género 1, es decir, es una curva elíptica.

Finalmente, empleamos que toda superficie reglada $\varrho_i \colon \widetilde{S_i} \to \widetilde{E}$ es de la forma $\widetilde{S_i} \cong \mathbb{P}_{\tilde{E}}(\mathscr{F}_i)$ para algún $\mathscr{F}_i$ localmente libre de rango 2 (cfr. Hartshorne [**3,** pág. 370], prop. V.2.2) y, por tanto, hay abiertos $U_i \subseteq \widetilde{E}$ tales que $\mathbb{P}_{\tilde{E}}(\mathscr{F}_i) \times_{\tilde{E}} U_i \cong \mathbb{P}^1_K \times_K U_i$, así que tomando $V := U_1 \cap U_2$, vemos que

$$\mathbb{P}_{\tilde{E}}(\mathscr{F}_1) \times_{\tilde{E}} \mathbb{P}_{\tilde{E}}(\mathscr{F}_2) \times_{\tilde{E}} V \cong (\mathbb{P}^1_K \times_K U_1) \times_{\tilde{E}} (\mathbb{P}^1_K \times_K U_2) \cong \mathbb{P}^1_K \times_K \mathbb{P}^1_K \times_K V.$$

En síntesis, probamos que $\widetilde{X}$ (que es un recubrimiento étale de X_K) es birracional a $\mathbb{P}^1_K \times_K \mathbb{P}^1_K \times_K \widetilde{E}$, donde $\widetilde{E}$ es una curva elíptica, y aplicamos la invarianza birracional de T^1. □

Referencias

Para introducirse a la geometría algebraica recomendamos el texto de Liu [**5],** ya que es el que más énfasis pone en teoremas con generalidad suficiente para las aplicaciones a la teoría de números. Más específicamente recomendamos prestarle atención a los conceptos de: cambio de base y morfismos de Frobenius, morfismos planos/suaves/étale, cohomología de haces, los teoremas de Riemann-Roch y la fórmula de Hurwitz para curvas, y un poco de teoría de intersección en superficies. Con ello, se puede leer la exposición de las conjeturas de Weil para curvas en Hartshorne [**3**] y el apéndice en el mismo sirve como motivación para el caso general. Para una exposición rápida del tema, recomendamos los capítulos 6 y 7 de Poonen [**13],** y para los detalles sobre cohomología étale recomendamos el texto de Milne [**12].**

Las cosas que perdimos en el fuego. Desgraciada o afortunadamente para el lector, no podemos seguir escribiendo infinitamente, y es claro que en unas pocas páginas es imposible siquiera esbozar todos los tópicos de esta historia. Específicamente, cosas de las que (casi) no hablamos incluyen: henselizaciones (estrictas) de anillos, cohomología de Čech para topologías de Grothendieck,[22] relaciones entre la cohomología de Galois, el grupo de Brauer y la cohomología étale; el grupo fundamental algebraico, representaciones

[22]El cálculo de cohomología de Čech de Liu [**5**] (§5.2) pasa por el «teorema de aciclicidad de Leray». El enfoque moderno (cfr. Kashiwara y Schapira [**28**]) demuestra esto para sitios y tras ello la exposición debería ser más o menos análoga.

de Galois y funciones L de Artin para variedades sobre cuerpos finitos –especialmente las implicancias de las conjeturas de Weil sobre esto–. Otros temas perdidos son la nula mención de los torsores étale, los cuales han demostrado tener aplicaciones para el estudio de puntos racionales e inclusive enteros; y finalmente la omisión total de motivos en la exposición, los cuales esclarecen la relación entre las conjeturas de Weil y de Tate.

Geometría algebraica

Stacks. De Jong, A. J. *et al. Stacks project* `https://stacks.math.columbia.edu/`.

1. Fulton, W. *Intersection theory* (Springer-Verlag, 1998).
2. Görtz, U. y Wedhorn, T. *Algebraic Geometry I: Schemes. With Examples and Exercises* 2.ª ed. (Springer Spektrum Wiesbaden, 2010).
3. Hartshorne, R. *Algebraic Geometry Graduate Texts in Mathematics* **52** (Springer-Verlag New York, 1977).
4. Kollár, J. *Rational curves on algebraic varieties* (Springer-Verlag, 2001).
5. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).
6. Milne, J. S. *Jacobian Varieties* en *Arithmetic Geometry* (eds. Cornell, G. y Silverman, J. H.) (Springer-Verlag, 1986), 167-212.
7. Voisin, C. *Hodge theory and complex algebraic geometry I* (Cambridge University Press, 2003).

Las conjeturas de Weil y de Tate

8. Campana, F. y Peternell, T. Projective manifolds whose tangent bundles are numerically effective. *Math. Ann.* **289,** 169-187. doi:`10.1007/BF01446566` (1991).
9. Deligne, P. La conjecture de Weil I. *Publ. Math. I.H.É.S.* **43,** 273-307. `http://www.numdam.org/item/?id=PMIHES_1974__43__273_0` (1974).
10. Deligne, P. La conjecture de Weil II. *Publ. Math. I.H.É.S.* **52,** 137-252. `http://www.numdam.org/item/PMIHES_1980__52__137_0/` (1980).
11. Kleiman, S. L. *The Standard Conjectures* en *Motives* (eds. Jannsen, U., Kleiman, S. L. y Serre, J.-P.) (American Mathematical Society, 1994), 3-20.
12. Milne, J. S. *Étale Cohomology* (Princeton University Press, 1980).
13. Poonen, B. *Rational Points on Varieties* (American Mathematical Society, 2017).
14. Tate, J. *Algebraic cycles and poles of zeta functions* en *Arithmetical Algebraic Geometry* (ed. Schilling, O. F. G.) (Harper & Row, 1965), 93-110.
15. Tate, J. *Conjectures on Algebraic Cycles in ℓ-adic Cohomology* en *Motives* (eds. Jannsen, U., Kleiman, S. L. y Serre, J.-P.) (American Mathematical Society, 1994), 71-83.

Artículos históricos

16. Artin, E. Quadratische Körper im Gebiete der höheren Kongruenzen I. *Math. Z.* **19,** 153-206. doi:10.1007/BF01181074 (1924).
17. Bombieri, E. *Counting points on curves over finite fields (d'après S. A. Stepanov)* en *Seminaire Bourbaki. Vol 1972/73, Exposés 418-435* (ed. Bourbaki, N.) (Springer-Verlag Berlin Heidelberg, 1973). http://www.numdam.org/item/SB_1972-1973__15__234_0/.
18. Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. math.* **73,** 349-366. doi:10.1007/BF01388432 (1983).
19. Hasse, E. Beweis analogous der Riemannschen Vermutung für die Artinsche und F. K. Schmidtschen Kongruenz-zetafunktionen in gewisse elliptischen Fallen. *Nachr. Akad. Wiss. Göttingen,* 253-262. http://eudml.org/doc/59426 (1933).
20. Lang, S. y Weil, A. Number of points of varieties in finite fields. *Amer. J. Math.* **76,** 819-827. doi:10.2307/2372655 (1954).
21. Stepanov, S. A. The number of points of a hyperelliptic curve over a finite prime field. *Math. USSR Izv.* **33,** 1103-1114. doi:10.1070/IM1969v003n05ABEH000834 (1969).
22. Weil, A. On the Riemann Hypothesis in Function-Fields. *Proc. Nat. Acad. Sci. USA.* **27,** 345-347. doi:10.1073/pnas.27.7.345 (1941).
23. Weil, A. On some exponential sums. *Proc. Nat. Acad. Sci. USA.* **34,** 204-207. doi:10.1073/pnas.34.5.204 (1948).
24. Weil, A. *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent* (Hermann, 1948).

Historia

25. Grothendieck, A. *Cosechas y Siembras* trad. por Navarro, J. A. http://matematicas.unex.es/~navarro/res/ (1986).
26. Milne, J. S. *The Riemann Hypothesis over Finite Fields: From Weil to the Present Day* en *The Legacy of Bernhard Riemann After One Hundred And Fifty Years* (eds. Ji, L., Oort, F. y Yau, S.-T.) (International Press, 2016).

Otros recursos

27. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
28. Kashiwara, M. y Schapira, P. *Categories and Sheaves* (Springer-Verlag Berlin Heidelberg, 2006).
29. Matsumura, H. *Commutative Ring Theory* trad. por Reid, M. *Cambridge Studies in Advanced Mathematics* **8** (Cambridge University Press, 1986).
30. Rosen, M. *Number Theory in Function Fields* (Springer-Verlag, 2002).
31. Szamuely, T. *Galois groups and fundamental groups* (Cambridge University Press, 2009).

Correo electrónico: josecuevasbtos@uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
URL: josecuevas.xyz