VARIEDADES ABELIANAS, UNA INTRODUCCIÓN

MARC HINDRY, MARUSIA REBOLLEDO, DAVID ROBERTS

Resumen. Variedades abelianas son grupos algebraicos que, al mismo tiempo, son variedades algebraicas proyectivas. El primero ejemplo es dado por curvas elípticas que son las variedades abelianas de dimensión uno. Un ejemplo histórico y muy importante es la variedad jacobiana de una curva de género $\geqslant 2$. Este curso propone una breve introducción a la rica teoría de estos objetos, esbozando tres puntos de vista: complejo analítico (toros complejos, funciones theta, formas de Riemann), geométrico algebraico (teorema del cubo, grupo de Picard, isogenías) y aritmético (teorema de Mordell-Weil, teoría de Honda-Tate, modularidad).

Se puede encontrar referencias generales sobre variedades abelianas complejas en [2, 7, 11, 13], variedades abelianas y jacobianas sobre un cuerpo cualquier en [4, 7, 8, 9, 11, 12]. Para variedades abelianas con dimensión 1, es decir curvas elípticas en [6, 14, 15]. Se reunirán material más avanzado sobre variedades abelianas en [22, 25, 29, 30, 31], información computacional y base de datos sobre curvas elípticas y variedades abelianas de dimensión 2 en [16, 17, 19, 23, 28].

Índice

Date: Versión preliminar, 28 junio 2018.

2010 *Mathematics Subject Classification.* 11G, 14K.

Estas notas corresponden al curso dictado por los autores en la escuela AGRA III, Aritmética, Grupos y Análisis, del 9 al 20 de Julio de 2018 en Córdoba, Argentina. La presente versión es preliminar.

1. Introducción

Variedades abelianas son grupos algebraicos que, al mismo tiempo, son variedades algebraicas proyectivas. El primero ejemplo es dado por curvas elípticas que son las variedades abelianas de dimensión uno. Un ejemplo histórico y muy importante es la variedad jacobiana de una curva de género $\geqslant 2$. Empezamos con la exploración del caso de variedades complejas. Este caso es más concreto, pués cada variedad abeliana compleja puede ser

presentada como un toro complejo $\mathbb{C}^g/\Lambda$ donde Λ es un retículo $\cong \mathbb{Z}^{2g}$ dotado de una estructura adicional, una forma de Riemann. La segunda parte presenta la teoría del punto de vista de la geometría algebraica, es decir que se consideran variedades definidas sobre un cuerpo K; se demuestra que una gran parte de la geometría compleja puede ser recuperada. Como transición hacia la parte aritmética se demuestra el teorema de Mordell-Weil: el grupo $A(K)$ de los puntos de una variedad abeliana definida sobre un cuerpo de números K es un grupo de tipo finito. La tercera y última parte presenta la descripción aritmética de las variedades abelianas sobre un cuerpo finito $\mathbb{F}_q$ (teoría de Honda-Tate), sobre un cuerpo p-ádico y finalmente sobre $\mathbb{Q}$, donde investigaciones recientes intentan generalizar el teorema de modularidad de Wiles.

A pesar de no dar todas las pruebas, las dos primeras partes presentan material clásico y básico, la última parte tiene un sabor distinto, presentando material contemporáneo de investigación. Otra característica de la última parte es el uso de computadores, por ejemplo del código en *Magma*. De hecho clasificación explícita de variedades abelianas no es una cuestión puramente matemática. Esta clasificación explícita por medio de funciones L es el objetivo principal de la base de datos *L-functions and modular forms database*. La tercera parte de este curso también sirve como una introducción a la LMFDB, ya que cada clase corresponde directamente a una gran parte particular de la base de datos.

Parte 1. Variedades abelianas complejas

Definición 1.1. Una *variedad abeliana* es un grupo algebraico conexo que es también una variedad proyectiva.[1]

Recordamos que un grupo algebraico sobre un cuerpo k es una variedad A junto con aplicaciones regulares $m : A \times_k A \to A$ y $inv : A \to A$ y un elemento $e \in A(k)$ que satisfacen los axiomas de grupos usuales. Por lo tanto, definen una estructura de grupo sobre $A(\bar{k})$ con elemento neutro e.

En esta primera parte, consideramos variedades abelianas definidas sobre el cuerpo $\mathbb{C}$ de los números complejos. Veremos que las variedades abelianas sobre $\mathbb{C}$ son toros complejos. Las referencias principales para esta parte son: [2, 11, 7, 13] y [8].

2. Toros complejos

2.1. Variedades abelianas complejas son toros complejos. Sea A una variedad abeliana compleja. Entonces el conjunto $A(\mathbb{C})$ de los puntos complejos tiene una estructura de grupo de Lie complejo, o sea una variedad compleja donde las operaciones de grupo m, inv son aplicaciones holomorfas. Este grupo de Lie es además conexo y compacto.[2]

Veremos en esta sección (cf. Proposición 2.2) que eso implica que : 1. la ley de grupo sobre A es conmutativa; 2. $A(\mathbb{C})$ es un toro complejo, es decir el cociente de un $\mathbb{C}$-espacio vectorial de dimensión finita por un retículo Λ. Referencia principal: [11].

2.1.1. Exponencial de un grupo de Lie complejo. Recordamos, sin prueba, algunos resultados clásicos de teoría de los grupos de Lie. Sea T un grupo de Lie complejo, con elemento neutro e. Denotamos $V = Lie(T) = Tan_e(T)$ el álgebra de Lie asociada a T. Es un espacio vectorial de dimensión igual a la dimensión de T como variedad compleja.

[1] La definición usual sería un grupo algebraico conexo y completo, pero una variedad proyectiva es siempre completa y, además, la recíproca es verdad para una variedad abeliana. Este hecho es no obstante no trivial y no lo queremos demostrar.

[2] En efecto, la conexidad sale de la definición de A y el hecho que A sea proyectiva pone sobre $A(\mathbb{C})$ una estructura de subvariedad compleja de $\mathbb{P}^n(\mathbb{C})$ compacta pues cerrada en $\mathbb{P}^n(\mathbb{C})$.

Por cada vector tangente $v \in V$, hay un único morfismo $\lambda_v : \mathbb{C} \to T$ tal que $\lambda_v(0) = e$ y $(d\lambda_v)_0 : \mathrm{Tan}_0(\mathbb{C}) \to V$ manda el generador canónico $\left(\frac{\partial}{\partial t}\right)_0$ (la derivación en zero) de $\mathrm{Tan}_0(\mathbb{C})$ sobre v.

La *aplicación exponencial* $\exp_T = \exp : V \to T$ es definida por $\exp(v) = \lambda_v(1)$ para todo $v \in V$.

La unicidad de λ_v para cada v permite demostrar que para cada $v \in V, s \in \mathbb{C}, t \in \mathbb{C}$, $\lambda_v(st) = \lambda_{tv}(s)$. Entonces

$$\exp(tv) = \lambda_v(t) \qquad (t \in \mathbb{C}, v \in V).$$

Una vez identificado el espacio tangente en 0 de V con si mismo, $(d\exp)_0 = \mathrm{id}_V$. Por el teorema de las funciones implicitas, se deduce que la aplicación exp es un diffeomorfismo local en un entorno de $0 \in V$ hacia un entorno de $e \in T$.

Lema 2.1. *Si T es conexo, entonces* $\exp(V)$ *genera el grupo T : para cada $x \in T$, existen $v_1, \ldots, v_n$ en V tales que $x = \exp(v_1) \ldots \exp(v_n)$.*

Demostración. Como exp es un diffeomorfismo local en 0, Im(exp) contiene un entorno abierto U de e en T, y sus traslaciones $x.U$ son entornos abiertos de cada $x \in \langle \mathrm{Im}(\exp) \rangle$. Entonces $\langle \mathrm{Im}(\exp) \rangle$ es un abierto de T. Como también es cerrado[3], la conexidad de T implica $\langle \mathrm{Im}(\exp) \rangle = T$. □

Por la unicidad de $\lambda_v = (t \mapsto \exp_T(tv))$ se puede deducir también la siguiente propiedad: sea $F : T_1 \to T_2$ un morfismo de grupos de Lie complejos, entonces

$$F \circ \exp_{T_1} = \exp_{T_2} \circ (dF)_e, \tag{2.1}$$

es decir el siguiente diagrama conmuta:

$$\begin{array}{ccc} V_1 & \xrightarrow{(dF)_e} & V_2 \\ {\scriptstyle \exp_{T_1}}\downarrow & & \downarrow{\scriptstyle \exp_{T_2}} \\ T_1 & \xrightarrow{F} & T_2 \end{array}$$

2.1.2. Consecuencias para un grupo de Lie complejo conexo compacto.

Proposición 2.2. *Sea T un grupo de Lie complejo conexo compacto y $V = \mathrm{Tan}_e(T)$. Entonces*

1. *la ley de grupo sobre T es conmutativa;*
2. $\exp = \exp_T : V \to T$ *es un morfismo de grupos de Lie;*
3. *el morfismo* exp *es sobreyectivo;*[4]
4. *el núcleo de* exp *es un retículo del $\mathbb{C}-$espacio vectorial V y T es un toro complejo.*

Recordamos que un *retículo* de un $\mathbb{C}$-espacio vectorial V de dimensión finita g es un subgrupo de la forma $\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{2g}$ donde $e_1, \ldots, e_{2g}$ son vectores $\mathbb{R}$-linealmente independientes en V. Un subgrupo Λ de V es un retículo de V si y sólo si Λ es discreto y $T = V/\Lambda$ es compacto con la topología cociente[5]. Se puede dotar a tal cociente con una estructura de variedad compleja definiendo el haz de las funciones holomorfas: una función $f : U \to \mathbb{C}$ en un abierto U de T es *holomorfa* si y sólo si la función Λ-periódica $f \circ \pi$ es holomorfa sobre $\pi^{-1}(U)$. Observamos que toda función holomorfa f sobre T es constante, pues $f \circ \pi$ es holomorfa y acotada sobre V. Las operaciones de grupos naturales sobre T son aplicaciones holomorfas. El grupo de Lie obtenido es llamado un *toro complejo*.

Denotamos por $\mathcal{M}(T)$ el cuerpo de las funciones meromorfas de T.

[3]porque su complementario es la unión de sus traslados, que son abiertos.

[4]o suryectivo, como el lector prefiera.

[5]es decir $U \subset T$ es abierto si $\pi^{-1}(U)$ es abierto en V, para $\pi : V \to T$ la proyección canónica.

Demostración. 1. Por un elemento $x \in T$, consideramos $f_x : T \to T$ el morfismo de conjugación: $f_x(y) = xyx^{-1}$ y su diferencial $(df_x)_e : V \to V$ en el neutro $e \in T$. La aplicación $T \to \mathrm{End}(V); x \mapsto (df_x)_e$ es holomorfa sobre la variedad compleja conexa compacta T y a valores en el espacio de dimensión finita V, entonces es constante. Por consecuencia, tenemos para todo $x \in T$, $(df_x)_e = (df_e)_e = \mathrm{id}_V$.

Se deduce de (2.1) y de lo precedente que $f_x \circ \exp_T = \exp_T \circ (df_x)_e = \exp_T$, lo que muestra que la imagen de exp está en el centro de T. Por conexidad de T, se deduce que $\exp(V) \subset Z(T)$ genera T como grupo (cf Lema 2.1), entonces T es conmutativo.

2. Es consecuencia de la unicidad de λ_v: Sean x, y en V. Como T es abeliano, la aplicación $t \mapsto \exp(tx).\exp(tv)$ es un morfismo de grupos de Lie. Además su diferencial en 0 manda $\left(\frac{\partial}{\partial t}\right)_0$ sobre $x+y$, entonces $\varphi = \lambda_{x+y}$, o sea $\exp(tx).\exp(ty) = \exp(t(x+y))$ para todos $t \in \mathbb{C}, x, y \in V$. Tomando $t = 1$, obtenemos que exp es un morfismo de grupos de Lie (exp es holomorfa por definición).
3. Por 2., la imagen de exp es un subgrupo de T y genera T, entonces es igual a T.
4. Por el hecho que exp es un homeomorfismo local alrededor de 0, hay un entorno U de 0 tal que $U \cap \ker(\exp) = \{0\}$ (exp es localmente inyectiva). Eso demuestra que $\ker(\exp)$ es discreto. Además, por lo que precede, exp induce una aplicación $\phi : V/\Lambda \to T$ que es un isomorfismo de grupos holomorfo. Su diferencial en 0 es biyectiva, entonces ϕ es un isomorfismo de grupos de Lie complejos. Como T es compacto, también lo es V/Λ y así el subgrupo discreto Λ es un retículo de V. Deducimos que $T \cong V/\Lambda$ es un toro complejo.

□

Corolario 2.3. *Sea A una variedad abeliana sobre $\mathbb{C}$. Entonces A es un grupo abeliano y $A(\mathbb{C})$ es un toro complejo.*

En lo sucesivo, denotaremos aditivamente la ley de grupo sobre un toro complejo y 0 su elemento neutro.

2.1.3. Isogenías.

Lema 2.4. *Sean $T_1 = V_1/\Lambda_1$ y $T_2 = V_2/\Lambda_2$ dos toros complejos y $f : T_1 \to T_2$ una aplicación holomorfa. Entonces f es inducida por una aplicación $\mathbb{C}$-afina $\tilde{f} : V_1 \to V_2$ tal que $\tilde{f}(\Lambda_1) \subset \Lambda_2$. Si además $f(0) = 0$, entonces f es un morfismo de grupos de Lie. Su imagen es un subtoro de T_2 y su núcleo es un subgrupo cerrado de T_1, de cual la componente conexa es un subtoro de índice finito. (En el caso general, f es la composición de un morfismo por una traslación).*

Demostración. Cf. [7, lemma 1.5.1.1] o [1, Teorema 2.3]. □

Definición 2.5. Decimos que un morfismo $\varphi : T_1 \to T_2$ es una *isogenía* si es sobreyectivo y de núcleo finito. El orden de $\ker \varphi$ es llamado *grado* de φ.

Observación 2.6. Si $\varphi : T_1 \to T_2$ es una isogenía, entonces $\dim(T_1) = \dim(T_2)$.

Ejemplo 2.7 (Multiplicación por un entero)**.** Sea $T = V/\Lambda$ un toro complejo de dimensión g y $n \in \mathbb{Z}, n \geqslant 0$. La multiplicación por n denotada $[n] = n\mathrm{id}_T \in \mathrm{End}(T)$ es una isogenía de grado n^{2g}. En efecto, $\ker[n] = (1/n)\Lambda/\Lambda \cong \Lambda/n\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Dejamos como ejercicio la prueba del lema siguiente, lo cual demuestra que la relación de isogenía es una relación de equivalencia. Así decimos que T_1 y T_2 son *isógenos* si existe una isogenía $T_1 \to T_2$.

Lema 2.8. *Sean $\varphi : T_1 \to T_2$ y $\psi : T_2 \to T_3$ dos isogenías.*

1. $\psi \circ \varphi$ es una isogenía de grado $\deg(\psi)\deg(\varphi)$;

2. *existe una isogenía* $\hat{\varphi} : T_2 \to T_1$ *tal que* $\varphi \circ \hat{\varphi} = [d]_{T_2}$ *y* $\hat{\varphi} \circ \varphi = [d]_{T_1}$*, donde denotamos* $d = \deg(\varphi)$*. La isogenía* $\hat{\varphi}$ *es llamada* isogenía dual de φ*.*

Ejemplo 2.9. En dimensión 1.

Ver Teorema 2.15 y Corolario 2.16 para la descomposición de las variedades abelianas a menos de una isogenía. En Sección 5 estudiaremos el anillo de los endomorfismos de una variedad abeliana.

2.2. Cuando un toro complejo es una variedad abeliana. En Subsección 2.1, demostramos que una variedad abeliana es un toro complejo. Es natural preguntarse si todos los toros complejos son variedades abelianas, es decir si admiten una inmersión holomorfa en un espacio proyectivo.

2.2.1. Condición necesaria y suficiente. Sea Λ un retículo de un espacio vectorial complejo V de dimensión g. Teorema 2.12 da condiciones necesarias y suficientes para que un toro complejo V/Λ sea una variedad abeliana. Daremos las líneas principales de la demostración en Subsecciones 3.3 y 3.4.

Recordamos que una *forma hermitiana sobre* V es una aplicación $H : V \times V \to \mathbb{C}$ que es $\mathbb{C}$-bilineal en la primera variable y tal que $H(z, w) = \overline{H(w, z)}$. Para una forma hermitiana $H : V \times V \to \mathbb{C}$, denotamos $E = \Im(H) : V \times V \to \mathbb{R}$ su parte imaginaria, la cual es una forma real bilineal alternada. Dejamos la prueba al lector del siguiente hecho:

Lema 2.10. *La aplicación* $H \mapsto E = \Im(H)$ *define una correspondencia biyectiva desde el conjunto de las formas hermitianas en el conjunto de las formas reales bilineales alternadas* E *verificando además* $E(ix, iy) = E(x, y)$*. La biyección inversa manda* E *sobre* H *definida por* $H(x, y) = E(ix, y) + iE(x, y)$*.*

Definición 2.11 (Forma de Riemann)**.** Diremos que una forma hermitiana $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ es una *forma de Riemann con respecto a un retículo* Λ *de* V si $E(\Lambda \times \Lambda) \subset \mathbb{Z}$, donde $E = \Im(H)$.

Teorema 2.12. *Un toro complejo* V/Λ *es una variedad abeliana si y sólo si existe una forma de Riemann con respecto a* Λ *que sea no degenerada (i.e. definida positiva).*

Ejemplo 2.13 (Curvas elípticas)**.** Consideramos $\mathbb{C}/\Lambda$ un toro de dimensión 1. La función elíptica de Weierstrass $\mathcal{P}(z, \Lambda)$ y su derivada inducen una inmersión holomorfa de $\mathbb{C}/\Lambda$ en $\mathbb{P}^2(\mathbb{C})$ mediante $z \mapsto (1 : \mathcal{P}(z, \Lambda) : \mathcal{P}'(z, \Lambda))$. Entonces los toros de dimensión 1 son todos variedades abelianas. Son llamadas *curvas elípticas.*

Eso es confirmado por el teorema precedente porque existe una forma de Riemann natural sobre $\mathbb{C}$ con respecto a $\Lambda = Z\lambda_1 + \mathbb{Z}\lambda_2$ con $\Im(\lambda_1/\lambda_2) > 0$: definimos H por $H(z, w) = \frac{z\bar{w}}{\lambda_1 \lambda_2}$. Se puede verificar que H es una forma de Riemann no degenerada (Ejercicio).

Ejemplo 2.14 (Variedades abelianas a multiplicación compleja)**.** Sea K un *cuerpo CM*, es decir una extensión cuadrática totalmente imaginaria de un cuerpo de números totalmente real que denotaremos K^+. Denotamos $[K^+ : \mathbb{Q}] = g$ el grado de K^+ (de tal manera que $[K : \mathbb{Q}] = 2g$).

Decimos que un conjunto Φ de inmersiones $\varphi_k : K \hookrightarrow \mathbb{C}$ es un *tipo CM de* K si $\mathrm{Hom}(K, \mathbb{C})$ es la unión disjunta de Φ y $\bar{\Phi}$ donde para $\Phi = \{\varphi_1, \ldots, \varphi_g\}$, denotamos $\bar{\Phi} = \{\bar{\varphi}_1, \ldots, \bar{\varphi}_g\}$ con $\bar{\varphi}_i$ dada por la composición de φ_i con la conjugación compleja. Un tipo CM de K induce un isomorfismo $f : K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}^g$ por $x \otimes 1 \mapsto (\varphi_1(x), \ldots, \varphi_g(x))$.

Para un orden $\mathcal{O}$ de K, $f(\mathcal{O})$ es un retículo de $\mathbb{C}^g$. Vamos a definir una forma de Riemann no degenerada sobre el toro complejo $\mathbb{C}^g/f(\mathcal{O})$. La variedad abeliana así obtenida es dicha *a multiplicación compleja por* K*, de tipo CM* (K, Φ).

Se puede demostrar que $K = K^+(\xi)$ con ξ un entero algebraico tal que $-\xi^2$ es totalmente positivo en K^+ y para todo $k \in \{1, \dots, g\}$, $\Im(\varphi_k(\xi)) > 0$. Definimos E por

$$E(z,w) = \sum_{k=1}^{g} \varphi_k(\xi)(\bar{z}_k w_k - z_k \bar{w}_k), \qquad (z, w \in \mathbb{C}^g) \tag{2.2}$$

Eso define claramente una forma $\mathbb{R}$-bilineal antisimétrica. La forma $E(iz, w)$ es simetrica, definida positiva. Se puede además demostrar que para todos $x, y \in K$, tenemos

$$E(f(x), f(y)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi \tilde{x} y) \tag{2.3}$$

donde $x \mapsto \tilde{x}$ es el automorfismo no trivial de K/K^+. Entonces $E(f(\mathcal{O}) \times f(\mathcal{O})) \subset \mathbb{Z}$. La forma de Riemann asociada es no degenerada (Ejercicio).

2.2.2. Teorema de reducibilidad de Poincaré. La prueba del teorema siguiente requiere la existencia de una forma de Riemann no degenerada sobre el toro considerado.

Teorema 2.15 (Teorema de reducibilidad de Poincaré)**.** *Sea A una variedad abeliana y B una subvariedad abeliana. Entonces existe una subvariedad abeliana C de A tal que $B + C = A$ y $B \cap C$ es finito, es decir tal que $B \times C \to A; (b, c) \mapsto b + c$ sea una isogenía.*

Demostración. Cf. [7] página 96. □

Decimos que un toro es *simple* si no tiene ningún subtoro no trivial. Denotamos $\mathrm{End}(A)$ el anillo de los endomorfismos de una variedad abeliana A. Es un orden en la $\mathbb{Q}$-álgebra de dimensión finita $\mathrm{End}_0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$. Observamos que un elemento $\varphi \in \mathrm{End}(A)$ es una isogenía si y sólo si φ es invertible en $\mathrm{End}_0(A)$.

Corolario 2.16. *1. Si A es simple, entonces $\mathrm{End}_0(A)$ es un álgebra de división (un cuerpo que puede ser no conmutativo);*

2. Toda variedad abeliana A es isógena a un producto de la forma $A_1^{n_1} \times \cdots \times A_s^{n_s}$ donde $A_1, \dots, A_s$ son variedades abelianas simples, dos a dos no isógenas. La $\mathbb{Q}$-álgebra $\mathrm{End}_0(A)$ es semisimple: $\mathrm{End}_0(A) \cong M_{n_1}(\mathrm{End}_0(A_1)) \times \cdots \times M_{n_r}(\mathrm{End}_0(A_r))$.

Demostración. Cf. [7] página 96. □

Cf. Sección 5 para una descripción mas avanzada de $\mathrm{End}_0(A)$.

3. Divisores sobre un toro, funciones theta y formas de Riemann

Esta sección es dedicada a introducir el material necesario y las ideas de la demostración de Teorema 2.12. Sea $T = V/\Lambda$ un toro complejo con V un $\mathbb{C}$-espacio vectorial de dimensión g y Λ un retículo de V. Deseamos determinar bajo que condiciones existe una inmersión holomorfa en un espacio proyectivo $\mathbb{P}^n(\mathbb{C})$, es decir una aplicación holomorfa $u : T \to \mathbb{P}^n(\mathbb{C})$ que induzca un isomorfismo de variedades complejas entre T y $u(T)$. Por el teorema de las funciones implícitas, u es una inmersión si y sólo si es inyectiva y si du es inyectiva en todo punto.

3.1. Funciones teta.

3.1.1. Para todo $t \in \mathbb{C}$, denotamos $e(t) = \exp(2i\pi t)$.

Definición 3.1 (Función teta)**.** Una *función teta relativamente a Λ* es una función meromorfa $\theta : V \to \mathbb{C}$ que satisface una ecuación de la forma

$$\theta(z + \lambda) = e(f_\lambda(z)).\theta(z) \qquad ((z, \lambda) \in V \times \Lambda) \tag{3.1}$$

donde $f_\lambda : V \to \mathbb{C}$ es una función afín en $z \in V$ para todo $\lambda \in \Lambda$. En otras palabras $f_\lambda(z) = L(z, \lambda) + J(\lambda)$, con $J : \Lambda \to \mathbb{C}$ y $L : V \times \Lambda \to \mathbb{C}$ es $\mathbb{C}$-lineal en $z \in V$ para todo $\lambda \in \Lambda$. El par (L, J) es llamado el *tipo* de la función teta.

Ejemplo 3.2. Toda función de la forma $z \mapsto e(F(z))$ donde F es un polinomio de grado $\leqslant 2$ es una función teta llamada *trivial*.

3.1.2. Forma de Riemann asociada a una función teta. Sea θ una función teta de tipo (L, J) relativamente a Λ. La relación (3.1) implica que para todos $\lambda_1, \lambda_2 \in \Lambda, z \in V$, tenemos

$$L(z, \lambda_1 + \lambda_2) - L(z + \lambda_1, \lambda_2) - L(z, \lambda_1) \equiv J(\lambda_1 + \lambda_2) - J(\lambda_1) - J(\lambda_2) \pmod{\mathbb{Z}},$$

de lo que deducimos

1. $L(z, \lambda_1 + \lambda_2) = L(z, \lambda_1) + L(z, \lambda_2)$.
2. $L(\lambda_1, \lambda_2) \equiv J(\lambda_1 + \lambda_2) - J(\lambda_1) - J(\lambda_2) \pmod{\mathbb{Z}}$
3. $L(\lambda_1, \lambda_2) \equiv L(\lambda_2, \lambda_1) \pmod{\mathbb{Z}}$.

De 1., podemos extender L a $\mathbb{R}$-linealidad a derecha, en una forma $L : V \times V \to \mathbb{C}$. Así la nueva forma L es $\mathbb{C}$-lineal a izquierda y $\mathbb{R}$-lineal a derecha. Entonces la forma E definida por $E(z, w) = L(z, w) - L(w, z)$ para todo $(z, w) \in V \times V$ es $\mathbb{R}$-bilineal alternada y, por 3., tiene valores enteras sobre $\Lambda \times \Lambda$. Además, tenemos (Ejercicio)

$$E(iz, iw) = E(z, w) \qquad ((z, w) \in V \times V) \tag{3.2}$$

Así, a una función teta θ le asociamos la forma de Riemann H_θ definida por $H_\theta(z, w) = E(iz, w) + iE(z, w)$. Observamos que H_θ depende sólo del tipo (L, J) de θ.

Decimos que dos funciones teta θ, θ' son *equivalentes* si θ/θ' es trivial.

Ejercicio 3.3. Demostrar que si θ es trivial, entonces $H_\theta = 0$ y que para θ, θ' dos funciones teta, tenemos $H_{\theta/\theta'} = H_\theta - H'_\theta$. Deducir que si θ y θ' son equivalentes, entonces $H_\theta = H_{\theta'}$.

3.1.3. Función teta normalizada.

Lema 3.4. *Sea θ una función teta y $H = H_\theta$ la forma de Riemann asociada. Entonces existe una función teta $\tilde{\theta}$, llamada* normalizada*, dada por la ecuación*

$$\tilde{\theta}(z + \lambda) = e\left(\frac{1}{2i}H(z, \lambda) + \frac{1}{4i}H(\lambda, \lambda) + K(\lambda)\right)\tilde{\theta}(z) \qquad ((z, \lambda) \in V \times \Lambda) \tag{3.3}$$

donde K es a valores reales y verifica

$$K(\lambda + \mu) - K(\lambda) - K(\mu) \equiv \frac{1}{2}E(\lambda, \mu) \pmod{\mathbb{Z}}. \tag{3.4}$$

Además, existe $c > 0$ tal que, para todo $z \in V$, $|\tilde{\theta}(z)| \leqslant c.e\left(\frac{1}{4i}H(z, z)\right)$.

La función ψ definida por $\psi(z) = e(K(z))$ como precede verifica

$$\psi(\lambda + \mu) = \psi(\lambda)\psi(\mu)e\left(\frac{1}{2}E(\lambda, \mu)\right) \tag{3.5}$$

y es llamada *semi-carácter* asociado a la forma de Riemann H.

Denotamos por $\mathcal{R}(T)$ el grupo de las formas de Riemann sobre el toro complejo T y

$$\mathcal{P}(T) = \{(H, \psi); H \in \mathcal{R}(T), \psi \text{ semi-carácter asociado a } H\}.$$

El conjunto $\mathcal{P}(T)$ es un grupo por la ley $(H_1, \psi_1).(H_2, \psi_2) = (H_1 + H_2, \psi_1\psi_2)$.

Demostración. HACER □

Proposición 3.5. *1. Tenemos $H_\theta = 0$ si y sólo si θ es trivial*

2. Si θ es entera, entonces H_θ es positiva (es decir $H_\theta(z, z) \geqslant 0$ para todo $z \in V$).

3. Para todo $z_0 \in V$, la función $z \mapsto \theta(z_0 + z)$ es constante sobre el núcleo de H_θ:

$$N = \{z \in V; H_\theta(z, w) = 0, \forall w \in V\}.$$

Demostración. Hacer. □

3.2. Divisores. Recordamos:

Definición 3.6 (Divisores)**.** Sea X una variedad compleja conexa.

1. Sea $(U_\alpha, f_\alpha)_\alpha$ una familia donde $(U_\alpha)_\alpha$ es un recubrimiento de X y f_α son funciones meromorfas sobre U_α no idénticamente cero sobre ninguna componente conexa de U_α. Decimos que una tal familia es *admisible* si para todos α, β, sobre $U_\alpha \cap U_\beta$, f_α/f_β es holomorfa y no se anula. Dos tales familias admisibles son equivalentes si su unión todavía es admisible.
2. Un *divisor (de Cartier) sobre* X es una clase de equivalencia de una familia admisible (U_α, f_α).
3. Decimos que un divisor D es *efectivo* si puede ser descrito por una familia (U_α, f_α) con f_α holomorfa sobre U_α para todo α.
4. Si D es dado por (U_α, f_α) entonces la familia $(U_\alpha, 1/f_\alpha)$ define un divisor que depende sólo de D y es denotado $-D$. Si D' es un divisor dado por (U'_α, f'_α) entonces $(U_\alpha \cap U'_\beta, f_\alpha.f'_\beta)$ define un divisor que depende sólo de D y D', denotado por $D + D'$.
5. Un divisor es *principal* si está dado por (X, f) con f meromorfa sobre X. Decimos que dos divisores son linealmente equivalentes si $D - D'$ es principal. Lo denotamos $D \sim D'$.

El conjunto de los divisores sobre X es un grupo abeliano que denotamos $\mathrm{Div}(X)$. Cf. [1, 13].

Consideramos ahora $X = T = V/\Lambda$ como antes. La proyección $\pi : V \to T$ define una aplicación $\pi^* : \mathrm{Div}(T) \to \mathrm{Div}(V)$, cuya imagen es constituida por los divisores Λ-*periódicos*, es decir los divisores D' tales que $t^*_\lambda D' = D'$ para todo $\lambda \in \Lambda$, donde t_λ es la traslación por λ[6].

Observamos que el divisor (sobre V) de una función teta relativa a Λ es Λ-periódico y por eso define un divisor sobre T.

Teorema 3.7 (Poincaré)**.** *Todo divisor sobre T proviene de una función teta meromorfa: para todo $D \in \mathrm{Div}(T)$, existe θ una función teta relativa a Λ tal que $\pi^*(D) = (\theta)$. Además, si D es efectivo, la función θ asociada es holomorfa. Dos funciones teta θ, θ' definen el mismo divisor si y sólo si son equivalentes (i.e. θ/θ' es una función teta trivial). En otras palabras, tenemos un isomorfismo de grupos $\{$funciones teta$\}/\{$funciones triviales$\} \cong \mathrm{Div}(T)$.*

Demostración. Cf. [1] página 43 o [11]. □

De Proposición 3.5, Teorema 3.7 y Ejercicio 3.3, tenemos el siguiente resultado.

Corolario 3.8. *La aplicación que a un divisor $D \in \mathrm{Div}(T)$ asocia la forma de Riemann $H_D := H_\theta$ donde $\pi^*(D) = (\theta)$ está bien definida. Es un morfismo de grupos $\mathrm{Div}(T) \to \mathcal{R}(T)$. Si D es efectivo, θ es entera entonces H_D es positiva.*

3.3. Condición necesaria en Teorema 2.12. Supongamos que un toro complejo T es una variedad abeliana i.e. que existe una inmersión $u : T \to \mathbb{P}^n(\mathbb{C})$. Denotamos por $(x_0 : \cdots : x_n)$ la función coordenadas en $P^n(\mathbb{C})$.Podemos suponer que la imagen de u no es contenida en el hiperplano $(x_0 = 0)$ (a meno de una permutación de los índices). Entonces el pull-back de este hiperplano define un divisor efectivo D sobre T. Denotamos θ_0 la función teta normalizada asociada a D. Es una función entera, entonces la forma de Riemann asociada H es positiva (cf. Proposición 3.5). Las funciones $\theta_j := \left(\frac{x_j}{x_0}\right)\theta_0$ son funciones teta equivalentes a θ_0, entonces tienen la misma forma de Riemann asociada H. Las funciones $\theta_0, \ldots, \theta_n$ son enteras y no tienen cero común. Asi u se escribe $u(z) = (\theta_0(z) : \cdots : \theta_n(z))$

[6]Si D' es dado por (U_α, f_α) entonces $t^*_\lambda D'$ es dado por $(U_\alpha + \lambda, f_\alpha(z - \lambda))$.

Como cada función θ_j es constante sobre los conjuntos $z_0 + N$ ($z_0 \in V$), el hecho que u sea una inmersión fuerza el núcleo N de H a ser trivial (la inmersión tiene que separar los puntos!). En conclusión la forma de Riemann H asociada a D es no degenerada.

3.4. Teoremas de Riemann-Roch y de Lefschetz. En esta parte queremos dar las ideas del final de la prueba de Teorema 2.12. Consideramos un toro complejo $T = V/\Lambda$ con una forma de Riemann no degenerada. Queremos construir una inmersión holomorfa en un espacio proyectivo. Vimos en Sección 3.3 que tales inmersiones provienen de funciones teta de mismo tipo. Por eso, examinamos en primer lugar la dimensión de los espacios de funciones teta del mismo tipo.

Recordamos que para una forma $\mathbb{R}$-bilineal alternada E entera sobre un retículo Λ de rango $2g$ que es no degenerada, existen enteros $d_1, \ldots, d_g$ tales que $d_i > 0$, $d_1 \mid \cdots \mid d_g$ y una base $(\gamma_1, \ldots, \gamma_{2g})$ de Λ en la cual la matriz de E es

$$\begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix}$$

con $\Delta = Diag(d_1, \ldots, d_g)$. Deducimos que $\det(E) > 0$. Su raíz cuadrada es llamada el *Pfaffiano de* E: $\mathrm{Pf}(E) = \sqrt{\det(E)} = d_1 \ldots d_g$.

Teorema 3.9 (Teorema de Riemann-Roch para las variedades abelianas)**.** *Si (L, J) es un tipo*[7] *de forma de Riemann asociada H definida positiva, entonces el $\mathbb{C}$-espacio vectorial (L, J) de las funciones teta de mismo tipo tiene dimensión $\mathrm{Pf}(E) > 0$ donde E es la forma $\mathbb{R}$-bilineal alternada definida por H.*

Observación 3.10. Para un divisor efectivo D sobre T, hay una función teta entera θ_0 tal que $(\theta_0) = \pi^*(D)$. La aplicación $\theta \mapsto \theta/\theta_0$ define un isomorfismo entre $\mathcal{L}(\theta_0)$ y el espacio vectorial $\mathcal{L}(D) = \{f \in \mathcal{M}(T); D + (f) \geqslant 0\} \cup \{0\}$. Este explica el nombre de Teorema 3.9.

Observación 3.11. Sea H una forma de Riemann sobre V relativa a un retículo Λ. Entonces, existe una aplicación $\alpha : \Lambda \to U(1)$ que es un semi-carácter para H (Ejercicio). Por consecuencia, existe un tipo (L, J) de forma de Riemann asociada H.

Continuamos con el final de la prueba de Teorema 2.12. Supongamos que el toro T es dotado de una forma de Riemann no degenerada H, la cual es asociada a un tipo (L, J) por Observación 3.11. De Teorema 3.9 existe una función teta entera θ_0 de tipo (L, J). Denotamos $(\theta_0, \ldots, \theta_n)$ una base de $\mathcal{L}(\theta_0)$ y D el divisor efectivo dado por $\pi^*(D) = (\theta_0)$. Obtenemos una aplicación holomorfa $\Phi_D : T \to \mathbb{P}^n(\mathbb{C}); z \mod \Lambda \mapsto (\theta_0(z) : \cdots : \theta_n(z))$.

Definición 3.12. Decimos que un divisor D es *muy amplio* si Φ_D es una inmersión holomorfa. Decimos que D es *amplio* si un múltiplo positivo de D es muy amplio.

La fín de la prueba se deduce del siguiente resultado:

Teorema 3.13 (Lefschetz)**.** *Sea D un divisor sobre T con forma de Riemann asociada H_D no degenerada. Entonces $3D$ es muy amplio, es decir, $3D$ define una inmersión holomorfa $\Phi_{3D} : T \to \mathbb{P}^n(\mathbb{C})$.*

Observamos que, con Sección 3.3, el Teorema de Lefschetz demuestra:

Corolario 3.14. *Un divisor D sobre T es amplio si y sólo si H_D es una forma de Riemann no degenerada.*

[7] es decir un par donde L es $\mathbb{C}$-lineal a izquierda y $\mathbb{R}$-lineal a derecha y con las propiedades 1,2,3 de §3.1.2.

4. Teorema de Appell-Humbert y variedad abeliana dual

4.1. Teorema de Appell-Humbert. Sea ahora $A = V/\Lambda$ un toro complejo. Por Lema 3.4 y Teorema 3.7, a un divisor D sobre A podemos asociarle una función teta y entonces una función teta normalizada y un par (H, ψ) como en Lema 3.4 y (3.5). Recordamos que el conjunto $\mathcal{P}(A)$ de las parejas (H, ψ) con $H \in \mathcal{R}(A)$ una forma de Riemann sobre A y ψ un semi-carácter asociado a H, es un grupo. Consideramos la aplicación $\Psi : \mathrm{Div}(T) \to \mathcal{P}(T); D \mapsto (H_D, \psi_D)$.

Denotamos por $\mathrm{Pic}(A)$ el cociente de $\mathrm{Div}(A)$ por el subgrupo $Princ(A)$ de los divisores principales, y $\mathrm{Pic}^0(A)$ el cociente por $Princ(A)$ del subgrupo de los divisores D tales que $H_D = 0$. El *grupo de Neron-Severi* es el cociente $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$. Observamos que los semi-caracteres para la forma de Riemann cero son exactamente los elementos del dual de Pontryagin $\mathrm{Hom}(\Lambda, U(1))$ de Λ, donde $U(1) = \{z \in \mathbb{C}, |z| = 1\}$.

Teorema 4.1 (Appell-Humbert)**.** *La aplicación* $\Psi : \mathrm{Div}(A) \to \mathcal{P}(A); (D \mapsto (H_D, \psi_D))$ *es un morfismo de grupos que induce un isomorfismo* $\mathrm{Pic}(A) \to \mathcal{P}(A)$*, por lo cual* $\mathrm{Pic}^0(A) \cong \mathrm{Hom}(A, U(1))$ *y* $NS(A) \cong \mathcal{R}(A)$.

Demostración. □

4.2. Variedad abeliana dual. Denotamos por $\bar{V}^*$ el conjunto de las formas $\mathbb{C}$-anti-lineales sobre V (es decir las formas $\ell : V \to \mathbb{C}$ tales que $\ell(\alpha z) = \bar{\alpha}\ell(z)$ para todo $\alpha \in \mathbb{C}, z \in V$). La aplicación $\ell \mapsto \mathrm{Im}(\ell)$ define un isomorfismo entre el $\mathbb{R}$-espacio vectorial definido por $\bar{V}^*$ y $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ (Ejercicio). Entonces la forma $\mathbb{R}$-bilineal $\langle , \rangle : \bar{V}^* \times V \to \mathbb{R}$ definida por $\langle \ell, v \rangle = \mathrm{Im}(\ell(v))$, es no degenerada. Eso implica que $\widehat{\Lambda} := \{\ell \in \bar{V}^*; \langle \ell, \Lambda \rangle \subset \mathbb{Z}\}$ es un retículo de $\bar{V}^*$ (Ejercicio).

Definición 4.2. Llamamos a $\widehat{\Lambda}$ el *retículo dual de* Λ y al toro de dimensión g

$$\widehat{A} := \bar{V}^*/\widehat{\Lambda}$$

el *toro dual de* A.

Observación 4.3. La aplicación $\bar{V}^* \to \mathrm{Hom}(\Lambda, U(1)); \ell \mapsto e(\langle \ell, . \rangle)$ es un morfismo sobreyectivo, de núcleo $\widehat{\Lambda}$, induciendo un isomorfismo $f : \bar{V}^*/\widehat{\Lambda} \cong \mathrm{Hom}(\Lambda, U(1))$.

Supongamos ahora que A es una variedad abeliana y sea $D \in \mathrm{Div}(A)$. Consideramos la aplicación $\varphi_D : A \to \mathrm{Pic}(A); a \mapsto [t_a^* D - D]$, donde $t_a : x \mapsto x + a$ es la traslación por a en A.

Proposición 4.4. *1. la imagen de* φ_D *está en* $\mathrm{Pic}^0(A)$ *;*

2. la aplicación φ_D *depende sólo de la clase* $[D]$ *de* D *en* $NS(A)$*;*

3. si D *es amplio, entonces* $\varphi_D : A \to \mathrm{Pic}^0(A) = \widehat{A}$ *es una isogenía de grado* $\det(E) = \mathrm{Pf}(E)^2$.

Demostración. 1. Sea $a \in V$ y seguimos denotando a a su imagen en $A = V/\Lambda$. Sea θ una función teta asociada a D, entonces $\pi^*(t_a * D) = (\theta_a)$ donde $\theta_a(z) = \theta(z + a)$. Entonces $\pi^*(t_a^* D - D) = (\theta_a/\theta)$. Un calculo muestra que la ecuación de la función teta normalizada equivalente a que θ_a/θ tiene multiplicador $e(\frac{1}{2i}H(a, \lambda)) = e(E(a, \lambda))$, donde $H = H_D$ y $E = \mathrm{Im}(H)$, lo que demuestra que la función de Riemann asociada es cero.

2. Si D es tal que $H_D = 0$, entonces la función teta normalizada asociada a θ_a/θ es trivial, es decir $[t_a^* D - D] = 0$.

3. Observamos que con Teorema 4.1 podemos ver la aplicación φ_D a través del diagrama

$$\begin{array}{ccc} A & \xrightarrow{\varphi_D} & \mathrm{Pic}^0(A) \\ & \searrow^{\psi} & \downarrow \cong \\ & & \mathrm{Hom}(\Lambda, U(1)) \end{array}$$

donde la aplicación vertical asocia a un divisor D' el semi-carácter de la función teta normalizada asociada, entonces, como lo hemos visto en 1., el morfismo ψ es dado por $\psi(a) = (\lambda \mapsto e(E(a,\lambda))$. En el caso donde E es no degenerada, ψ es sobreyectivo, entonces φ_D es una isogenía. Su núcleo es $\{z \in V; E(z,\lambda) \in \mathbb{Z} \text{ para todo } \lambda \in \Lambda\}/\Lambda$. Considerando una base simpléctica de Λ, se puede demostrar que es un grupo finito de orden $\mathrm{Pf}(E)^2$.

□

Corolario 4.5. *Si A es una variedad abeliana, entonces $\widehat{A}$ es también una variedad abeliana llamada* variedad abeliana dual de A.

Demostración. Sea H una forma de Riemann no degenerada sobre A y D un divisor amplio asociado. Por Observación 4.3, Teorema 4.1 y la prueba de Proposición 4.4, 3., tenemos el diagrama conmutativo

$$\begin{array}{ccc} A = V/\Lambda & \xrightarrow{a \mapsto E(a,.)} & \bar{V}^*/\widehat{\Lambda} \\ \downarrow \varphi_D & & \downarrow \ell \mapsto e(\langle \ell, . \rangle) \\ \mathrm{Pic}^0(A) & \xrightarrow{\cong} & \mathrm{Hom}(A, U(1)) \end{array}$$

Como E es no degenerada la aplicación $\varphi_H : a \mapsto E(a,.)$ es un isomorfismo de V con $\bar{V}^*$ que manda Λ sobre $\widehat{\Lambda}$. Consideramos la forma hermitiana H^* sobre $\bar{V}^*$ definida por $H^*(z,w) := H(\varphi_H^{-1}(z), \varphi_H^{-1}(w))$. Desde Proposición 4.4,3., el núcleo de φ_H es finito, entonces $\varphi_H^{-1}(\widehat{\Lambda})/\Lambda$ es finito. Deducimos que un multiplo de H^* es una forma de Riemann y es no degenerada porque H lo es. □

Proposición 4.6. *1. Tenemos $\widehat{\widehat{A}} = A$.*

2. Un morfismo de toros $f : A_1 \to A_2$ induce un morfismo dual *$\hat{f} : \widehat{A}_2 \to \widehat{A}_1$ y $\hat{\hat{f}} = f$.*

3. El functor $\hat{\cdot}$ de la categoría de los toros es exacto.

4.3. Polarización.

Definición 4.7. Sea A una variedad abeliana. Una *polarización* sobre A es la data de la clase de un divisor amplio en $NS(A)$. De manera equivalente, es la data de una forma de Riemann H no degenerada. Digamos que (A,H) es una variedad abeliana *polarizada*. Una polarización H es *principal* si $\mathrm{Pf}(\Im(H)) = 1$ y decimos en este caso que (A,λ) es *principalmente polarizada.*

Por Proposición 4.4, una polarización $[D]$ define una isogenía $\varphi_D : A \to \widehat{A}$ de grado $\mathrm{Pf}(\Im(H_D))$. Entonces, si la polarización es principal, la correspondiente isogenía es un isomorfismo. Reciprocamente, una isogenía $\varphi : A \to \widehat{A}$ proviene de la clase de un divisor amplio D si y sólo si la aplicación analítica $V \to \bar{V}^*$ de la cual es inducida, es una forma hermitiana positiva definida.

Un importante ejemplo de variedad principalmente polarizada es dado por las jacobianas de curvas (cf. Parte 2). Pero no toda variedad abeliana es principalmente polarizada, aún si tenemos el resultado siguiente:

Proposición 4.8. *Toda variedad abeliana polarizada es isógena a una variedad abeliana principalmente polarizada.*

5. Endomorfismos de las variedades abelianas

Sea (A, H) una variedad abeliana polarizada. La inducida isogenía $\varphi = \varphi_H$ define un elemento invertible en $\mathrm{End}_0(A)$.

Definición 5.1 (Involución de Rosati)**.** Para $u \in \mathrm{End}(A)$ consideramos

$$u^\dagger := \varphi^{-1}\widehat{u}\varphi \in End_0(A).$$

Se puede ver que

$$(u^\dagger)^\dagger = u, \quad (u+v)^\dagger = u^\dagger + v^\dagger \quad (u \circ v)^\dagger = v^\dagger \circ u^\dagger.$$

La anti-involución inducida sobre $\mathrm{End}_0(A)$ es llamada *involución de Rosati.*

Para $u \in \mathrm{End}_0(A)$ denotamos $\mathrm{Tr}(u)$ la traza del endomorfismo real de V inducido por u.

Teorema 5.2. *La aplicación $(u, v) \mapsto \mathrm{Tr}(u^\dagger \circ v)$ es una forma bilineal simétrica definida positiva y racional sobre* $\mathrm{End}_0(A)$.

Entonces, si (A, φ) es una variedad simple polarizada, $D := \mathrm{End}_0(A)$ es un álgebra de división de rango finito sobre $\mathbb{Q}$, dotada de una anti-involución $\dagger$ tal que $\mathrm{Tr}(u^\dagger u) > 0$ para todo $u \neq 0$. Tales álgebras de división han sido clasificados por Albert en 1930. Sea K el centro de D y K_0 el subcuerpo de los elementos fijos por $\dagger$. Como $D \otimes_K \bar{K}$ es un álgebra de matrices, la dimensión de D sobre F es un cuadrado que denotamos d^2. Ademas, pues $\dagger$ es una anti-involución, $[K : K_0] \leqslant 2$. Denotamos $e = [K : \mathbb{Q}]$.

Teorema 5.3 (Clasificación de Albert)**.** *El cuerpo K_0 es un cuerpo de números algebraico totalmente real. Además, $D, \dagger$ son de uno de los tipos siguientes:*

Tipo I: *$D = K = K_0$ ($d = 1$) y $\dagger = \mathrm{id}$.*

Tipo II: *$K = K_0$ y D es un álgebra de cuaterniones indefinida*[8] *sobre K ($d = 2$). La involución $\dagger$ es de la forma $x^\dagger = ax^*a^{-1}$ donde $.^*$ es la involución usual de D y $a \in D$ un elemento tal que $a^2 \in K$ con a^2 totalmente negativo.*

Tipo III: *$K = K_0$ y D es un álgebra de cuaterniones definida*[9] *sobre K ($d = 2$). En este caso $x^\dagger = x^*$ es la involución usual sobre D.*

Tipo IV: *$[K : K_0] = 2$: K es un cuerpo CM*[10]*. En el caso donde $K = D$, A es una variedad abeliana CM por K.*

Además, para todos tipos, tenemos la restricción de dimensión: $ed^2 \mid 2g$. En particular, para los tipos II y III tenemos $e \mid 2g$. Para el tipo I, tenemos hasta $e \mid g$.

Observación 5.4. Con estas restricciones respectadas, para cada uno de este tipo, existe una variedad abeliana con el álgebra de endomorfismos correspondiente, a menos de dos excepciones para los tipos III y IV.

Para mas detalles, el lector podrá consultar [11] p186 o la sección 5.5 y el capítulo 9 de [2].

[8] o sea $D \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ para toda inmersión $K \hookrightarrow \mathbb{R}$.

[9] o sea $D \otimes_K \mathbb{R}$ es el cuerpo de los cuaterniones para toda inmersión $K \hookrightarrow \mathbb{R}$.

[10] es decir, por definición, una extensión cuadratica totalmente imaginaria de un cuerpo de números totalmente real

6. Espacio de moduli

Definición 6.1. El *semi-espacio de Siegel* es el conjunto de matrices

$$\mathfrak{h}_g = \{Z \in M_g(\mathbb{C}); {}^tZ = Z, \Im(Z) > 0\}.$$

El grupo $\mathrm{Sp}_{2g}(\mathbb{R})$ actúa (a la izquierda) sobre $\mathfrak{h}_g$ por $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).Z = (aZ+b)(cZ+d)^{-1}$. El cociente

$$\mathcal{A}_g(\mathbb{C}) = \mathcal{H}_g/\mathrm{Sp}_{2g}(\mathbb{Z})$$

tiene una estructura de variedad analítica compleja. Sus puntos están en correspondencia biyectiva con las clases de isomorfía de variedades abelianas complejas principalmente polarizadas: $\mathcal{A}_g$ es un *espacio de moduli* para las variedades principalmente polarizadas.

Ver capítulo 8 de [2].

7. Ejercicios

1. Sea τ una matriz $g \times g$ simétrica con $\mathrm{Im}\,\tau$ definida positiva (es decir un elemento de $\mathfrak{h}_g$). Denotamos $A_\tau = \mathbb{C}^g/\Lambda_\tau$ donde:

   $$\Lambda_\tau := \mathbb{Z}^g + \tau\mathbb{Z}^g = \{m + \tau n \mid m,\, n \in \mathbb{Z}^g\}.$$

   Mostrar que $H(z,w) := {}^tz(\mathrm{Im}\,\tau)^{-1}\bar{w}$ define una forma de Riemann que induce una polarización principal sobre A_τ. [Indicación: verificar que $\mathrm{Im}\,H(m+\tau n, h+\tau\ell) = {}^tnh - {}^tm\ell$.]
2. Mostrar directamente que, cuando $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es una matriz en $\mathrm{Sp}_{2g}(\mathbb{Z})$ y $\tau' = g\cdot\tau = (a\tau+b)(c\tau+d)^{-1}$, entonces las variedades abelianas A_τ y$A_{\tau'}$ son isomorfos como variedades abelianas polarizadas.

Parte 2. Variedades abelianas: Geometría

Por varias razones queremos poder utilizar variedades abelianas sobre cualquier cuerpo K. Si la característica de K es cero, podemos en parte utilizar el *principio de Lefschetz*. Si A es definida sobre K entonces es definida sobre un subcuerpo $K_0 \subset K$, que es de tipo finito sobre $\mathbb{Q}$, y se puede considerar una inyección $K_0 \hookrightarrow \mathbb{C}$ y considerar A como una variedad abeliana compleja. Sin embargo este principio es inaplicable cuando la característica de K es positiva, por ejemplo cuando K es un cuerpo finito. Además cuando, por ejemplo, K es un cuerpo de números, queremos guardar las propiedades aritméticas, es decir que $A(K)$ es un grupo (lo que no es obvio si se mira $A(K)$ como un subconjunto de $A(\mathbb{C})$) y, por ejemplo, considerar la acción del grupo de Galois $G_K := \mathrm{Gal}(\bar{K}/K)$ sobre $A(\bar{K})$. Veremos que se puede recuperar algebraicamente casi toda la geometría compleja como dualidad, formas de Riemann, con estructuras más ricas.

Aviso. *Esta parta requiere algún entendimiento del vocabulario básico de geometría algebraica: variedades, cuerpo de funciones de una variedad, morfismos, dimensión, puntos lisos y singulares, divisores (Weil, Cartier) y fibrados (en líneas) tal como están presentados por ejemplo en los dos primeros capítulos de* [5]. *Naturalmente, durante la presentación podremos dar algunos detalles sobre estas nociones.*

8. Grupos algebraicos

Repetimos en el contexto de la geometría algebraica la definición vista en el inicio del curso.

Definición 8.1. Un *grupo algebraico* sobre un cuerpo K es una variedad algebraica G junto con morfismos definidos sobre K, multiplicación $m_G : G \times_K G \to G$, inversión $\mathrm{inv}_G : G \to G$ y un elemento $e \in G(K)$ que satisfacen los axiomas de grupos usuales.

Una *variedad abeliana* definida sobre un cuerpo K es un grupo algebraico sobre el cuerpo K que, además, es una variedad proyectiva.

Observamos que la estructura de grupo algebraico produce aplicaciones naturales:

- traslaciones por un elemento $x \in G$ que denotamos $t_x : G \to G$ (cuando G no es conmutativo, por supuesto, hay dos tipos : traslaciones a la derecha y a la izquierda); la aplicación t_x es biyectiva con inverso $t_{\mathrm{inv}_G(x)}$.
- La "multiplicación por $[n]$" es definida inductivamente por $[0](x) = e_G$, $[1](x) = x$, $[-1](x) = \mathrm{inv}_G(x)$ y finalmente la relación de recurrencia $[n](x) = m_G(x, [n-1](x))$. Observamos que $[n]$ es un homomorfismo sólo cuando G es conmutativo. Sin embargo en todos casos la diferencial $d[n]_{e_G} : \mathrm{Tan}_{e_G}(G) \to \mathrm{Tan}_{e_G}(G)$ es simplemente la multiplicación por n, así observamos que, cuando n es coprimo con la característica del cuerpo K, la aplicación $[n]_G : G \to G$ define un morfismo finito separable y en particular sobreyectivo.

Ejemplo 8.2. Es fácil dar ejemplos de variedades afines con una ley de grupo.

1. (Grupo $\mathbb{G}_a$) La línea afín $G := \mathbb{A}^1$ con la adición $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$, el elemento $0 \in \mathbb{A}^1(K)$ y la aplicación $\mathrm{inv}(x) = -x$ es un grupo algebraico afín.
2. (Grupo $\mathbb{G}_m$) La línea afín pinchada $G := \mathbb{A}^1 \backslash \{0\}$ con la multiplicación $G \times G \to G$ definida por $(x, y) \mapsto xy$, el elemento $1 \in G(K)$ y la aplicación $\mathrm{inv}(x) = x^{-1}$ es un grupo algebraico afín.
3. (Grupo GL_n) La variedad afín de las matrices de tamaño $n \times n$ con determinante no nulo $G := \mathbb{A}^{n^2} \backslash \{\det = 0\}$ con la multiplicación de matrices $G \times G \to G$, el elemento identidad $I_n \in G(K)$ y la aplicación $\mathrm{inv}(M) = M^{-1}$ es un grupo algebraico afín. Otros ejemplos pueden ser dados como subgrupo de GL_n: grupo especial SL_n, grupo simpléctico, grupo ortogonal, etc. Debido a su importancia para las variedades abelianas, detallamos el ejemplo del grupo de las *similitudes simplécticas*. Denotamos $J_g = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ la matriz antisimétrica de tamaño $2g \times 2g$ y definimos

$$\mathrm{GSp}_{2g} := \left\{ M \in \mathrm{GL}_{2g} \mid \exists \mu = \mu(M) \in \mathbb{G}_m, \text{ tal que } {}^t M J M = \mu J \right\}$$

Este grupo puede ser colocado en una sucesión exacta

$$0 \to \mathrm{Sp}_{2g} \to \mathrm{GSp}_{2g} \xrightarrow{\mu} \mathbb{G}_m \to 0,$$

donde Sp_{2g} es el subgrupo de isometrías simplécticas (que cumplen $\mu(M) = 1$).

Ejemplo 8.3. Es más difícil construir ejemplos de grupos algebraicos proyectivos. El primer ejemplo de grupo algebraico proyectivo es una curva elíptica, o sea, una curva de género 1 con un punto marcado. Veremos que una curva de género $g \geqslant 2$ corresponde a una variedad abeliana de dimensión g, su jacobiana.

1. (curvas elípticas [6, 14, 15]) Se puede representar como una cúbica plana; damos la ecuación cuando la característica del cuerpo K es diferente de 2 y 3:

$$E = \{(x, y, z) \in \mathbb{P}^2 \mid zy^2 = x^3 + axz^2 + bz^3\}$$

con la condición para que la curva sea lisa $\Delta := 4a^3 - 27b^2 \neq 0$. El elemento neutro es el "punto en el infinito" $(0, 1, 0)$ el inverso es dado por $[-1](x, y, z) = (x, -y, z)$ y se puede describir la adición con la regla: $P + Q + R = 0$ si y sólo si P, Q, R estén alineados.
2. El producto de dos variedades abelianas es claramente una variedad abeliana. En particular, si $E_1, \ldots, E_g$ son curvas elípticas, el producto $E_1 \times \cdots \times E_g$ es una variedad abeliana de dimensión g.

3. (Jacobianas de dimensión 2 [7, 12]) Veremos que se puede asociar a cada curva de género g una variedad abeliana (un grupo algebraico proyectivo) de dimensión g, llamada *jacobiana*. La descripción en el caso $g = 2$ puede ser dada concretamente. Una curva de género 2 es siempre hiperelíptica, es decir existe un morfismo finito de grado dos $\pi : C \to \mathbb{P}^1$ con una involución canónica $\iota : C \to C$ tal que $\pi \circ \iota = \pi$ (si la curva es dada por una ecuación $y^2 = f(x)$ la involución canónica es simplemente $\iota(x, y) = (x, -y)$). Consideramos la superficie $X = C \times C/\mathcal{S}_2$ cociente de $C \times C$ por el grupo $\mathcal{S}_2$ generado por $\sigma(P_1, P_2) = (P_2, P_1)$. Los puntos de la superficie X pueden identificarse con divisores efectivos de grado 2 sobre C; la superficie contiene la curva $L = \{[(P, \iota(P))] \mid P \in C\}$ que es isomorfa a $\mathbb{P}^1$ y se puede contractar[11] en un punto $\pi : X \to J$; más precisamente si $0 \in J$ es el punto tal que $\pi(L) = \{0\}$, la aplicación π es un isomorfismo de $X\backslash L$ sobre $J\backslash\{0\}$ que manda L sobre el punto 0. La variedad algebraica J es una variedad abeliana, se puede definir una ley de grupo así. Escogemos 0 como elemento neutro y denotamos $D_0 = [(P, \iota(P)]$ un divisor que lo representa, para D_1, D_2 divisores efectivos de grado 2 existe un divisor efectivo D_3 tal que $D_1 + D_2 \sim D_3 + D_0$ y se define $[D_1] + [D_2] := [D_3]$; en general D_3 es único (salvo cuando $D_3 \sim D_0$). El inverso se obtiene con $\mathrm{inv}([D]) = [\iota(D)]$.

Lema 8.4. *(Lema de rigidez) Sea X variedad proyectiva, Y, Z variedades algebraicas y $f : X \times Y \to Z$ un morfismo. Si f es constante sobre un trozo $X \times \{y_0\}$, entonces es constante sobre todo trozo $X \times \{y\}$. Si además f es constante sobre un trozo $\{x_0\} \times Y$, entonces f es constante.*

Demostración. Ver [7] Lemma A.7.1.1 o [11] p.43. □

Observamos que la proyectividad de X es esencial para el lema. Por ejemplo la aplicación $f : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ definida por $f(x, y) = xy$ es constante sobre $\mathbb{A}^1 \times \{0\}$ y $\{0\} \times \mathbb{A}^1$ pero no es constante. La primera consecuencia es el siguiente teorema que corresponde, sobre $\mathbb{C}$, a la Proposición 2.2.

Teorema 8.5. *Una variedad abeliana es un grupo algebraico conmutativo. Más generalmente un morfismo $\phi : A \to B$ entre dos variedades abelianas que cumple que $\phi(e_A) = e_B$ es un homomorfismo.*

Demostración. Sea $\phi : A \to B$, introducimos $f(x, y) = \phi(xy)\,\mathrm{inv}_B(\phi(y))\,\mathrm{inv}_B(\phi(x))$. Observamos que $f(e_A, y) = \phi(e_A y)\,\mathrm{inv}_B(\phi(y))\,\mathrm{inv}_B(\phi(e_A)) = \phi(y)\,\mathrm{inv}_B(\phi(y)) = e_B$ e igualmente $f(x, e_A) = e_B$. El lema de rigidez implica que $f(x, y) = e_B$ y entonces que ϕ es un homomorfismo: $\phi(xy) = \phi(x)\phi(y)$. Aplicando esto a $\phi = \mathrm{inv}_A$, vemos que para todos x, y tenemos $\mathrm{inv}_A(xy) = \mathrm{inv}_A(x)\,\mathrm{inv}_A(y)$, lo que es posible sólo si A es conmutativo. □

Teorema 8.6. *(Weil) Sean X una variedad lisa y A una variedad abeliana, sean U un subconjunto abierto no vacío (denso) de X y $\phi : U \to A$ un morfismo. Entonces se puede extender ϕ a un morfismo de X hacia A.*

Demostración. Ver [7] Corollary A.7.1.4. □

La importancia de este resultado viene del hecho que una inclusión de cuerpos de funciones $i : K(A) \hookrightarrow K(X)$ induce automáticamente un morfismo $f : X \to A$ tal que $f^* = i$, y no sólo una aplicación racional.

[11] Para verificar este punto, invocamos el criterio de Castelnuovo ([5], Theorem 5.7 p. 414) y verificamos que L es una recta $\cong \mathbb{P}^1$ con auto-intersección $L \cdot L = -1$, ver ejercicio 1.

9. Fibrados en líneas sobre variedades abelianas

Empezamos con dos resultados generales describiendo fibrados en líneas sobre productos de variedades proyectivas. Como sólo usaremos "fibrados en líneas", después de un tiempo hablaremos simplemente de "fibrados".

Teorema 9.1. *(Teorema del subibaja) Sean X, Y variedades y $\mathcal{L}$, sea un fibrado en líneas sobre $X \times Y$. Denotamos p_1, p_2 las dos proyecciones de $X \times Y$ y para cada $x \in X$ (resp. $y \in Y$), denotamos $i_x(y) = (x, y)$ (resp. $j_y(x) = (x, y)$). Suponemos que para cada $x \in X$, tenemos $i_x^*\mathcal{L}$ es trivial, entonces existe $\mathcal{M}$, un fibrado en líneas sobre X tal que $\mathcal{L} = p_1^*\mathcal{M}$. Si, además, existe $y_0 \in Y$ tal que $j_y^*\mathcal{L}$ sea trivial, entonces $\mathcal{L}$ es trivial.*

Demostración. Ver [7] Lemma A.7.2.3 o [11] Corollary 6, p. 54. □

Teorema 9.2. *(Teorema del cubo abstracto) Sean X, Y, Z tres variedades proyectivas y x_0, y_0, z_0 puntos sobre ellas. Sea $\mathcal{L}$ un fibrado sobre $X \times Y \times Z$ con la propiedad de tornarse trivial cuando se le restringe a $\{x_0\} \times Y \times Z$, $X \times \{y_0\} \times Z$, $X \times Y \times \{z_0\}$, entonces $\mathcal{L}$ es trivial sobre $X \times Y \times Z$.*

Demostración. Ver [11] p. 55. □

Se deduce fácilmente.

Teorema 9.3. *(Teorema del cubo para variedades abelianas) Sea A una variedad abeliana y $\mathcal{L}$ un fibrado sobre A. Para cada subconjunto $I \subset \{1, 2, 3\}$ denotamos $s_I(x_1, x_2, x_3) = \sum_{i \in I} x_i$. El siguiente fibrado es trivial sobre $A \times A \times A$:*

$$\sum_{I \neq \emptyset} (-1)^{|I|} s_I^*\mathcal{L} = 0.$$

Demostración. Llamamos $Cubo(\mathcal{L})$ al miembro izquierdo de la última igualdad. Aplicamos Teorema 11.2 mostrando que $Cubo(\mathcal{L})$ restringido a $A \times A \times \{0\}$ es trivial; notando simetrías tendremos también que $Cubo(\mathcal{L})$ es trivial sobre los dos trozos $A \times \{0\} \times A$ y $\{0\} \times A \times A$. Si denotamos $i(x, y) = (x, y, 0)$ tenemos $s_{123} \circ i = s_{12} \circ i$ y también $s_{23} \circ i = s_2 \circ i$, $s_{12} \circ i = s_1 \circ i$ y $s_3 \circ i = 0$; así la fórmula deseada cumple

$$i^*(cubo(\mathcal{L})) = i^*(s_{12}^*\mathcal{L} - s_{12}^*\mathcal{L} - s_2^*\mathcal{L} - s_1^*\mathcal{L} + s_1^*\mathcal{L} + s_2^*\mathcal{L}) = 0.$$

□

Corolario 9.4. *Sea f, g, h tres morfismos de X hacia una variedad abeliana A y $\mathcal{L}$ un fibrado sobre A. El siguiente fibrado es trivial sobre X:*

$$(f + g + h)^*\mathcal{L} - (f + g)^*\mathcal{L} - (g + h)^*\mathcal{L} - (f + h)^*\mathcal{L} + f^*\mathcal{L} + g^*\mathcal{L} + f^*\mathcal{L} = 0.$$

Demostración. Considerando $(f, g, h) : X \to A^3$, la igualdad anterior es equivalente a $(f, g, h)^*(cubo(\mathcal{L})) = 0$. □

Aplicando Corolario 11.4 con $X = A$ y las aplicaciones $f = [n]$, $g = [1] = id_A$, $h = [-1]$, obtenemos

$$[n]^*\mathcal{L} - [n + 1]^*\mathcal{L} - [0]^*\mathcal{L} - [n - 1]^*\mathcal{L} + [n]^*\mathcal{L} + \mathcal{L} + [-1]^*\mathcal{L} = 0.$$

Por inducción deducimos

Lema 9.5. *(Mumford) Sea $\mathcal{L}$ un fibrado sobre una variedad abeliana A. Tenemos:*

$$[n]^*\mathcal{L} = \frac{n^2 + n}{2}\mathcal{L} + \frac{n^2 - n}{2}[-1]^*\mathcal{L}. \tag{9.1}$$

En particular si $\mathcal{L}$ es simétrico (es decir $[-1]^*\mathcal{L} = \mathcal{L}$) tendremos

$$[n]^*\mathcal{L} = \mathcal{L}^{n^2}. \tag{9.2}$$

Si $\mathcal{L}$ es antisimétrico (es decir $[-1]^*\mathcal{L} = \mathcal{L}^{-1}$) tendremos

$$[n]^*\mathcal{L} = \mathcal{L}^n. \tag{9.3}$$

Para el corolario siguiente utilizamos la noción de número de intersección de n divisores (o fibrados) sobre una variedad proyectiva de dimensión n.

Corolario 9.6. *Sea A una variedad abeliana de dimensión g; la multiplicación $[n]_A$ es un morfismo finito de grado n^{2g}.*

Demostración. Escogemos un fibrado amplio $\mathcal{L}$, el número de intersección $\mathcal{L}^g := (\mathcal{L} \cdot \cdots \cdot \mathcal{L}) > 0$ y calculamos $(([n]^*\mathcal{L})^g) = ((n^2\mathcal{L})^g) = n^{2g}(\mathcal{L}^g) = \deg([n])(\mathcal{L}^g)$. □

Con respecto a traslaciones, la propiedad más importante es la siguiente.

Teorema 9.7. *(Teorema del cuadrado) Sea A una variedad abeliana y $\mathcal{L}$ un fibrado sobre A. La aplicación $\phi_{\mathcal{L}} : A \to \mathrm{Pic}(A)$ definida por $\phi_{\mathcal{L}}(x) := t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ es un homomorfismo de grupos.*

Demostración. Sigue de aplicar Corolario 11.4 con $f(x) = x$, $g(x) = a$ y $h(x) = b$. □

Definición 9.8. El grupo $\mathrm{Pic}^0(A)$ es el subgrupo de los $\mathcal{L} \in \mathrm{Pic}(A)$ tales que $\phi_{\mathcal{L}} = 0$.

Observamos que, utilizando el teorema del cuadrado, vemos que $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \in \mathrm{Pic}^0(A)$. En particular el homomorfismo $\phi_{\mathcal{L}}$ toma valores en $\mathrm{Pic}^0(A)$.

Proposición 9.9. *Un fibrado $\mathcal{L}$ es antisimétrico, i.e. $[-1]^*\mathcal{L} = \mathcal{L}^{-1}$, si y sólo si*

$$s_{1,2}^*\mathcal{L} = p_1^*\mathcal{L} + p_2^*\mathcal{L} \text{ en } \mathrm{Pic}(A \times A), \tag{9.4}$$

si y sólo si $\mathcal{L} \in \mathrm{Pic}^0(A)$, es decir si $K(\mathcal{L}) = A$.

Un fibrado $\mathcal{L}$ es simétrico, i.e. $[-1]^*\mathcal{L} = \mathcal{L}$, si y sólo si

$$s_{1,2}^*\mathcal{L} + d_{1,2}^*\mathcal{L} = 2p_1^*\mathcal{L} + 2p_2^*\mathcal{L} \text{ en } \mathrm{Pic}(A \times A)$$

donde se usó las notaciones $s_{1,2}(x_1, x_2) = x_1 + x_2$, $d_{1,2}(x_1, x_2) = x_1 - x_2$ y $p_i(x_1, x_2) = x_i$.

Demostración. Ver [7] Proposition A.7.3.2, A.7.3.3. □

10. Polarización, isogenía, variedad dual

Recordamos que, en el "mundo" de la característica p, una extensión finita de cuerpos L/K se descompone en una parte separable y una parte inseparable. De la misma manera un morfismo finito $\phi : X \to Y$ se descompone en una parte separable y una parte inseparable y tenemos $\deg \phi = \deg_{sep} \phi . \deg_{insep} \phi$. La definición siguiente corresponde, sobre $\mathbb{C}$, a la Definición 2.5.

Definición 10.1. Una isogenía $\alpha : A \to B$ entre dos variedades abelianas es un homomorfismo que cumple:

- El núcleo de α es finito.
- El homomorfismo α es sobreyectivo.
- Tenemos $\dim A = \dim B$.

Definición 10.2. El grado de una isogenía $\alpha : A \to B$ es su grado como morfismo finito, es decir $\deg(\alpha) = [K(A) : \alpha^*(K(B))]$. Cuando la isogenía es separable $\deg(\alpha) = |(\ker \alpha)(\bar{K})|$; en el caso general, si p^e es el grado de inseparabilidad de la extensión $K(A)/\alpha^*(K(B))$, tenemos $\deg(\alpha) = p^e|(\ker \alpha)(\bar{K})|$.

De hecho dos de las tres propiedades implican la tercera. El principal ejemplo de isogenía es la multiplicación por un entero $n \neq 0$, pero un otro ejemplo clave es el llamado *Frobenius* que sólo existe en característica p.

Definición 10.3. Sea X una variedad (proyectiva) definida sobre un cuerpo K de característica p. El *Frobenius* de X es el morfismo definido en coordenadas por

$$\mathrm{Frob}_X(x_0, \ldots, x_n) := (x_0^p, \ldots, x_n^p)$$

Su imagen es una variedad también definida sobre K y denotada $X^{(p)}$.

Observación 10.4. La definición no depende de las coordenadas; además si X es definida sobre el cuerpo finito $\mathbb{F}_p$, tenemos $X^{(p)} = X$. El Frobenius es el ejemplo tipo de morfismo inseparable, es decir que la extensión $K(X)/\operatorname{Frob}_X^*(K(X^{(p)}))$ es una extensión finita *puramente inseparable* (de grado $p^{\dim X}$). Observamos que la diferencial $(d\operatorname{Frob}_X)_x : \tan_x(X) \to \tan_{\operatorname{Frob}_X(x)}(X^{(p)})$ es la aplicación nula.

Teorema 10.5. *Sea A una variedad abeliana de dimensión g sobre un cuerpo K. Para todo $n \neq 0$ la multiplicación $[n] = [n]_A$ es una isogenía de grado* $\deg[n] = n^{2g}$.

- *Si* $\operatorname{car}(K) = 0$ *o* $\operatorname{car}(K) = p$ *no divide n, entonces* $\ker[n](\bar{K}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.
- *Si* $\operatorname{car}(K) = p$, *existe $r = r_A \in [0, g]$ tal que* $\ker[p^m](\bar{K}) \cong (\mathbb{Z}/p^m\mathbb{Z})^r$. *El entero r_A se llama el p-rango de A.*

Demostración. Utilizaremos el siguiente lema elemental de grupos (Ejercicio).

"*Un grupo conmutativo de cardinal n^r y tal que para todo m divisor de n, el cardinal de los elementos cancelados por m es igual a m^r es necesariamente isomorfo a $(\mathbb{Z}/n\mathbb{Z})^r$*"

Esta observación es suficiente cuando $p = \operatorname{car}(K)$ no divide n, porque entonces la diferencial es inyectiva y la isogenía es separable. Cuando $n = p = \operatorname{car}(K)$ la diferencial es nula y se puede deducir que $[p]$ se factoriza a través del Frobenius, es decir existe una otra isogenía $V : A^{(p)} \to A$ tal que $[p] = V \circ \operatorname{Frob}_A$. [12] De hecho el homomorfismo de cuerpos $K(A) \to K(A)$ dado por $f \mapsto f \circ [p]$ tiene imagen contenida en $K(A)^p = K(A^{(p)})$ y obtenemos una inyección $K(A) \to K(A^{(p)})$ que corresponde a un aplicación racional $V : A^{(p)} \to A$ tal que $V \circ \operatorname{Frob} = [p]$. Además el Teorema 10.6 nos dice que V es un morfismo. Tenemos $p^{2g} = \deg[p] = \deg V \deg \operatorname{Frob}_A = p^g \deg V$, así $\deg V = p^g$. Suponemos que $\deg_{\mathrm{insep}} V = p^s$, con $s \in [0, g]$ entonces $\deg_{\mathrm{insep}}[p] = p^{s+g}$ y $\ker[p](\bar{K})$ tiene p^{g-s} elementos. El teorema sigue con $r = g - s$. □

Notación 10.6. Denotaremos $A[n]$ al grupo finito $\ker[n]_A(\bar{K})$ de puntos de torsión cancelados por n.

El lema siguiente contiene el hecho que, como sobre $\mathbb{C}$ (Lema 2.8) la relación de isogenía es simétrica y también que una isogenía es "invertible después de tensorizar por $\mathbb{Q}$".

Lema 10.7. *Sea $\phi : A \to B$ una isogenía de grado d entre variedades abelianas definidas sobre K. Entonces existe otra isogenía $\hat{\phi} : B \to A$ tal que $\hat{\phi} \circ \phi = [d]_A$ y $\phi \circ \hat{\phi} = [d]_B$.*

Demostración. Damos la prueba cuando la característica de K no divide d. Tenemos claramente en este caso $\ker \phi \subset A[d]$. La imagen del homomorfismo de cuerpos $K(A) \to K(A)$ dado por $f \mapsto f \circ [d]$ se puede identificar con $K(A)^{\ker[d]}$ (el subcuerpo fijado por los elementos de $\ker[d]$ actuando por traslaciones). De la misma manera, el homomorfismo de cuerpos $K(B) \to K(A)$ dado por $h \mapsto h \circ \phi$ permite identificar $K(B)$ con $K(A)^{\ker \phi}$. Observamos que $K(A) \cong K(A)^{\ker[d]} \subset K(A)^{\ker \phi} \cong K(B)$. Ahora esta aplicación corresponde a una inyección $h \mapsto h \circ \hat{\phi}$ por una aplicación racional $\hat{\phi} : B \to A$; además $\hat{\phi}$ es un morfismo gracias a Teorema 10.6. Por construcción tenemos $\hat{\phi} \circ \phi = [d]_A$ entonces $\phi \circ \hat{\phi} \circ \phi = \phi \circ [d]_A = [d]_B \circ \phi$. Así, como ϕ es sobreyectiva, vemos que $\phi \circ \hat{\phi} = [d]_B$. □

Definición 10.8. Si $\mathcal{L}$ es un fibrado en líneas sobre una variedad abeliana A, denotamos $K(\mathcal{L})$ el núcleo del homomorfismo $\phi_{\mathcal{L}} : A \to \mathrm{Pic}^0(A)$ dado por $\phi_{\mathcal{L}}(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$.

[12] La letra "V" es tradicional y corresponde a la palabra alemana *Verschiebung*.

Teorema 10.9. *Sea $\mathcal{L}$ un fibrado en líneas, amplio sobre una variedad abeliana A, el grupo $K(\mathcal{L})$ es finito.*

Demostración. Ver [7] Theorem A.7.2.10 o [11] (consecuencia del) Theorem 1, p.77. □

Enunciamos ahora la versión algebraica de la variedad abeliana dual (Cf. Subsección 4.2 sobre $\mathbb{C}$).

Definición 10.10. Una variedad abeliana *dual* de A es una variedad abeliana B con un fibrado (llamado fibrado de Poincaré) $\mathcal{P} \in \mathrm{Pic}(A \times B)$ que verifica que los dos homomorfismos:

$$\begin{array}{ccc} B & \longrightarrow & \mathrm{Pic}^0(A) \\ b & \longmapsto & j_b^*\mathcal{P} \end{array} \quad \text{y} \quad \begin{array}{ccc} A & \longrightarrow & \mathrm{Pic}^0(B) \\ a & \longmapsto & i_a^*\mathcal{P} \end{array}$$

son biyecciones (donde $j_b(a) = (a, b) = i_a(b)$).

Teorema 10.11. *La variedad abeliana dual de A existe y es única (salvo isomorfismo); es denotada $\check{A}$.*

Demostración. Ver [11] Chapter III.13. □

Cuando $\mathcal{L}$ es amplio, se puede construir $\check{A}$ como el cociente $A/K(\mathcal{L})$. En el caso $K(\mathcal{L}) = 0$, quien corresponde a una *polarización principal*, tenemos $A \cong \check{A}$ y el divisor (fibrado) de Poincaré se puede describir como $\mathcal{P} = s_{12}^*\mathcal{L} - p_1^*\mathcal{L} - p_2^*\mathcal{L}$.

En general $\check{A}$ no es isomorfa a A pero se tiene isogenías particulares que se llama *polarizaciones* $\lambda : A \to \check{A}$ que son de la forma $\lambda = \phi_{\mathcal{L}}$ para un fibrado amplio $\mathcal{L}$. Se puede demostrar que λ es simétrica en el sentido que $\check{\lambda} = \lambda$.

Identificando $\check{A}$ y $\mathrm{Pic}^0(A)$, se puede definir el dual de un homomorfismo $\alpha : A \to B$ como la composición de los homomorfismos:

$$\check{\alpha} : \check{B} \cong \mathrm{Pic}^0(B) \xrightarrow{\alpha^*} \mathrm{Pic}^0(A) \cong \check{A}.$$

Podemos ahora demostrar la versión algebraica del teorema de reducibilidad de Poincaré (cf. sobre $\mathbb{C}$, Teorema 2.15).

Teorema 10.12. *(Teorema de reducibilidad de Poincaré) Si B es una subvariedad abeliana de A definida sobre K, existe C una subvariedad abeliana de A también definida sobre K tal que $B \cap C$ es finito y $s(b, c) = b + c$ define una isogenía $s : B \times C \to A$.*

Demostración. Sea $i : B \hookrightarrow A$ la inyección; escogemos $\mathcal{L}$ amplio sobre A y consideramos la isogenía $\phi_{\mathcal{L}} : A \to \check{A}$. Definimos C como el componente conexo del núcleo de $\check{\imath} \circ \phi_{\mathcal{L}}$. Tenemos $\dim C = \dim(\ker \check{\imath}) \geqslant \dim \check{A} - \dim \check{B} = \dim A - \dim B$. Si $x \in B \cap C$ entonces $0 = \check{\imath} \circ \phi_{\mathcal{L}}(x) = \check{\imath}(t_x^*\mathcal{L} \otimes \mathcal{L}^{-1})$; si denotamos $\mathcal{L}_B$ la restricción de $\mathcal{L}$ a B o sea $i^*(\mathcal{L})$ entonces tenemos $t_x^*\mathcal{L}_B \otimes \mathcal{L}_B^{-1} = 0$ que se puede traducir por $x \in K(\mathcal{L}_B)$. Observamos que $\mathcal{L}_B$ es amplio sobre B y entonces $K(\mathcal{L}_B)$ es finito (por Teorema 12.9). Terminamos concluyendo que $s : B \times C \to A$ tiene un núcleo finito y por consecuencia $\dim s(B \times C) = \dim B + \dim C \geqslant \dim A$; así tenemos igualdad y s es sobreyectiva. □

11. Representaciones de Galois

En esta sección denotamos $G_K := \mathrm{Gal}(\bar{K}/K)$ el grupo de Galois absoluto de un cuerpo K. Este grupo, para digamos K cuerpo de números, es demasiado grande para ser controlado en su totalidad y se le estudia a través de sus representaciones.

Definición 11.1. Sea G_i una familia de grupos (resp. módulos, resp. anillos) con homomorfismos $\psi_i : G_{i+1} \to G_i$. El límite proyectivo es el grupo (resp. módulo, resp. anillo)

$$\varprojlim G_i := \left\{ (g_i)_i \in \prod_i G_i \mid \forall i,\ \psi_i(g_{i+1}) = g_i \right\}$$

Utilizaremos los siguientes ejemplos claves:

- El anillo de los enteros p-ádicos se obtiene como
$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$
donde los morfismos son las proyecciones $\psi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ que mandan la clase de x módulo p^{n+1} sobre su clase módulo p^n.
- El *módulo de Tate* de una variedad abeliana que se define como
$$T_p(A) = \varprojlim A[p^n],$$
donde $\psi_n : A[p^{n+1}] \to A[p^n]$ es la multiplicación por p. Como grupo tenemos $T_p(A) \cong \mathbb{Z}_p^{2\dim A}$, mientras $p \neq \mathrm{car}(K)$.
- Si μ_{ℓ^n} es el grupo de la raíces ℓ^n-ésimas de la unidad (para ℓ distinto de la característica), podemos definir análogamente
$$T_\ell(\mathbb{G}_m) := \varprojlim \mu_{\ell^n}$$

Para cada n coprimo con la característica de K, el grupo G_K actúa sobre el grupo $\ker[n](\bar{K})$ a través de un cociente finito (de hecho a través de $\mathrm{Gal}(K(A[n])/K)$), así obtenemos la representación :
$$\rho_{A,n} : G_K \to \mathrm{GL}(2g, \mathbb{Z}/n\mathbb{Z})$$
Tomando límites inductivos sobre ℓ^n (donde ℓ es primo distinto a $p = \mathrm{car}(K)$) obtenemos
$$\rho_{A,\ell^\infty} : G_K \to \mathrm{GL}(T_\ell(A)) \cong \mathrm{GL}(2g, \mathbb{Z}_\ell)$$

Sea $a \in A[m]$ y $\check{a} \in \check{A}[m]$, escogemos D divisor sobre A tal que la clase de D sea $\check{a} \in \mathrm{Pic}^0(A)$, entonces existe $f \in K(A)^\times$ tal que $\mathrm{div}(f) = mD$. Tomando imágenes por $[m]^*$ vemos que $\mathrm{div}(f \circ [m]) = [m]^* \mathrm{div}(f) = m([m]^* D) = m(mD + \mathrm{div}(h)) = m\,\mathrm{div}(fh)$, es decir que, ajustando constantes, existe $g \in K(A)^\times$ tal que $f \circ [m] = g^m$. Esto permite definir:

$$e_m : A[m] \times \check{A}[m] \longrightarrow \mu_m, \quad \text{por} \quad e_m(a, \check{a}) = \frac{g(x+a)}{g(x)}, \tag{11.1}$$

observando que $e_m(a,\check{a})^m = \left(\frac{g(x+a)}{g(x)}\right)^m = \frac{f\circ[m](x+a)}{f\circ[m](x)} = 1$ y entonces $\frac{g(x+a)}{g(x)}$ es constante (independiente de x) y es una raíz m-ésima de la unidad. Las aplicaciones e_m verifican:

Teorema 11.2. *(Emparejamiento[13] de Weil) Las aplicaciones $e_m : A[m] \times \check{A}[m] \longrightarrow \mu_m$ son bilineales y cumplen:*

1. *El emparejamiento e_m es no degenerado (núcleo trivial a la derecha y izquierda).*
2. *(Compatibilidad) Tenemos la relación $e_n(ma, m\check{a}) = (e_{mn}(a,\check{a}))^m$, lo que permite extender los e_{ℓ^n} a un emparejamiento*
$$e_{\ell^\infty} : T_\ell(A) \times T_\ell(\check{A}) \to T_\ell(\mathbb{G}_m).$$
3. *(Galois equivariancia) Sea $\sigma \in G_K$ entonces*
$$e_m(\sigma(a), \sigma(\check{a})) = \sigma(e_m(a, \check{a})).$$
4. *Sea $\mathcal{L}$ un fibrado sobre A, entonces el emparejamiento*
$$e^{\mathcal{L}} : A[m] \times A[m] \to \mu_m, \qquad (a,b) \mapsto e_m(a, \phi_{\mathcal{L}}(b))$$
es antisimétrico.

Demostración. Ver [11] Proposition p.185–186. □

[13]En inglés *pairing*; en francés *accouplement*.

Observación 11.3. Como el emparejamiento es Galois equivariante, vemos que las representaciones ρ_n o ρ_{ℓ^∞}, a priori con valores en GL_{2g}, toman sus valores en GSp_{2g}.

Este emparejamiento nos permite "reconstruir" las formas de Riemann en un cuadro algebraico.

Definición 11.4. Sea $\mathcal{L}$ un fibrado sobre A, definimos un emparejamiento

$$e_\ell^{\mathcal{L}} : T_\ell(A) \times T_\ell(A) \longrightarrow \mathbb{Z}_\ell \tag{11.2}$$

por la fórmula

$$e_\ell^{\mathcal{L}}(x, y) = e_{\ell^\infty}(x, \phi_{\mathcal{L}}(y)). \tag{11.3}$$

Vínculo con las formas de Riemann sobre un toro complejo. Hemos visto que una variedad abeliana compleja de dimensión g se puede ver como un toro $A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ y que, a cada fibrado $\mathcal{L}$ (o divisor) amplio, corresponde una forma de Riemann que podemos describir como una aplicación bilineal antisimétrica:

$$E_{\mathcal{L}} : \Lambda \times \Lambda \longrightarrow \mathbb{Z}$$

En verdad, no conseguimos por completo recuperar algebraicamente $E_{\mathcal{L}}$, pero notando que, para una variedad abeliana compleja $A = \mathbb{C}^g/\Lambda$, tenemos $A[n] = \Lambda/n\Lambda$ y entonces

$$\varprojlim A[n] = \varprojlim \Lambda/n\Lambda = \Lambda \otimes_{\mathbb{Z}} \varprojlim \mathbb{Z}/n\mathbb{Z}, \quad \text{y} \quad T_\ell(A) = \varprojlim A[\ell^n] = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.$$

Así tenemos $T_\ell(A) \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ y finalmente podemos identificar

$$E_{\mathcal{L},\mathbb{Z}_\ell} : (\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell) \times (\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell) \longrightarrow \mathbb{Z}_\ell$$

con el emparejamiento de Weil (13.2). La acción del anillo $\mathrm{End}(A)$ sobre $T_\ell(A)$ nos da una inyección $\mathrm{End}(A) \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ (Ejercicio). Es un poco más sutil ver que eso induce una inyección $\mathrm{End}(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell(A)$ entonces $\dim \mathrm{End}(A) \leqslant 4(\dim A)^2$.

La involución de Rosati puede ser definida en este contexto : escogemos un fibrado amplio $\mathcal{L}$ y la polarización asociada $\phi_{\mathcal{L}} : A \to \check{A}$ y obtenemos

$$\alpha \in \mathrm{End}(A) \otimes \mathbb{Q} \mapsto \alpha^\dagger := \phi_{\mathcal{L}}^{-1} \circ \check{\alpha} \circ \phi_{\mathcal{L}} \in \mathrm{End}(A) \otimes \mathbb{Q}$$

Observamos que si $\phi_{\mathcal{L}}$ no es una polarización principal entonces $\phi_{\mathcal{L}}^{-1}$ sólo existe después de tensorizar con $\mathbb{Q}$.

Terminamos esta sección con un resultado mucho más difícil,

Teorema 11.5. *(Tate, Zarhin, Faltings) Sea K un cuerpo finito, un cuerpo de números o un cuerpo de tipo finito sobre ellos, y sean A, B variedades abelianas sobre K y p un primo distinto de la característica de K. El homomorfismo*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(T_p(A), T_p(B)) \tag{11.4}$$

es un isomorfismo.

12. Curvas y jacobianas

El ejemplo histórico de variedad abeliana es la jacobiana de una curva: el grupo de clases de divisores de grado cero $\mathrm{Pic}^0(C)$ tiene una estructura de grupo algebraico proyectivo. Admitiendo este hecho se pueden describir algunas propiedades de esta variedad abeliana que denotamos J_C y que se llama *jacobiana* de C. Escogiendo un punto "origen" P_0 tenemos el morfismo

$$j = j_{P_0} : C \to J_C, \quad \text{dado por } P \mapsto [(P) - (P_0)]$$

que se puede extender a un morfismo

$$j_r = j_{r,P_0} : C^r \to J_C, \quad \text{dado por } (P_1, \ldots, P_r) \mapsto [\sum_{i=1}^{r} (P_i) - r(P_0)].$$

Con la ayuda del teorema de Riemann-Roch (para la curva C), se puede ver que, cuando $g = g(C) \geqslant 1$, el morfismo j es una inmersión y que $W_r(C) := j_r(C^r)$ es una subvariedad de dimensión $\min(r, g)$. En particular tenemos el siguiente resultado clásico.

Teorema 12.1. *La jacobiana de una curva C de género g es una variedad abeliana de dimensión g; esta variedad abeliana está dotada de un divisor canónico (salvo traslaciones) $\Theta_C := W_{g-1} = j_{g-1}(C^{g-1})$, quien induce una polarización principal sobre J_C.*

Demostración. Ver [7] Theorem A.8.11. □

Sobre los complejos, la construcción clásica parece diferente. Si X es una curva lisa proyectiva definida sobre $\mathbb{C}$, entonces $X(\mathbb{C})$ es una superficie[14] de Riemann compacta. El espacio vectorial de las 1-formas diferenciales holomorfas $H^0(X(\mathbb{C}), \Omega^1_X)$ es de dimensión g, el grupo de homología singular (o de Betti) se denota $H^1(X(\mathbb{C}), \mathbb{Z}) \cong \mathbb{Z}^{2g}$ y los dos están vinculados por la integración

$$H^0(X(\mathbb{C}), \Omega^1_X) \times H^1(X(\mathbb{C}), \mathbb{Z}) \to \mathbb{C}, \quad (\omega, [\gamma]) \mapsto \int_\gamma \omega.$$

Esto nos permite ver a $H^1(X(\mathbb{C}), \mathbb{Z}) \cong \mathbb{Z}^{2g}$ como un retículo en el dual $H^0(X(\mathbb{C}), \Omega^1_X)^* \cong \mathbb{C}^g$. Las *relaciones de Riemann* (ver [7] Chapter A.6) entre los periodos permite demostrar

Teorema 12.2. *El toro complejo $H^0(X(\mathbb{C}), \Omega^1_X)^*/H^1(X(\mathbb{C}), \mathbb{Z})$ es una variedad abeliana, y la forma de Riemann canónicamente asociada induce una polarización principal.*

Notamos $J_X(\mathbb{C})$ este toro complejo; el lazo con la presentación algebraica es dada por el teorema de Abel-Jacobi: escogiendo un punto $P_0 \in X(\mathbb{C})$, se puede definir una inyección

$$j = j_{P_0} : X(\mathbb{C}) \to J_X(\mathbb{C}) \quad \text{dada por } \; j_{P_0}(P)(\omega) = \int_{P_0}^{P} \omega \quad \text{mód } H^1(X(\mathbb{C}), \mathbb{Z})$$

y extenderla a divisores.

Teorema 12.3. *(Teorema de Abel-Jacobi) Consideramos el morfismo j del grupo de los divisores de grado nulo $\mathrm{Div}^0(X)$ hacia $J_X(\mathbb{C})$, entonces j es sobreyectivo y el núcleo es compuesto por los divisores principales $\mathrm{div}(f)$. En particular, se puede identificar $J_X(\mathbb{C})$ y $\mathrm{Pic}^0(X)(\mathbb{C})$.*

En otra dirección, cuando la curva es definida sobre un cuerpo finito, hay una relación interesante entre el número de puntos sobre C y sobre J_C.

Teorema 12.4. *(Weil) Sea $C/\mathbb{F}_q$ una curva lisa proyectiva de género g. Existe enteros algebraicos $\alpha_1, \dots \alpha_{2g}$ tales que:*

1. *El conjunto de los α_i es estable por Galois y cada α_i verifica $|\alpha_i| = \sqrt{q}$; así el conjunto es permutado por $\alpha \mapsto q/\alpha$.*
2. *Para cada $m \geqslant 1$, tenemos $|C(\mathbb{F}_{q^m})| = q^m + 1 - \sum_{i=1}^{2g} \alpha_i^m$.*
3. *Tenemos $|J_C(\mathbb{F}_q)| = \prod_{i=1}^{2g}(\alpha_i - 1)$.*

13. Alturas de Néron-Tate y Teorema de Mordell-Weil

13.1. Buena reducción, criterio de Néron-Ogg-Shafarevich. Sea K un cuerpo de números y v una plaza finita, quien corresponde a un ideal primo $\mathfrak{p}_v$ y tiene cuerpo residual $\mathbb{F}_v := \mathcal{O}_K/\mathfrak{p}_v$. Podemos definir la *reducción* de puntos módulo $\mathfrak{p}_v$ o módulo v como

$$\mathrm{red}_v : \mathbb{P}^n(K) \to \mathbb{P}^n(\mathbb{F}_v), \qquad (x_0, \dots, x_n) \mapsto (\tilde{x}_0, \dots, \tilde{x}_n)$$

[14]El choque entre las palabras "curva" (objeto algebraico de dimensión 1 sobre $\mathbb{C}$) y "superficie". (objeto topológico de dimensión 2) es histórico y inevitable.

donde $\tilde{x}$ denota la imagen en $\mathbb{F}_v$ de un elemento $\mathfrak{p}_v$-entero de K, y se escoge coordenadas x_i, quienes son $\mathfrak{p}_v$-enteras tales que una de ellas sea una $\mathfrak{p}_v$-unidad.

Se puede también dar una primera noción ingenua de reducción de una variedad proyectiva. Si $X \subset \mathbb{P}^n$ es definida por un ideal $I_X \in K[x_0, \ldots, x_n]$, se define $\mathcal{I}_X = I_X \cap \mathcal{O}_K[x_0, \ldots, x_n]$ y finalmente

$$\tilde{\mathcal{I}}_X = \left\{ \tilde{F} \mid F \in \mathcal{I}_X \right\} \quad \text{y} \quad \tilde{X} = \left\{ x \in \mathbb{P}^n_{\mathbb{F}_v} \mid \forall \tilde{F} \in \mathcal{I}_X,\ \tilde{F}(P) = 0 \right\}$$

Con esta definición es más o menos claro que la aplicación de reducción de puntos es compatible, es decir que nos proporciona la aplicación

$$\mathrm{red}_v : X(K) \to \tilde{X}(\mathbb{F}_v). \tag{13.1}$$

Definición 13.1. Diremos que X tiene buena reducción en v si la reducción $\tilde{X}$ es lisa.

El defecto de esta definición es que la noción depende de la inmersión $X \hookrightarrow \mathbb{P}^n$, una definición mas intrínseca es que X tiene buena reducción si existe un modelo donde X tiene buena reducción en el sentido ingenuo. Con ambas definiciones el hecho más importante es el siguiente

Proposición 13.2. *Sea X una variedad proyectiva lisa definida sobre un cuerpo de números K. Existe un conjunto finito S de ideales primos de K, tal que para todo $\mathfrak{p}_v \notin S$, la variedad X tiene buena reducción en $\mathfrak{p}_v$.*

Demostración. Utilizando la caracterización de la propriedad de ser liso por el criterio de Jacobi, un punto es liso si un menor de tamaño adecuado de la matriz de la diferencial de las ecuaciones es no nulo; esta propiedad sigue siendo verdad para cada $\mathfrak{p}_v$ que no divide este determinante. □

Volvemos a las variedades abelianas. Si A es una variedad abeliana definida sobre K y tiene buena reducción en v, entonces $\tilde{A}_v$ es también una variedad abeliana (definida sobre $\mathbb{F}_v$) y el morfismo

$$\mathrm{red}_v : A(K) \to \tilde{A}_v(\mathbb{F}_v) \tag{13.2}$$

es un homomorfismo de grupos. Obviamente este homomorfismo no es en general inyectivo (Ejercicio)pero una propiedad importante tiene que ver con inyectividad.

Lema 13.3. *Sea $m \geqslant 2$ un entero y A una variedad abeliana definida sobre un cuerpo de números K. Sea $\mathfrak{p}_v$ un ideal primo de K que no divide m y donde A tiene buena reducción. El homomorfismo de reducción*

$$\mathrm{red}_v : A[m](K) \to A(\mathbb{F}_v)$$

es inyectivo.

Demostración. Ver [7] Theorem C.1.4. □

Observamos que el análogo para el grupo $\mathbb{G}_m$ puede ser demostrado de manera elemental.

Lema 13.4. *(Análogo del lema 15.3 para $\mathbb{G}_m$) Sea p y m coprimos. Sea $\mathbb{G}_m[m] = \mu_m$ el grupo de las raíces m-ésima de la unidad, $K = \mathbb{Q}(\mu_m)$ y $\mathfrak{p}$ un ideal de K con característica residual p. Entonces la reducción módulo $\mathfrak{p}$ es inyectiva sobre μ_m.*

Demostración. Sean $\zeta \neq \zeta'$ dos raíces m-ésimas de la unidad. Si $\zeta \equiv \zeta' \mod \mathfrak{p}$ tenemos también $1 - \zeta^{-1}\zeta' \equiv 0 \mod \mathfrak{p}$. Pero es elemental ver que si $\zeta'' \neq 1$ es una raíz de la unidad entonces $1 - \zeta''$ es una unidad o una p-unidad cuando el orden de ζ'' es una potencia de p. □

Volviendo a la noción intrínseca de buena reducción, tenemos la caracterización siguiente en términos de la representación sobre el módulo de Tate.

Teorema 13.5. *(Criterio de Néron-Ogg-Shafarevich) Una variedad abeliana A tiene buena reducción en v si y sólo si el subgrupo de inercia de v en G_K actúa trivialmente sobre $T_\ell(A)$.*

Demostración. Para el caso de las curvas elípticas, ver [14] Theorem 7.1. La prueba se adapta al caso general, utilizando los modelos de Néron de una variedad abeliana. □

13.2. Alturas de Weil. Cada cuerpo de números K es dotado de un conjunto de plazas: una plaza para cada ideal primo de K y una plaza para cada inmersión $\sigma : K \hookrightarrow \mathbb{R}$ o par de inmersión conjugada $\tau, \bar{\tau} : K \hookrightarrow \mathbb{C}$. Asociamos a cada plaza un valor absoluto $|\cdot|_v : K \to \mathbb{R}$, normalizando de manera que se cumple la fórmula siguiente, donde $n_v = [K_v : \mathbb{Q}_v]$ por un ideal primo y $n_v = 1$ (resp. $n_v = 2$) si v es real (resp. compleja):

Teorema 13.6. *(fórmula del producto) Para $\alpha \in K^\times$,*

$$\prod_{v \in M_K} |\alpha|_v^{n_v} = 1. \tag{13.3}$$

Definición 13.7. Sea $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(K)$, la altura (logarítmica) de Weil está dada por la fórmula:

$$h(P) := \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \log \max_{i=0}^{n} |x_i|_v. \tag{13.4}$$

Observamos que la definición no depende de las coordenadas proyectivas de P, gracias a la fórmula del producto (15.6). Además, $h(P)$ no depende del cuerpo de racionalidad de P, así podemos ver a h como una función $h : \mathbb{P}^n(\bar{\mathbb{Q}}) \to \mathbb{R}$. La propiedad importante más básica es la siguiente.

Teorema 13.8. *(Northcott) El conjunto siguiente es finito para todo $D \geqslant 1$, $T \geqslant 1$:*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) \mid h(P) \leqslant T \text{ y } [\mathbb{Q}(P) : \mathbb{Q}] \leqslant D\}.$$

En particular para un cuerpo de números K, vemos que el conjunto $\{P \in \mathbb{P}^n(K) \mid h(P) \leqslant T\}$ es finito.

Podemos extender la noción de alturas a variedades proyectivas considerando inmersiones $\phi : V \hookrightarrow \mathbb{P}^n$ y definiendo $h_\phi(P) := h_{\mathbb{P}^n}(\phi(P))$. Cuando $\mathcal{L}$ es un fibrado amplio sobre V, se puede asociar una inmersión $\phi_{\mathcal{L}} : V \hookrightarrow \mathbb{P}^n$ que es única sólo módulo una transformación lineal $\alpha \in \mathrm{PGL}_{n+1}$. El lema elemental siguiente muestra que eso no altera mucho las alturas (Ejercicio).

Lema 13.9. *Sea $\alpha \in \mathrm{PGL}_{n+1}$ un automorfismo $\alpha : \mathbb{P}^n \to \mathbb{P}^n$, existe una constante $C = C_\alpha$ tal que*

$$|h(\alpha(P)) - h(P)| \leqslant C.$$

Seja $\mathcal{L}$ un fibrado sobre una variedad proyectiva V, se puede escribir como la diferencia de dos fibrados muy amplios: $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2^{-1}$ y definir la altura asociada a $\mathcal{L}$ por

$$h_{\mathcal{L}}(P) = h_{\mathcal{L}_1}(P) - h_{\mathcal{L}_2}(P) = h(\phi_{\mathcal{L}_1}(P)) - h(\phi_{\mathcal{L}_2}(P)) \tag{13.5}$$

Observamos que $h_{\mathcal{L}}$ es única salvo una función acotada; se denota esto tradicionalmente con $h_{\mathcal{L}} = h'_{\mathcal{L}} + O(1)$. [15]

Teorema 13.10. *("Máquina de las alturas de Weil") A cada fibrado $\mathcal{L}$ sobre V variedad proyectiva, es asociada una altura $h_{\mathcal{L}} : V(\bar{Q}) \to \mathbb{R}$, única módulo funciones acotadas. Estas alturas verifican las propiedades siguientes:*

[15] El contexto y la tipografía permite distinguir entre el fibrado $\mathcal{O}(1)$ y la función acotada $O(1)$.

1. *(normalización) Sea $\mathcal{O}(1)$ el fibrado de Serre sobre $\mathbb{P}^n$, entonces*
$$h_{\mathcal{O}(1)} = h_{\mathbb{P}^n} + O(1)$$
2. *(aditividad) Si $\mathcal{L}$ y $\mathcal{M}$ son dos fibrados sobre V, entonces*
$$h_{\mathcal{L}\otimes\mathcal{M}} = h_{\mathcal{L}} + h_{\mathcal{M}} + O(1)$$
3. *(functorialidad) Sean $\phi : V \to W$ un morfismo de variedades proyectivas y $\mathcal{L}$ un fibrado sobre W, entonces*
$$h_{\mathcal{L}} \circ \phi = h_{\phi^*\mathcal{L}} + O(1)$$
4. *(positividad) Sea $\mathcal{L}$ un fibrado sobre V con secciones no nulas; denotamos Z el conjunto de los ceros comunes de todas las secciones, entonces*
$$\forall P \in V(\bar{\mathbb{Q}})\backslash Z, \quad h_{\mathcal{L}}(P) \geqslant -c.$$

Demostración. Ver [7] Chapter B, Theorems B.3.2, B.3.6. □

13.3. Alturas sobre variedades abelianas. Utilizando la máquina de las alturas de Weil y las relaciones entre fibrados sobre variedades abelianas obtenemos la fórmulas siguientes(Ejercicio).

Proposición 13.11. *Sean A una variedad abeliana y $\mathcal{L}$ un fibrado sobre ella.*

1. *Si $\mathcal{L}$ es simétrico, entonces*
$$h_{\mathcal{L}}([n](P)) = n^2 h_{\mathcal{L}}(P) + O(1)$$
y también
$$h_{\mathcal{L}}(P+Q) + h_{\mathcal{L}}(P-Q) = 2h_{\mathcal{L}}(P) + 2h_{\mathcal{L}}(Q) + O(1)$$
2. *Si $\mathcal{L}$ es antisimétrico, tenemos:*
$$h_{\mathcal{L}}([n](P)) = nh_{\mathcal{L}}(P) + O(1)$$
y también
$$h_{\mathcal{L}}(P+Q) = h_{\mathcal{L}}(P) + h_{\mathcal{L}}(Q) + O(1)$$

Demostración. Damos la prueba de la primera relación, mientras que las otras se demuestran de manera similar. Sigue de la functorialidad $h_{\mathcal{L}}([n](P)) = h_{[n]^*\mathcal{L}}(P) + O(1)$, y de las relaciones de fibrados y la aditividad $h_{[n]^*\mathcal{L}}(P) = h_{n^2\mathcal{L}}(P) = n^2 h_{\mathcal{L}}(P) + O(1)$. □

Estas relaciones nos dicen que la altura asociada a un fibrado simétrico (resp. antisimétrico) es casi-cuadrática (resp. casi-lineal). Gracias al siguiente lema de Tate podemos definir las alturas canónicas de Néron-Tate.

Lema 13.12. *(Tate) Sean S un conjunto, $\alpha > 1$ y dos aplicaciones $h : S \to \mathbb{R}$ y $\phi : S \to S$ tales que $|h(\phi(x)) - \alpha h(x)| \leqslant c_1$ entonces la sucesión $\alpha^{-n} h(\phi^n(x))$ es convergente y la función*
$$\hat{h}(x) := \lim_{n\to\infty} \frac{h(\phi^n(x))}{\alpha^n},$$
cumple las dos propiedades

1. $|\hat{h}(x) - h(x)| \leqslant c_1/(\alpha - 1)$;
2. $\hat{h}(\phi(x)) = \alpha\hat{h}(x)$.

Demostración. Empezamos por verificar que $u_n := \alpha^{-n}h(\phi^n(x))$ es una sucesión de Cauchy. De hecho, como $-c_1 \leqslant h(\phi^n(x)) - \alpha h(\phi^{n-1}(x)) \leqslant c_1$, multiplicando por α^{-n} y sumando las desigualdades, obtenemos

$$-c_1\left(\frac{1}{\alpha^n} + \dots \frac{1}{\alpha^{m+1}}\right) \leqslant u_n - u_m \leqslant c_1\left(\frac{1}{\alpha^n} + \dots \frac{1}{\alpha^{m+1}}\right)$$

Esto comprueba que u_n es una sucesión de Cauchy. Tomando n infinito obtenemos

$$-\frac{c_1}{\alpha^m(\alpha-1)} \leqslant \hat{h}(x) - \alpha^{-m}h(\phi^m(x)) \leqslant \frac{c_1}{\alpha^m(\alpha-1)}$$

y en particular que $|\hat{h}(x) - h(x)|$ es acotada por $c_1/(\alpha-1)$. Finalmente

$$\hat{h}(\phi(x)) = \lim_{n\to\infty} \frac{h(\phi^n(\phi(x)))}{\alpha^n} = \alpha \lim_{n\to\infty} \frac{h(\phi^{n+1}(x))}{\alpha^{n+1}} = \alpha\hat{h}(x).$$

□

Este lema 15.12 juntado con la proposición 15.11 nos permite definir las alturas canónicas, también llamadas alturas de Néron-Tate.

Definición 13.13. Sea A una variedad abeliana y $\mathcal{L}$ un fibrado sobre ella.

- Si $\mathcal{L}$ es simétrico, ponemos:
$$\hat{h}_{\mathcal{L}}(P) = \lim_{n\to\infty} 4^{-n}h_{\mathcal{L}}([2^n](P))$$
- Si $\mathcal{L}$ es antisimétrico, ponemos:
$$\hat{h}_{\mathcal{L}}(P) = \lim_{n\to\infty} 2^{-n}h_{\mathcal{L}}([2^n](P))$$

Teorema 13.14. *Sea $\mathcal{L}$ un fibrado amplio simétrico sobre una variedad abeliana A definida sobre un cuerpo de números K. La altura canónica $\hat{h}_{\mathcal{L}}$ satisface las propiedades:*

1. *Es una forma cuadrática, en particular verifica la ley del paralelogramo:*
$$\hat{h}_{\mathcal{L}}(P+Q) + \hat{h}_{\mathcal{L}}(P-Q) = 2\hat{h}_{\mathcal{L}}(P) + \hat{h}_{\mathcal{L}}(Q)$$
2. *Es definida positiva, es decir que, después de tensorizar por $\mathbb{R}$, la forma $\hat{h}_{\mathcal{L},\mathbb{R}} : A(K)\otimes_{\mathbb{Z}}\mathbb{R} \to \mathbb{R}$ es definida positiva en el sentido usual. En particular: $\hat{h}_{\mathcal{L}}(P) = 0$ si y sólo si P es torsión.*

Demostración. Sea $h_{\mathcal{L}}$ una altura de Weil asociada a $\mathcal{L}$, utilizando la relación (11.4) y la máquina de alturas, deducimos que $h_{\mathcal{L}}(P+Q) + h_{\mathcal{L}}(P-Q) = 2h_{\mathcal{L}}(P) + 2h_{\mathcal{L}}(Q) + O(1)$. Remplazando P y Q por 2^nP y 2^nQ y dividiendo por 4^n y haciendo $n \to \infty$ nos da la ley del paralelogramo, que caracteriza formas cuadráticas. Utilizando el teorema de Northcott, se puede verificar la segunda parte. □

13.4. Teorema de Mordell-Weil. La finalidad de esta sección es de dar un esbozo de demostración del teorema siguiente.

Teorema 13.15. *(Mordell-Weil) Sea A una variedad abeliana definida sobre un cuerpo de números K, el grupo $A(K)$ es un grupo de tipo finito, o sea, existe $r \geqslant 0$ y puntos $P_1,\dots, P_r$ en $A(K)$ tales que:*

$$A(K) = A(K)_{\text{tor}} \oplus \mathbb{Z}P_1 \oplus \dots \oplus \mathbb{Z}P_r$$

donde el grupo de torsión $A(K)_{\text{tor}}$ es finito.

Demostración. Como para las curvas elípticas, la prueba combina una versión "débil" del teorema con la teoría de alturas. Damos debajo un esbozo de la prueba del Teorema débil de Mordell-Weil y el lema que junta los dos argumentos. □

Lema 13.16. *(lema del descenso) Sea G un grupo abeliana tal que $G/2G$ e finito y el grupo es dotado de una forma cuadrática $q : G \to \mathbb{R}$ tal que para todo real X el conjunto $\{x \in G \mid q(x) \leqslant X\}$ es finito. Entonces el grupo G es un grupo de tipo finito.*

Observamos que se podría remplazar 2 en este lema por cualquier $m \geqslant 2$.

Demostración. Empezamos por notar que q es positiva (si existe $x \in G$ tal que $q(x) < 0$, entonces tenemos $q(nx) = n^2 q(x)$ y el conjunto $\{x \in G \mid q(x) \leqslant 0\}$ seria infinito) y así podemos definir una semi-norma $|x| = \sqrt{q(x)}$. Sea $y_1, \ldots y_m$ representantes de $G/2G$, denotamos $C = \text{máx}_i |y_i|$ y $S := \{x \in G \mid q(x) \leqslant C^2\}$; podemos demostrar que S genera el grupo G. Sea x un punto de G, su clase módulo $2G$ es igual a la clase de y_{i_1}, es decir existe $x_1 \in G$ tal que $x = 2x_1 + y_{i_1}$. Observamos que

$$2|x_1| = |2x_1| = |x - y_{i_1}| \leqslant |x| + |y_{i_1}| \leqslant |x| + C$$

entonces o $x \in S$ o tenemos $|x| > C$ y entonces $|x_1| \leqslant \frac{|x|+C}{2} < |x|$. Iterando el proceso encontramos una sucesión de $x_k \in G$ tales que $x_k = 2x_{k+1} + y_{i_k}$ con la propiedad que

$$|x_k| < |x_{k-1} < \ldots |x_1| < |x|.$$

El conjunto de los puntos x_k tales que $|x_k| \leqslant |x|$ es finito y entonces existe un k tal que $|x_k| \leqslant C$. Por tanto se puede expresar el punto x como combinación lineal de $x_k \in S$ y dos y_i que también pertenecen a S. □

Teorema 13.17. *(Teorema débil de Mordell-Weil) Sea A una variedad abeliana definida sobre un cuerpo de números K, el grupo $A(K)/2A(K)$ es un grupo finito.*

El primer paso de la demostración es de agrandar el cuerpo hasta que contenga los coordenadas de los puntos de 2-torsión :

Paso 1.– El siguiente lema permite de agrandar K hasta que $A[2] \subset A(K)$.

Lema 13.18. *Si L/K es galoisiana finita y si $A(L)/2A(L)$ es finito, entonces $A(K)/2A(K)$ es finito.*

Demostración. Podemos construir una inyección del núcleo de $A(K)/2A(K) \to A(L)/2A(L)$ en el conjunto de las funciones de $G = \text{Gal}(L/K)$ hacia $A[2]$. □

Paso 2.– Supongamos ahora que K es tal que $A[2] \subset A(K)$. Se define un emparejamiento dicho *emparejamiento de Kummer* $\lambda : A(K) \times G_K \longrightarrow A[2]$ de la manera siguiente: sea $(P, \sigma) \in A(K) \times G_K$, escogemos $Q \in A(\bar{K})$ tal que $2Q = P$, entonces se define $\lambda(P, \sigma) = \sigma(Q) - Q$, observando que $2\lambda(P, \sigma) = [2]\sigma(Q) - [2]Q = \sigma([2](Q)) - [2]Q = \sigma(P) - P = 0$ y por consecuente $\lambda(P) \in A[2]$.

Lema 13.19. *Sea $L = K([2]^{-1}A(K))$ el compositum de los cuerpos donde son definidos los puntos Q tal que $2Q \in A(K)$. El emparejamiento de Kummer induce un emparejamiento perfecto (es decir el núcleo a la derecha y el núcleo a la izquierda son triviales)*

$$\lambda : A(K)/2A(K) \times \text{Gal}(L/K) \longrightarrow A[2].$$

De este lema, deducimos que $A(K)/2A(K)$ es finito si y sólo si L/K es una extensión finita.

Paso 3.– Demostramos que los cuerpos $K(Q)$ con $Q \in [2]^{-1}A(K)$ son no ramificados afuera de un conjunto finito de plazas de K, más precisamente si S es el conjunto de los ideales primos de K, quienes dividen 2 o son primos de mala reducción, entonces $K(Q)/K$ no es ramificada fuera de S. Un teorema de Minkowski muestra entonces que hay un número finito de tales extensiones $K(Q)$ de K y deducimos de esto que L/K es finita. Este paso es basado sobre el lema 15.3. Se utiliza este lema para demostrar el hecho fundamental:

Lema 13.20. *Sea A una variedad abeliana definida sobre un cuerpo de números K y $m \geqslant 2$, suponemos que $[m](Q) \in A(K)$; sea S es el conjunto de los ideales primos de K, quienes dividen m o son primos de mala reducción, entonces $K(Q)/K$ no es ramificada fuera de S.*

Demostración. Denotamos $F := K(Q)$; la extensión F/K es no ramificada en v si y sólo si el grupo de inercia I_v actúa trivialmente sobre F. Por definición, si $\sigma \in I_v$, la reducción módulo v de σ actúa trivialmente. Así tenemos $\sigma(Q) = Q + \lambda(P, \sigma)$ y $\tilde{Q} = \tilde{\sigma}(\tilde{Q}) = \tilde{Q} + \widetilde{\lambda(P, \sigma)}$. Entonces $\widetilde{\lambda(P, \sigma)} = 0$ y, gracias al Lema 15.3 concluimos que $\lambda(P, \sigma) = 0$ y, por consecuente, σ actúa trivialmente sobre F. □

14. Ejercicios

1. Sea C una curva hiperelíptica y ι su involución canónica. Sea $L = \{(P, \iota(P)) \mid P \in C\}$, aplicando la fórmula de adjunción a $L \subset C \times C$ (si $C \subset X$ es una curva en una superficie y K_S es el divisor canónico, $C^2 + K_S \cdot C = 2g(C) - 2$) mostrar que $L^2 = -2g + 2$. Sea $\pi : C \times C \to X$ el cociente por $\sigma(P, Q) = (Q, P)$ y $L_0 = \pi(L)$, mostrar que $L_0 \cdot L_0 = -g + 1$ y $L_0 \cong \mathbb{P}^1$. En el caso $g = 2$ concluir que L_0 es una curva excepcional (i.e. auto-intersección -1 y isomorfa a $\mathbb{P}^1$).
2. Sea E una variedad abeliana de dimensión 1. Definimos $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$. Mostrar que $\mathrm{End}^0(E)$ puede ser $\mathbb{Q}$, una extensión cuadrática imaginaria o una álgebra de cuaterniones $[\mathrm{End}^0(E) : \mathbb{Q}] = 4$. Si la característica es cero, mostrar que sólo los dos primeros casos existen [Indicación: ver [14], Theorem 9.3. El ejercicio siguiente muestra que el tercero caso pode ocurrir en característica positiva.]
3. Consideramos la curva elíptica E sobre $\mathbb{F}_2$ definida por $y^2 + y = x^3$. Mostrar que $\mathrm{Frob}^2(x, y) = (x^4, y^4)$ coincide con $[+2]$ o $[-2]$ y deducir que $T_2(E) = 0$. Sea $a^3 = 1$ y $e^2 + e = 1$, mostrar que $\phi_{a,e}(x, y) = (a(x + 1), y + x + e)$ es un automorfismo de E. Verificar que en general $\phi_{a,e}$ no conmuta con $\phi_{a',e'}$ y concluir que $\mathrm{End}(E)$ no es conmutativo y debe ser un orden en una álgebra de cuaterniones.
4. Sea $A/\mathbb{F}_q$, mostrar que $|A(\mathbb{F}_q)| = \deg(Id_A - Frob_A)$. Suponemos que $\phi : A \to B$ es una isogenía definida sobre $\mathbb{F}_q$, mostrar que $|A(\mathbb{F}_q)| = |B(\mathbb{F}_q)|$ (N.B. en general los grupos $A(\mathbb{F}_q)$, $B(\mathbb{F}_q)$ no son isomorfos). [Indicación: utilizar $\phi \circ (Id_A - Frob_A) = (Id_B - Frob_B) \circ \phi$.]
5. Sea K cuerpo de característica $\neq 2$ y $f(x) = (x - a_1) \dots (x - a_{2g+1})$ un polinomio separable. Consideramos la curva proyectiva C con ecuación afín $y^2 = f(x)$ y los puntos $P_i = (a_i, 0)$ y el punto al infinito que denotamos ∞. Denotamos J la jacobiana de C y $j : C \to J$ la inmersión $j(P) := Cl\,((P) - (\infty))$.
   a) Mostrar que $\mathrm{div}(x - a_i) = 2(P_i) - 2(\infty)$ y $\mathrm{div}(y) = \sum_i (P_i) - (2g + 1)(\infty)$.
   b) Mostrar que las únicas relaciones entre los puntos $j(P_i)$ son dadas por $[2]j(P_i) = 0$ y $\sum_i j(P_i) = 0$.
   c) Mostrar que los puntos $j(P_i) \in J$ tienen orden 2 y generan el grupo $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$.
6. Utilizar el Teorema 14.4 para mostrar que si C es una curva de género 2 y $N_i = |C(\mathbb{F}_{q^i})|$, entonces
$$|J_C(\mathbb{F}_q)| = \frac{N_1^2 + N_2}{2} - q.$$
Aplicar eso a la curva $C : y^2 = x^5 + 1$, mostrando que por $p \neq 2, 5$, si $p \equiv 2, 3$ mód 5 tenemos $|J_C(\mathbb{F}_p)| = p^2 + 1$. Utilizar el Lema 15.3 y deducir que $|J_C(\mathbb{Q})|$ divide 10. Sea ∞ el punto "en el infinito", $P_0 = (-1, 0)$ y $Q = (0, 1)$, verificar que $\mathrm{div}(y - 1) = 5(Q) - 5(\infty)$ y también $\mathrm{div}(x + 1) = 2(P_0) - 2(\infty)$ y concluir que:
$$J_C(\mathbb{Q})_{\mathrm{tor}} =< j(P_0), j(Q) > \cong \mathbb{Z}/10\mathbb{Z}.$$

7. Sean A y B duas variedades abelianas definidas sobre un cuerpo de números K y v una plaza donde ambas tienen buena reducción; denotamos $\tilde{A}_v$ y $\tilde{B}_v$ las reducciones. Mostrar que la aplicación natural:

$$\mathrm{Hom}(A,B) \longrightarrow \mathrm{Hom}(\tilde{A}_v, \tilde{B}_v)$$

es inyectiva. [Indicación: utilizar el Lema 15.3 para demostrar que si $\Phi \neq 0$, la reducción $\tilde{\Phi}$ no puede anularse sobre todos los puntos de torsión.] Construir un ejemplo donde la aplicación no es sobreyectiva [Indicación: examinar el ejemplo del ejercicio 3.]

Parte 3. Variedades abelianas: Aritmética

Esta tercera parte se enfoca en el difícil problema de *clasificación de variedades abelianas principalmente polarizadas* de una dimensión g dada sobre un cuerpo K dado por medio de *invariantes aritméticos explícitos*.

Sección 17 establece un marco general. Dentro del marco , presenta el caso relativamente simple de $K = \mathbb{F}_p$, donde los fundamentos teóricos de una clasificación completa para todo g son conocidos. Sección 18 describe conjeturas profundas dando la naturaleza de la clasificación para $K = \mathbb{Q}$ para todo g. Describe cómo las conjeturas son conocidas para $g = 1$ y más aún los cálculos han dado extensas tablas. Sección 19 aún asume $K = \mathbb{Q}$, aunque entra en el caso salvaje de $g \geqslant 2$. Explica que las conjeturas son conocidas sólo para casos especiales, pero los cálculos actuales soportan las conjeturas produciendo tablas gigantes.

En ambos casos, $K = \mathbb{F}_p$ y $K = \mathbb{Q}$, la clasificación se centra en funciones L. En el caso de $\mathbb{F}_p$, la función L $L_p(A,s)$ asociada a una variedad abeliana A de dimensión g proviene de un solo polinomio

$$F_p(A,T) = \sum_{j=0}^{2g} a_{p,j} T^j$$

como uno tiene la fórmula $L_p(A,s) = F_p(A,p^{-s})$. En el caso de $\mathbb{Q}$, la función L $L(A,s)$ es un objeto de enorme riqueza, siendo de la forma $\prod_p L_p(A,s)^{-1}$, con la definición de $L_p(A,s)$ requiriendo modificaciones importantes en los primos malos de A. La cuestión central en el caso del cuerpo base $\mathbb{Q}$ es cómo se comporta $F_p(A,T)$ cuando uno varía p.

La dificultad de consideraciones explícitas aumenta muy rápidamente con la dimensión g. Asimismo una "curva abeliana principalmente polarizada" es solo una curva de género uno con un punto distinguido , i.e. una curva elíptica. Una superficie abeliana principalmente polarizada es o la Jacobiana de una curva de género dos, el producto de dos curvas elípticas, o la restricción de Weil de una curva elíptica sobre una extensión cuadrática. Por lo tanto, las dos últimas secciones se enfocarán sobre todo en curvas.

La clasificación explícita de variedades abelianas principalmente polarizadas no es una cuestión puramente matemática. De hecho, es posible obtener tablas completas de tamaño modesto sólo con el uso sistemático de computadoras. Estas notas apuntan a reflejar un equilibrio teórico/computacional apropiado, presentando cálculos explícitos que ilustran diferentes aspectos de la situación general. Incluimos algunos fragmentos del código en *Magma* para que incluso los principiantes sin copias de *Magma* puedan hacer algunos cómputos en la versión en línea de *Magma*. La clasificación explícita de objetos por medio de funciones L es el objetivo principal de la base de datos *L-functions and modular forms database*. Este curso también sirve como una introducción a la LMFDB, ya que cada clase corresponde directamente a una gran parte particular de la base de datos.

15. Invariantes geométricos y de isogenía

Esta primera sección se centra en definir invariantes y discutir la clasificación para un cuerpo base K. Dado K, fijamos una clausura algebraica $\overline{K}$. Si K tiene característica finita p, denotamos por $\mathbb{F}_{p^e}$ el subcuerpo de $\overline{K}$ con p^e elementos. Esta sección provee ejemplos para el caso más fáciles de cuerpos bases $K = \mathbb{F}_q$ a manera de calentamiento para el caso principal de $K = \mathbb{Q}$.

15.1. Cuatro conjuntos interrelacionados. Para un cuerpo arbitrario K y un entero positivo g, existen cuatro conjuntos interrelacionados dignos de atención:

$$\begin{array}{ccc} \mathrm{PPAb}_g(K) & \to & \mathrm{Ab}_g(K) \\ m\downarrow & & \downarrow \\ A_g(K) & & \mathrm{IsAb}_g(K) \end{array} . \tag{15.1}$$

El conjunto $\mathrm{Ab}_g(K)$ es el conjunto de variedades abelianas sobre K de dimensión g salvo isomorfismo. Es el conjunto en el que uno podría pensar que es mejor estudiarlo primero, pero de hecho los otros tres se comportan mejor.

15.2. Variedades abelianas principalmente polarizadas. Nuestro objetivo principal es la descripción explícita del conjunto $\mathrm{PPAb}_g(K)$ de variedades abelianas principalmente polarizadas sobre K de dimensión g.

El caso $g = 1$. El caso unidimensional puede hacerse de manera muy concreta. Para $\mathrm{char}(K) > 3$, cualquier curva elíptica E/K puede ser dada por una ecuación afín

$$y^2 = x^3 + bx + c \tag{15.2}$$

con $\Delta := -4b^3 - 27c^2 \neq 0$. Sustituyendo $(x, y) \to (x/u^2, y/u^3)$ y luego multiplicando por u^6 obtenemos que

$$y^2 = x^3 + bu^4x + cu^6 \tag{15.3}$$

también define E.

En efecto, esta construcción identifica $\mathrm{PPAb}_1(K)$ con el conjunto cociente

$$\{(b, c) \in K^2 | -4b^3 - 27c^2 \neq 0\}/K^\times,$$

donde la acción está dada por $(b, c)u = (bu^4, cu^6)$. Denotemos $\mu_m(K)$ el conjunto de raíces m-ésimas de la unidad en K. Entonces el estabilizador de $(0, c)$ es $\mu_6(K)$ mientras que el de $(b, 0)$ es $\mu_4(K)$. En el caso que ambas coordenadas seas no nulas, el estabilizador de (b, c) es $\mu_2(K) = \{\pm 1\}$.

Ahora supongamos que K es un cuerpo finito $\mathbb{F}_q$. Entonces,

$$|\mu_6(\mathbb{F}_q)| = \begin{cases} 6 & \text{if } q \equiv 1\ (6) \\ 2 & \text{if } q \equiv 5\ (6) \end{cases}, \qquad |\mu_4(\mathbb{F}_q)| = \begin{cases} 4 & \text{if } q \equiv 1\ (4) \\ 2 & \text{if } q \equiv 3\ (4) \end{cases}.$$

El conjunto $\{(b, c)| - 4b^3 - 27c^2 \neq 0\}$ tiene $q^2 - q$ elementos. Contando el número de órbitas, concluimos que

$$|\mathrm{PPAb}_1(\mathbb{F}_q)| = \begin{cases} 2q + 6 & \text{if } q \equiv 1\ (12) \\ 2q + 2 & \text{if } q \equiv 5\ (12) \\ 2q + 4 & \text{if } q \equiv 7\ (12) \\ 2q & \text{if } q \equiv 11\ (12) \end{cases}.$$

Uno querría un conteo explícito similar a este para género arbitrario g!

15.3. El espacio de moduli A_g. La teoría profunda de los esquemas de módulos dice que existe un esquema de módulos gruesos A_g sobre $\mathbb{Z}$ para variedades abelianas. El mapa m en el extremo superior izquierdo de (17.1) envía $A \in \mathrm{PPAb}_g(K)$ a su punto moduli $m(A) \in A_g(K)$. Para K algebraicamente cerrado, m is biyectiva. Una función sobre $\mathrm{PPAb}_g(K)$ es llamada un *invariante geométrico* si proviene de una función sobre $A_g(\overline{K})$.

El caso $g = 1$. Claramente b^3/c^2 es un invariante geométrico de la clase de isomorfismo de una curva elíptica E dada por (17.2). Por uniformidad en las características 2 y 3 que estamos excluyendo aquí, uno se concentra en

$$j = \frac{6912b^3}{4b^3 + 27c^2} = \frac{-2^8 3^3 b^3}{\Delta}.$$

El invariante j identifica A_1 con la línea afín con coordenada j. En otras palabras (con una definición distinta de j en los casos excluidos por la característica), $A_1 = \mathrm{Spec}(\mathbb{Z}[j])$. De esta manera uno tiene la simple fórmula

$$|A_1(\mathbb{F}_q)| = q.$$

Uno querría generalizar esta fórmula para g arbitrario!

Enfoque a través de curvas. La Jacobiana de una curva es una variedad abeliana principalmente polarizada. Nuestros ejemplos provienen de curvas hiperelípticas de la forma afín

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

Aquí $\mathrm{char}(K) \neq 2$ y $f(x) \in K[x]$ es separable de grado $2g-1$ o $2g$. Para un género dado g, considere los espacios moduli ásperos de curvas hiperelípticas, de todas las curvas, y de las variedades abelianas principalmente polarizadas. Por medio de la inyectividad del mapeo Jacobiano, uno tiene

$$H_g \subseteq M_g \subseteq A_g. \tag{15.4}$$

Para $g = 1$, todas las inclusiones son igualdades. También $H_2 = M_2$, pero todas las demás inclusiones son estrictas.

Dimensiones en general. Para $g > 1$, las dimensiones relativas sobre $\mathbb{Z}$ de los tres esquemas moduli son $(2g-1, 3g-3, g(g+1)/2)$. Luego para $g = 2$, las dimensiones son $(3, 3, 3)$. Como explicaremos en la tercera clase, $|H_2(\mathbb{F}_q)| = |M_2(\mathbb{F}_q)| = q^3$ mientras que $|A_2(\mathbb{F}_q)| = q^3 + q^2$. Para $g = 3$, uno necesita ir más allá de las curvas hiperelípticas, pero aún puede usar la estrategia de las Jacobianas, pues las dimensiones son $(5, 6, 6)$. En general, A_g es geométricamente conexo, lo que implica que

$$|A_g(\mathbb{F}_q)| \approx q^{g(g+1)/2}.$$

Aquí el radio de los dos lados tiene límite 1 para g fijo y $q \to \infty$.

La suryectividad de m falla. Para $j \neq 0, 1728$, la curva elíptica

$$y^2 = x^3 - \frac{3jx}{j - 1728} + \frac{2j}{j - 1728} \tag{15.5}$$

tiene invariante j igual a j. Además, $y^2 = x^3 - 1$ y $y^2 = x^3 - x$ tienen invariantes j igual a 0 y 1728 respectivamente. Por lo tanto, en el caso $g = 1$, el mapeo m es suryectivo. Para $g \geqslant 2$, m no es suryectiva. La obstrucción a la suryectividad en el caso de género 2 es descripta en términos muy concretos en [28]. Para cuerpos finitos, m es siempre suryectiva pues cuerpos finitos tienen dimensión cohomológica uno y las obstrucciones viven en el segundo grupo de cohomología.

La inyectividad de m falla. Sea $x \in A_g(K)$ representado por $A \in \mathrm{PPAb}_g(K)$. Para $K \subseteq K' \subseteq \overline{K}$, denotamos por $A_{K'}$ el cambio de base de A a la variedad abeliana sobre K'. Entonces uno tiene no solo Aut_K, sino también el grupo $\mathrm{Aut}(A_{K'})$ que probablemente es más grande. Para K^s la clausura separable de K en $\overline{K}$, el grupo $\mathrm{Gal}(K^s/K)$ actúa en $\mathrm{Aut}(A_{K^s})$ con $\mathrm{Aut}(A)$ como el conjunto de puntos fijos. La fibra arriba de m es entonces un conjunto de un punto indexado por un grupo de cohomología de Galois:

$$m^{-1}(x) = H^1(\mathrm{Gal}(K^s/K), \mathrm{Aut}(A_{K^s})).$$

Cuando K es finito, uno tiene que $\mathrm{Gal}(K^s/K) = \widehat{\mathbb{Z}}$ y la cohomología puede ser expresada en términos elementales. En particular, uno tiene

$$\sum_{t \in m^{-1}(x)} \frac{1}{\mathrm{Aut}(A_t)} = 1.$$

En el caso de las curvas elípticas, el lado izquierdo es m veces $1/m$ para $m \in \{2, 4, 6\}$. Como las variedades abelianas sobre cuerpos arbitrarios siempre tienen al menos el automorfismo negación -1, los grupos $\mathrm{Aut}(A_t)$ son siempre no triviales, mostrando que la falla de la inyectividad es más seria que en el caso paralelo donde A_g es reemplazado por M_g.

15.4. Clases de isogenía. Por definición, $\mathrm{IsAb}_g(K)$ es el conjunto de clases de isogenías de una variedad abeliana de dimensión g sobre K. Una función sobre $\mathrm{Ab}_g(K)$ es llamada *invariante de isogenía* si proviene de una función de $\mathrm{IsAb}_g(K)$. Para $K = \mathbb{F}_q$, uno tiene una función obvia sobre $\mathrm{Ab}_g(K)$ para cada entero positivo e. Ésta es $A \mapsto |A(\mathbb{F}_{q^e})|$. Notablemente, la cantidad $|A(\mathbb{F}_{q^e})|$ es un invariante de isogenía. Más aún, estos números pueden ser usados para indexar $\mathrm{IsAb}_p(\mathbb{F}_p)$ con un conjunto $\mathcal{L}_g(\mathbb{F}_p)$ fácil de describir.

Conteo de puntos. La famosa hipótesis de Riemann de Weil para variedades abelianas sobre $\mathbb{F}_q$ es la siguiente.

> *Sea A una variedad abeliana g-dimensional sobre $\mathbb{F}_q$. Entonces existen números complejos $\alpha_1, \ldots, \alpha_{2g}$ tales que*
>
> $$|A(\mathbb{F}_{q^e})| = \prod_{j=1}^{2g} (1 - \alpha_j^e)$$
>
> *para todos los enteros positivos e. Más aún, estos números complejos tiene valor absoluto $\sqrt{q}$.*

La lista desordenada de los $2g$ números α_j está determinada por $|A(\mathbb{F}_{q^e})|$ para $e \leqslant g$, con parte del formalismo presentado a continuación.

Si A es la Jacobiana de una curva C de género g, entonces los mismo números determinan el número de puntos en C:

$$|C(\mathbb{F}_{q^e})| = q^e + 1 - \sum_{j=1}^{2g} \alpha_j^e.$$

Por ejemplo, si C está dada por $y^2 = f(x)$ con $f(x) \in \mathbb{F}_q[x]$ de grado $2g-1$, entonces una cuenta ingenua puede ser conceptualmente formulada como

$$|C(\mathbb{F}_{q^e})| = q^e + 1 - \sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q^e} \right). \tag{15.6}$$

Aquí estamos usando el símbolo del residuo cuadrático,

$$\left(\frac{z}{q^e} \right) = (\text{número de raíces cuadradas de } z \text{ en } \mathbb{F}_{q^e}) - 1.$$

Existe maneras mucho más rápidas de calcular $|C(\mathbb{F}_{q^e})|$ que evaluando directamente el lado derecho de (17.6).

Funciones L desde distintos puntos de vista. Uno puede pensar a los $2g$ números α_j de varias formas, y diferentes términos estrechamente relacionados están involucrados. Primero que todo, un número algebraico que tiene todos sus conjugados con valor absoluto $\sqrt{q}$ es llamado un *q-número de Weil*. Luego, α_j es un q-número de Weil para todo j.

Como segundo paso, uno puede eliminar la ambigüedad del orden formando el *polinomio de Frobenius*

$$F_q(A,T) = \prod_{j=1}^{2g}(1-\alpha_j T) =: \sum_{j=0}^{2g} a_j T^j.$$

Aquí los coeficientes pertenecen a $\mathbb{Z}$ y el polinomio es conformalmente palíndromo en el sentido que

$$a_{2g-j} = q^j a_j.$$

Así $a_0 = 1$, $a_{2g} = q^g$ y el polinomio es determinado por los coeficientes $a_1, \ldots, a_g$.

Como tercer paso, uno puede re escalar las raíces para obtener el *polinomio de Frobenius unitarizado*

$$f_q(A,t) = \prod_{j=1}^{2g}(1-\frac{\alpha_j}{\sqrt{q}}t) =: \sum_{j=0}^{2g} u_j t^j.$$

Este re escalamiento tiene la ventaja que el polinomio es realmente un palíndromo, aunque la desventaja que los coeficientes u_i tienen en general denominadores que involucran $\sqrt{q}$.

En el cuarto punto, uno puede ver los coeficientes de $f_q(A,t)$ como el vector

$$\mathrm{fr}_p = (u_1, \ldots, u_g)\,.$$

La hipótesis de Riemann se traduce en desigualdades entre las coordenadas, que no hacen mención de q debido a la normalización. El simple curvilíneo en el cual los vectores viven se puede ver de manera natural como el conjunto $Sp_{2g}^\natural$ de clases de conjugación en el grupo simpléctico compacto Sp_{2g}. El caso $g = 2$ está dibujado en Figura 1. Las curvas fronterizas de arriba, a la izquierda, y a la derecha, corresponden a $f_p(t)$ con raíces de la forma $(\alpha, \bar{\alpha}, \alpha, \bar{\alpha})$, $(-1, -1, \alpha, \bar{\alpha})$, y $(\alpha, \bar{\alpha}, 1, 1)$ respectivamente. Así, los vértices de la izquierda, de la derecha, y de abajo, corresponden a las raíces $(-1, -1, -1, -1)$, $(1, 1, 1, 1)$, y $(-1, -1, 1, 1)$.

Quinto paso; uno puede trasladarse al lenguaje de *funciones L* escribiendo

$$L_q(A,s) = F_q(A, q^{-s}).$$

Este es un punto de vista que destacaremos, escribiendo $\mathcal{L}_g(\mathbb{F}_q)$ para el conjunto de todas las funciones L que surjan de cualquier colección de $2g$ q-números de Weil definidos sobre $\mathbb{Q}$ y estables bajo $\alpha \mapsto q/\alpha$.

Teorema de Honda-Tate. Este teorema describe completamente el conjunto *a priori* muy complicado $\mathrm{IsAb}(\mathbb{F}_q)$ en términos del conjunto elemental $\mathcal{L}(\mathbb{F}_q)$.

Teorema 15.1. (Parte del Teorema de Honda-Tate.) *El mapeo que envía una clase de isogenía de una variedad abeliana $A \in \mathrm{IsAb}(\mathbb{F}_q)$ a su función L $L(A,s) \in \mathcal{L}(\mathbb{F}_q)$ es inyectivo. Para $q = p$ primo, es también suryectivo.*

Cuando q no es primo, una función L está en la imagen si ciertas obstrucciones se anulan. Estas obstrucciones son extrañas. No entraremos en esta hermosa teoría de la obstrucción porque nuestro objetivo principal es describir un marco simple que sirva de guía para las próximas dos clases. Tate probó en [30] la parte de la inyectividad del teorema y describió las obstrucciones. Honda probó en [25] para q general que la imagen es en efecto igual a todas las funciones L no obstruidas.

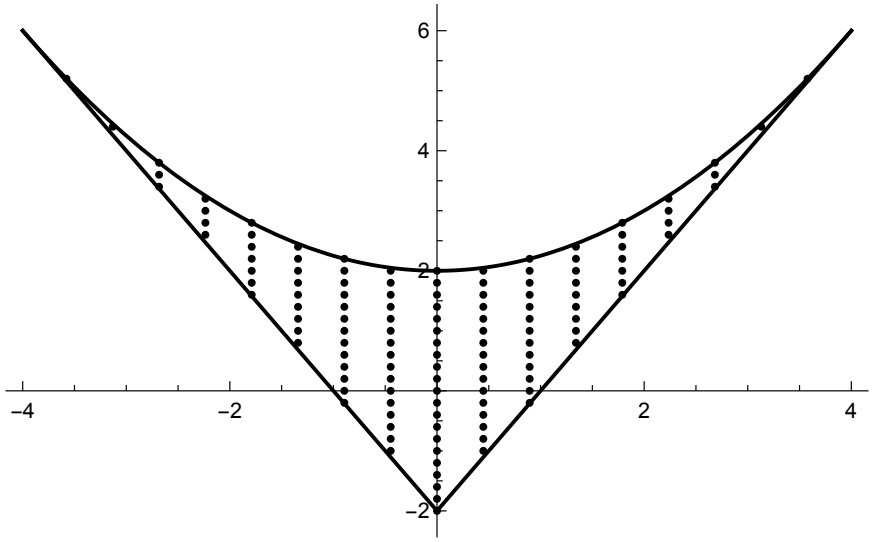


FIGURA 1. El simplex curvilineal $Sp_4^\natural$. Los 129 puntos $\mathrm{fr}_5 = (u_1, u_2) = (a_1/\sqrt{5}, a_2/5)$ corresponden a las 129 funciones $L\ 1 + a_1 5^{-s} + a_2 5^{-2s} + a_1 5^{1-3s} + 5^{2-4s}$ en $\mathcal{L}_2(\mathbb{F}_5)$.

Volúmenes de espacio de clases. El Teorema de Honda-Tate hace que sea importante entender bien el conjunto más simple $\mathcal{L}_g(\mathbb{F}_q)$. Como la Figura 1 sugiere, conteos exactos son posibles, y de hecho muchos conteos exactos de $\mathrm{IsAb}(\mathbb{F}_q)$ vía el Teorema de Honda-Tate está en la LMFDB. En un nivel aproximado, los conteos provienen de volúmenes como sigue. El intervalo $Sp_2^\natural = [-2, 2]$, que sirve como espacio ambiental de todos los $\mathcal{L}_1(\mathbb{F}_q)$, obviamente tiene longitud 4 . Las curvas fronteras en Tabla 1 tienen ecuaciones que se pueden ver en (19.6) abajo, y una integración muestra que el "escudo" $Sp_4^\natural$ conteniendo todo $\mathcal{L}_2(\mathbb{F}_q)$ tiene área 16/3. Un cómputo más sofisticado ([21]) del volúmen Euclidiano V_g de $Sp_{2g}^\natural$ para g arbitrario da

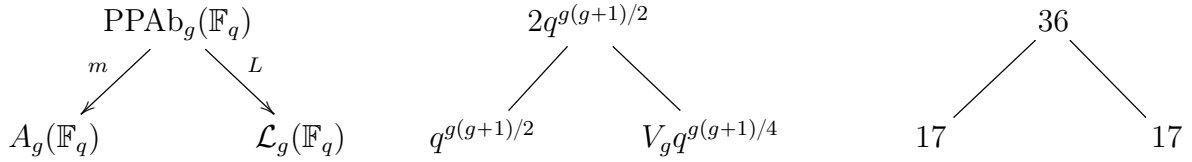
$$V_g = \prod_{j=1}^{g} \frac{2^{j+1}(j-1)!}{(2j-1)!!}.$$

El j-ésimo factor es asintótico a $\sqrt{\pi/j}$, por lo que en particular V_g tiende a 0. Re escalando la j-ésimo coordenada por $q^{j/2}$, obtenemos

$$|\mathcal{L}_g(\mathbb{F}_q)| \approx V_g q^{g(g+1)/4}. \tag{15.7}$$

Una interpretación rigurosa de esta aproximación es que el radio de los dos lados tiene a 1 cuando q va al infinito.

15.5. El diagrama principal revisitado. Los tres conjuntos en los que nos hemos concentrado en el caso $K = \mathbb{F}_q$ están a la izquierda:
(15.8)



Fórmulas aproximadas para sus tamaños, provenientes de nuestras consideraciones previas, están en el medio. Notemos que $\mathcal{L}_g(\mathbb{F}_q)$ es mucho más pequeño que los otros dos conjuntos en este diagrama.

El mapeo L es complicado: algunas fibras puedan ser vacías pero la mayoría de las fibras son grandes . Describimos aquí el caso $g = 1$ y $q = p$ primo, siguiendo [31]. Aquí el mapeo L es trivialmente suryectivo pues todas las curvas elípticas vienen con una polarización principal canónica. La descripción está en términos de discriminantes cuadráticos negativos, es decir, discriminantes de ordenes cuadráticos imaginarios. Estos son enteros negativos congruentes a 0 o 1 módulo 4. Tienen una factorización canónica como $D = dc^2$, donde d es el discriminante del cuerpo $K(\sqrt{d})$. Los números d son llamados discriminantes fundamentales y son reconocidos entre todos los discriminantes como los únicos libre de cuadrados si $d \equiv 1 \pmod 4$ y 4 veces un entero libre de cuadrados si $d \equiv 0 \pmod 4$.

El número de clase $h(D)$ de un discriminante general se puede expresar en términos del discriminante fundamental asociado d:

$$h(dc^2) = h(d)\frac{w(dc^2)}{w(d)}c\prod_{p|c}\left(1-\left(\frac{d}{p}\right)\frac{1}{p}\right).$$

Aquí, $w(D)$ cuenta raíces de la unidad, así que $w(-3) = 6$, $w(-4) = 4$, y $w(D) = 2$ en caso contrario. Definimos $H(dc^2) = \sum_{j|c} h(dj^2)$. Entonces la fórmula simple es que el tamaño de la fibra arriba $1 + ap^{-s} + p^{1-2s}$ es $H(a^2 - 4p)$.

j	**0**	1	2	3	4	5	6	7	8	9	10	**11**	12	13	14	15	16	t	D	$H(D)$
												1						8	-4	1
													1					7	-19	1
		1					1				1							6	$-8\cdot 2^2$	$1+2$
																1		5	-43	1
					1	1												4	-52	2
			1					1						1				3	-59	3
	1									1					1		1	2	$-4\cdot 4^2$	$1+1+2$
				1														1	-67	1
									2			2						0	-68	4
				1														-1	-67	1
	1									1					1		1	-2	$-4\cdot 4^2$	$1+1+2$
			1					1						1				-3	-59	3
					1	1												-4	-52	2
																1		-5	-43	1
		1					1				1							-6	$-8\cdot 2^2$	$1+2$
													1					-7	-19	1
												1						-8	-4	1

CUADRO 1. El número de curvas elípticas sobre $\mathbb{F}_{17}$ con invariante j igual a j y función L $1-tp^{-s}+p^{1-2s}$. El correspondiente discriminante $D = t^2-4p$ y el número de clases $h(D)$ están dados a la derecha.

La parte derecha de (17.8) es el caso del cuerpo base $\mathbb{F}_{17}$. Con mucho más detalle, Cuadro 1 muestra explícitamente cómo las fibras de L son gobernadas por los números de clases, mientras que las fibras de m tiene tamaño 2, excepto quizás sobre los invariantes j excepcionales 0 y 1728. En este caso, 0 aún tiene una fibra de tamaño 2 pues $|\mu_6(\mathbb{F}_{17})| = 2$ pero 1728, visto como 11 en $\mathbb{F}_{17}$, tiene una fibra de tamaño 4, pues $|\mu_4(\mathbb{F}_{17})| = 4$.

15.6. Grupos de Galois Motivicos y grupos de Sato-Tate. La teoría de Galois juega un papel más grande en esta situación que la que hemos indicado . Concluimos la primera clase definiendo grupos de Galois motivicos y grupos de Sato-Tate de variedades

abelianas sobre cuerpos finitos. Tal como $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, ellos son cíclicos en un sentido apropiado, siendo generados por un elemento de Frobenius. En contraste, los grupos de Galois motívicos y los grupos de Sato-Tate de las clases siguientes, como $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, estarán lejos de ser abelianos.

Grupos de números de Weil. Dado $A \in \mathrm{IsAb}(\mathbb{F}_q)$, sea Π el subgrupo de $\mathbb{C}^\times$ generado por sus q-números de Weil α. De manera similar, sea Θ el subgrupo del círculo unitario generado por los números normalizados de Weil $\alpha/\sqrt{q}$. El grupo Π es el *grupo de número de Weil* de A y el grupo Θ es el *grupo ángulo* de A. Claramente, Π y Θ son versiones similares una de otra.

Entre las diferentes cosas contabilizadas por la LMFDB para una clase de isogenía es su *rango angular* r, que significa el rango del grupo abeliano finitamente generado Θ. Como los números $\alpha/\sqrt{q}$ vienen en pares uno inverso del otro, este rango está en $\{0, \ldots, g\}$. El rango de Π es $r+1$. Sea t el tamaño del subgrupo de torsión de W. El tamaño del subgrupo de torsión de Θ es generalmente t, pero excepcionalmente puede ser $2t$. Este último caso se da cuando por ejemplo $q \in \{2, 3\}$ y $F_q(T) = 1 + qT + q^2$, donde $t = 2q$.

Rango angular en dimensión 2. Como un ejemplo que será de mucha ayuda después, tomamos $g = 2$ y $q = p \geqslant 7$. Entonces, existen siempre exactamente cinco polinomios de Frobenius de rango cero. Sus versiones normalizadas $f_p(t)$ son $1 + bt^2 + t^4$ con $b = -2$, $b = -1$, $b = 0$, $b = 1$, y $b = 2$. Los polinomios $f_p(t)$ son productos de polinomios ciclotómicos. Por ejemplo, cuando $b = -1$, $1 - t^2 + t^4 = (1 + t + t^2)(1 - t + t^2) = \Phi_3(t)\Phi_6(t)$.

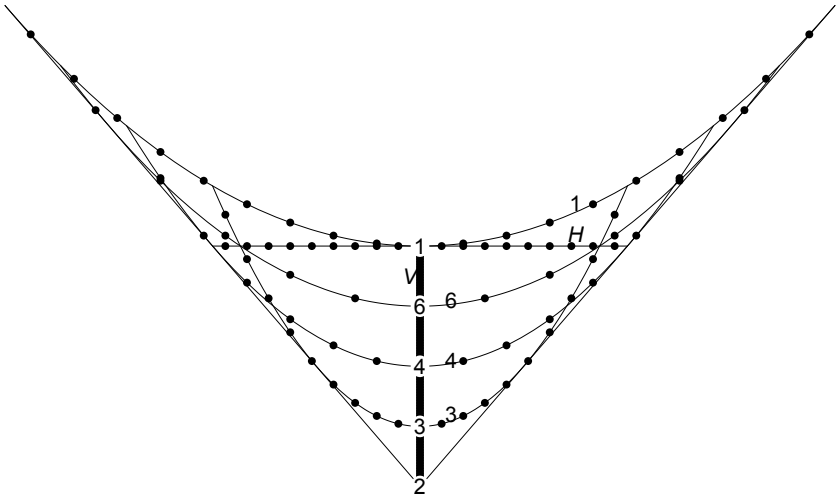


FIGURA 2. El espacio de clases $Sp_4^\natural$ de Figura 1, ahora con cinco puntos etiquetados p_i correspondientes al rango angular cero y seis curvas etiquetadas correspondientes a rango angular uno. Los 164 puntos de $\mathcal{L}_2(\mathbb{F}_{23})$ que tienen rango angular uno están también dibujados, con 88 de ellos en la línea vertical V.

El comportamiento es nuevamente uniforme con respecto al rango angular uno: los puntos $(u, v) \in Sp_4^\natural$ indexando los polinomios unitarizados $f_p(t) = 1 + ut + vt^2 + ut^3 + t^4$ viven todos en exactamente una de las seis curvas. Estas curvas son cuatro parábolas C_k, una línea vertical V_2 y una línea horizontal H_4. Los subíndices dan el número de torsión. Figura 2 dibuja y etiqueta cada una de las seis curvas. Coloca un índice k para indicar un punto p_k donde el rango de ángulo es cero. La notación de los puntos se hereda de la de las curvas, y también tiene la propiedad que $p_k = (0, 4\cos^2(\pi/k) - 2)$.

Point	$f_p(t)$	Curve	$f_p(t)$	$g_p(t)$	
$p_2=(0,-2)$	$(1-t)^2(1+t)^2$	$V_2: a=0$		$(t+1)^2$	(t^2-bt+1)
$p_3=(0,-1)$	$1-t^2+t^4$	$C_3: b=a^2-1$		(t^2+t+1)	$(-ta^2+t^2+2t+1)$
$p_4=(0,0)$	$1+t^4$	$C_4: b=\frac{a^2}{2}$		(t^2+1)	$(-\frac{ta^2}{2}+t^2+2t+1)$
$p_6=(0,1)$	$\Phi_3(t)\Phi_6(t)$	$C_6: b=\frac{a^2}{3}+1$		(t^2-t+1)	$(-\frac{ta^2}{3}+t^2+2t+1)$
$p_1=(0,2)$	$(1+t^2)^2$	$C_1: b=\frac{a^2}{4}+2$	$(t^2+\frac{at}{2}+1)^2$	$(1-t)^2$	$(-\frac{ta^2}{4}+t^2+2t+1)$
		$H_4: b=2$	$(t^2+1)(t^2+at+1)$		

CUADRO 2. Información de los cinco puntos correspondientes a rango angular cero y las seis curvas correspondientes a rango angular uno.

Más detalles son dados en Tabla 2. Sobre la derecha $f_p(t)$ es dado si se factorea en factores de menor grado. Esta factorización muestra cómo puntos genéricos en C_1 y H_4 tienen de hecho rango uno.

Para ver lo especial de las otras curvas, sean α, β, $\bar{\alpha}$, y $\bar{\beta}$ las raíces de $f_p(t)$. Entonces

$$g_p(t) := (1-\alpha\beta t)(1-\bar{\alpha}\beta t)(1-\bar{\beta}\bar{\alpha}t)(1-\bar{\alpha}\bar{\beta}t) = 1+(2-v)t+(2+u^2-2v)t^2+(2-v)t^3+t^4.$$

Cuando usamos la ecuación de la curva para remover la variable, entonces $g_p(t)$ se factorea en los casos listados en Tabla 2. Nuevamente estas factorizaciones muestran que los puntos genéricos sobre las curvas restantes tienen rango uno. Las factorizaciones también muestran que los números de torsión dados como subíndices son correctos.

Definiciones via dualidad. Sea A una variedad abeliana con grupo de Weil Π y grupo angular Θ. Sea r el rango angular de Θ y sea δt el número de torsión de Θ como arriba, por lo que Π tiene rango $r+1$ y número de torsión t.

Sea ST el grupo dual de Θ. Aquí vemos Θ como un grupo discreto tal que ST es compacto. Su componente de la identidad ST^0 es el producto de r círculos. El grupo ST/ST^0 es isomorfo a $\mathbb{Z}/(\delta t)$. El grupo ST es el *grupo de Sato-Tate* de A.

Para Π procedemos de manera similar. Sin embargo, esta vez, prestamos atención a la acción natural de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Sea G el grupo dual de Π, ahora considerado el marco de grupos algebraicos conmutativos sobre $\mathbb{Q}$. La componente identidad G^0 satisface $G^0(\mathbb{C}) \cong (\mathbb{C}^\times)^{r+1}$. Su grupo de componentes $Q = G/G^0$ satisface $Q(\mathbb{C}) = \mathbb{Z}/t$. El grupo G es el *grupo de Galois motívico* de A. El hecho que ambos grupos, Π y Θ, están dentro de $\mathbb{C}^\times$ provee a los grupos recién definidos generadores canónicos, los cuales son denotados $\mathrm{Fr}_q \in G(\mathbb{Q})$ y $\mathrm{fr}_q \in ST$.

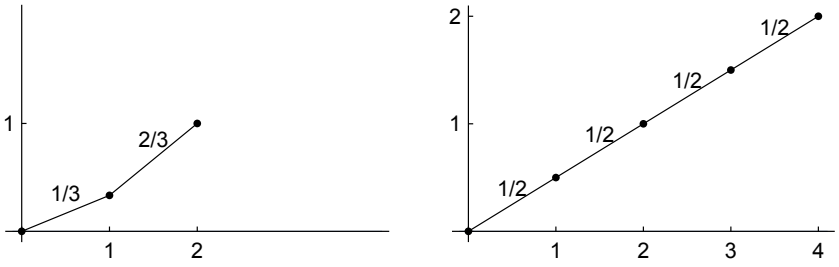
15.7. Ejercicios.

1. Chequear que la curva elíptica (17.5) realmente tiene invariante j igual a j.
2. Construir la tabla análoga a Tabla 1 para $p=5$.
3. Explorar la sección de la LMFDB sobre variedades abelianas sobre $\mathbb{F}_q$. Algunos posibles tópicos son:
   - ¿Cuán común es para A no ser una Jacobiana por que la curva correspondiente tendría un número negativo de puntos?
   - ¿Cuántos polígonos de Newton pueden ocurrir para un g dado y cuáles son sus frecuencias relativas aproximadas?
   - ¿Qué porcentaje de las clases de isogenía en la página (g,q) son primitivos?
4. Los puntos $(u_1,\ldots,u_g)$ en $Sp_{2g}^\natural$ correspondientes al rango angular 0 son aquellos con coordenadas enteras. Usar la factorización de polinomios de Frobenius unitarizados $f_p(x) = 1+u_1t+\cdots+u_1t^{2g-2}+1$ en polinomios ciclotómicos para contar el número N_g de tales puntos vía funciones generatrices. (Necesitarás considerar $\Phi_1(t) = t-1$

y $\Phi_2(t) = t + 1$ de manera diferente de los otros $\Phi_k(t)$, y tu respuesta debería dar $N_{10} = 20399$ como un caso especial.)

5. En la página de la LMFDB para superficies abelianas simples sobre cuerpos primos $\mathbb{F}_p$, encontrarás exactamente una clase de isogenía tal que el polinomio de Frobenius es reducible. ¿Qué es esto? Para una variedad abeliana de otras dimensiones sobre cuerpos primos $\mathbb{F}_p$, no encontrarás ningún polinomio irreducible. Explica cómo esto sigue de Teorema 17.1.
6. Lee en la literatura sobre el Teorema de Honda-Tate sobre $\mathbb{F}_q$ general. Da una segunda explicación para el fenómeno del ejercicio anterior en términos de obstruciones reales. Considera también los seguintes fenómenos que son visible en la LMFDB.
   - Los polinomios $1 \pm 2T + 8T^2$ no están en la página para curvas elípticas sobre $\mathbb{F}_8$. Sin embargo, $(1 \pm 2T + 8T^2)^3$ aparecen en la página de 3-variedades abelianas sobre $\mathbb{F}_8$ como los polinomios de Frobenius de variedades simples. Todas los demás 6458 polinomios de grado seis para variedades abelianas simples son irreducibles.
   - Los polinomios $1 + pT + p^2T^2 + p^3T^3 + p^4T^4$ se ven en las páginas para superficies abelianas sobre $\mathbb{F}_p$ para $p \leqslant 7$, pero no en la pagina para superficies abelianas sobre $\mathbb{F}_{11}$.

   Explica estos dos fenómenos en términos de obstruciones p-ádicas. Tu explicación debe hacer referencia a los polígonos de Newton siguientes, donde los números son las subidas verticales de los segmentos.



7. El grupo de Galois G de un polinomio conformalmente palíndromo $F_p(T) = 1 + a_1T + \cdots a_1p^{g-1}T^{2g-1} + p^gT^{2g}$ está en $2^g.S_g$, el grupo de orden $2^g g!$ que consiste de permutaciones de las raíces los cuales conmutan con la involución $\alpha \mapsto p/\alpha$ sobre las raíces. Probar que si $g \geqslant 2$ y $G = 2^g.S_g$, entonces el rango angular de $F_p(T)$ es g.

16. Variedades abelianas sobre $\mathbb{Q}$: generalidades ilustradas por curvas elípticas

Esta segunda clase de la tercera parte discute invariantes y la clasificación de variedades abelianas sobre $\mathbb{Q}$. Mostraremos el marco teórico para g arbitrario, pero centrándonos en el escenario relativamente familiar de $g = 1$. En particular, recalcaremos tres conjeturas de la década de 1960 para g general, las cuales están completamente resueltas únicamente para $g = 1$. Estas conjeturas y algunas otras abordan la cuestión de por qué uno querría tabular minuciosamente las variedades abelianas principalmente polarizadas: su aritmética es extremadamente rica.

Como ejemplos explícitos, tomamos

$$E_1 : y^2 = x^3 - x, \qquad \Delta_1 = 4 \qquad = 2^2, \qquad j_1 = 1728 \ = 2^6 3^3$$

$$E_2 : y^2 = x^3 + 6x - 7, \qquad \Delta_2 = -2187 = 3^7, \qquad j_2 = \frac{2048}{3} = \frac{2^{11}}{3}.$$

La curva E_1 tiene un automorfismo extra, $(x, y) \mapsto (-x, ix)$, definido sobre $\mathbb{Q}(i)$. En otras palabras, tiene multiplicación compleja potencial. Veremos de distintas formas que E_2 no tiene multiplicación compleja potencial; en otras palabras, es genérico.

16.1. Reducción buena versus reducción mala. Sea $A/\mathbb{Q}$ una variedad abeliana. Para p un primo, sea $\mathbb{Z}_{(p)}$ el anillo de números racionales con denominador coprimo a p. Entonces, se dice que A tiene *reducción buena* en p si existe un esquema abeliano $\underline{A}$ sobre $\mathbb{Z}_{(p)}$ con fibra genérica A. En caso contrario, se dice que A tiene *reducción mala* en p. El conjunto S de los primos malos es un invariante de isogenía.

Puede ser difícil identificar el conjunto S de reducciones malas de una $A/\mathbb{Q}$ dada, pero es usualmente fácil dar una cota superior razonable S' para él. Por ejemplo supongamos que A es la Jacobiana de $y^2 = f(x)$ con $f(x)$ un polinomio mónico en $\mathbb{Z}[x]$. Entonces uno puede tomar S' como 2 y los primos en los cuales $f(x)$ tiene un factor irreducible repetido cuando es reducido a $\mathbb{F}_p[x]$. Estos últimos primos son exactamente aquellos que dividen al discriminante Δ de $f(x)$. Luego, en nuestros ejemplos, $S'_1 = \{2\}$ y $S'_2 = \{2, 3\}$.

Un invariante fundamental de $A \in \mathrm{IsAb}_g(\mathbb{Q})$ más refinado que S es el entero positivo $N = \prod_p p^{c_p}$ llamado *conductor* de A. Los factores primos p de N son los primos de reducción mala de A. El exponente c_p en un primo p mide la naturaleza de la reducción mala: a mayor c_p, peor es la reducción. La magnitud de N es una medida importante de complejidad aritmética de A.

En nuestros casos,

$$N_1 = 32 = 2^5, \qquad N_2 = 72 = 2^3 3^2.$$

El factor 3^2 será explicado via representaciones módulo 2 al final de §18.10. De manera similar, los factores 2^c serán explicados allí vía una representación módulo 3.

16.2. Estrategia de clasificación. El punto de vista más usado para la aritmética es el de concentrarse primeramente en las clases de isogenía, y en las variedades abelianas dentro de una clase de isogenía en segundo lugar. Uno ordena las clases de isogenía con respecto al valor del conductor. Los invariantes geométricos juegan un papel secundario.

Para $g = 1$, las tablas clásicas ([16]) de Swinnerton-Dyer et al., publicadas en 1975, consideraron todos los casos hasta la cota 200 para el conductor. En el libro de Cremona de 1992 ([19]) se incrementó esta cota a 1000. La base de datos de Cremona actualmente llega hasta 400,000, y está en la LMFDB. Existen $1,741,002$ clases de isogenía y $2,483,649$ curvas, alrededor de 1.43 curvas por clase de isogenía.

La lista comienza a la izquierda de la tabla de abajo.

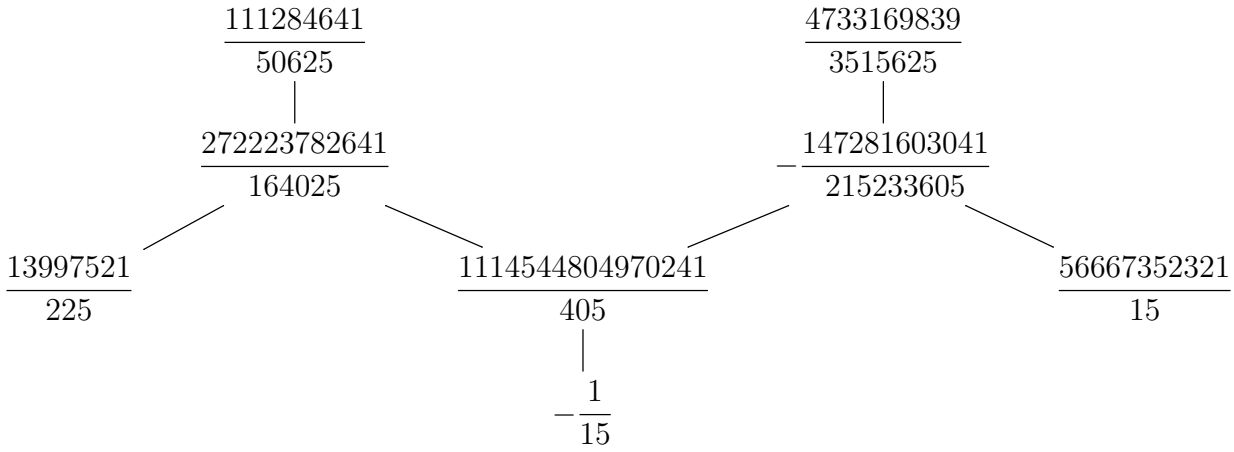
Conductor N	Número de curva elípticas	Número encontrado por una búsqueda muy rápida
11	3	1
14	6	1
15	8	1
17	4	1
19	3	1
20	4	1
21	6	1
24	6	1

En este rango, una clase de isogenía es determinada por su conductor, aunque ya para $N = 26$ existen dos clases de isogenía. También en este rango curvas diferentes dentro de una misma clase de isogenía tiene diferentes invariantes j, aunque para $N = 27$ hay dos curvas isógenas con el mismo invariante j.

Por diversión, los resultados de una muy corta búsqueda son presentados en la última columna. Las búsqueda consideró curvas elípticas en la "forma larga" estándar

$$y^2 + a_1xy + a_5y = x^3 + a_2x^2 + a_4x + a_6,$$

con $a_j \in \{-1, 0, 1\}$ para todo j. Encontramos exactamente una curva por cada uno de los primeras ocho clases de isogenía. El caso de $N = 15$, con las ocho invariantes j conectadas por 2-isogenías, es



La búsqueda encontró solo la curva con invariante j igual a -15. El diagrama ilustra que el tamaño N y la altura de j están muy débilmente relacionadas, así que es difícil encontrar todas las curvas elípticas de conductor pequeño buscando por las ecuaciones. La lista de Cremona fue calculada por el método modular discutido después de Teorema 18.8.

16.3. Funciones L como series de Dirichlet definidas por productos de Euler. Dado $A/\mathbb{Q}$ con reducción mala dentro de S', uno tiene inmediatamente infinitos invariantes, los factores locales $L_p(A, s) = F_p(A, p^{-s})$ de la primera clase (Section 17) para cualquier p que no está en S'. Estos son los correspondientes polinomios de Frobenius para nuestras dos curvas:

p	$F_p(E_1, T)$	$F_p(E_2, T)$
2	**1**	**1**
3	$1 + 3T^2$	**1**
5	$1 + 2T + 5T^2$	$1 - 2T + 5T^2$
7	$1 + 7T^2$	$1 + 7T^2$
11	$1 + 11T^2$	$1 + 4T + 11T^2$
13	$1 - 6T + 13T^2$	$1 + 2T + 13T^2$
17	$1 - 2T + 17T^2$	$1 + 2T + 17T^2$
19	$1 + 19T^2$	$1 + 4T + 19T^2$
23	$1 + 23T^2$	$1 - 8T + 23T^2$
29	$1 + 10T + 29T^2$	$1 + 6T + 29T^2$

Como lo indican los primeros tres símbolos **1** en la tabla, para $p \in S'$ existen también polinomios $F_p(A, T)$ bien definidos, que dan un factor local $L_p(A, s)$ por la misma substitución. Tiene grado $\leqslant 2g$ con desigualdad estricta exactamente cuando $p \in S$.

La función L asociada a A es

$$L(A, s) = \prod_p \frac{1}{L_p(A, s)} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{16.1}$$

(Notar que la inversión es forzada por el requerimiento de que $L(A, s)$ es la función L estándar sobre $\mathbb{Q}$ y $L_p(A, s)$ es la función L estándar sobre $\mathbb{F}_p$. En la literatura enfocada

únicamente en funciones L sobre $\mathbb{Q}$, uno usualmente encuentra que $L_p(A,s)$ significa lo que nosotros llamamos $1/L_p(A,s)$.)

El producto y la suma en (18.1) convergen absolutamente en el semi-plano derecho $\Re(s) > 3/2$. Por el momento, asuntos analíticos no jugarán ningún role, y uno puede considerar $L(A,s)$ como un paquete formal de cantidades $L_p(A,s)$, permitiendo las modificaciones en los finitos primos como describiremos abajo. Sea $\mathcal{L}_g(\mathbb{Q})$ el conjunto de todos estos productos formales.

Faltings [22] generalizó la parte de la inyectividad en Teorema de Honda-Tate, de tal manera que $i \in \mathrm{IsAb}_g(\mathbb{Q}) \to \mathcal{L}_g(\mathbb{Q})$ es inyectiva. Luego, el problema fundamental es caracterizar el conjunto numerable de la imagen dentro del dominio no numerable. En otras palabras, cuáles relaciones debe satisfacer una sucesión de polinomios para que aparezcan como una sucesión $F_p(A,T)$. Las tres conjeturas de abajo dan condiciones que se esperan que sean necesarias. Tal como lo veremos, se espera que la última condición esté cerca de ser suficiente.

16.4. Anillos de endomorfismos. No todas las clases de isogenía de variedades abelianas son creadas igual! Uno de los propósitos de los grupos de Galois motívicos G, y de sus variantes fáciles de los grupos de Sato-Tate ST, es hacer distinciones cualitativas entre clases de isogenía. Un principio simple es, *mientras más grande sea el grupo, más difícil será la aritmética*. Como un preludio de G y ST, discutiremos anillos de endomorfismos.

Una variedad abeliana A sobre un cuerpo K tiene el anillo de endomorfismos $\mathrm{End}(A)$ y el anillo de endomorfismos geométricos $\mathrm{End}(A_{\overline{K}})$. Para todo anillo de endomorfismos geométricos posible R, existe una correspondiente subvariedad X_R de A_g. Sus puntos complejos $X_R(\mathbb{C})$ por definición son la clausura del conjunto de los elementos x de $\mathrm{End}(A_x)$ isomorfos a R.

Para las curvas elípticas E sobre $\mathbb{Q}$, el anillo de endomorfismos $\mathrm{End}(E)$ es siempre $\mathbb{Z}$. Mientras que $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ es genéricamente $\mathbb{Z}$, también puede ser un anillo cuadrático R con discriminante negativo arbitrario D. En este caso, se dice que E tiene multiplicación compleja potencial E. La subvariedad X_R es irreducible de grado $h(D)$, lo que significa que $X_R(\mathbb{C})$ contiene $h(D)$ puntos, todos conjugados por $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Los siguientes casos donde $h(D) = 1$ son famosos:

D			j_D
-3			0
-4			1728
-7			-3375
-8			8000
-11			-32768
-12	$=$	$-3 \cdot 2^2$	54000
-16	$=$	$-4 \cdot 2^2$	287496
-19			-884736
-27	$=$	$-3 \cdot 3^2$	-12288000
-28	$=$	$-7 \cdot 2^2$	16581375
-43			-884736000
-67			-147197952000
-163			-262537412640768000

Así, E_1 tiene multiplicación compleja por -4 mientras que E_2 no tiene multiplicación compleja.

16.5. Grupos de Galois motívicos. Asociado a una variedad abeliana A sobre un subcuerpo K de $\mathbb{C}$ está su grupo de Galois motívico G. Éste es un subgrupo del grupo simpléctico conforme GSp_{2g}. Existen un número de definiciones competentes para G,

las cuales no son equivalentes en general. Nosotros tomamos la de Part I de [20], donde requiere que G fije los "ciclos de Hodge absolutos" en su acción natural $H^1(A(\mathbb{C}),\mathbb{Q}))^{\otimes 2j}\otimes \mathbb{Q}(j)$ donde $\mathbb{Q}(j)$ indica un "giro de Tate".

Omitiremos la definición completa de estos G, ya que tres propiedades de ellos son un substituto adecuado para estas notas. Primeramente, G siempre conmuta con $\mathrm{End}(A)$. En segundo lugar, la componente de la identidad G^0, también conocida como el grupo de Mumford-Tate, siempre conmuta con $\mathrm{End}(A_{\mathbb{C}})$. Finalmente , para $g \leqslant 3$, G^0 es siempre igual al conmutador completo en GSp_{2g} de $\mathrm{End}(A_{\mathbb{C}})$.

En el caso $g = 1$, el grupo simpléctico conforme GSp_2 no es más que otro nombre para GL_2, el cual es bien conocido por jugar un papel central en la teoría de curvas elípticas. El siguiente gráfico determina G:

	$\mathrm{End}(E)_{\mathbb{Q}}$	$\mathrm{End}(E_{\mathbb{C}})_{\mathbb{Q}}$	$G(\mathbb{Q})$
Genérico:	$\mathbb{Q}$	$\mathbb{Q}$	$GL_2(\mathbb{Q})$
Potential CM :	$\mathbb{Q}$	F	$N(F^\times)$
CM:	F	F	$F^\times$

Luego en el caso CM, G es un toro de dimensión dos. En el caso potencial CM, es el normalizador de este toro y por lo tanto tiene dos componentes.

16.6. Restricciones en los polinomios de Frobenius. Sea A una variedad abeliana sobre $\mathbb{Q}$. Su grupo de Galois motívico G actúa sobre sí mismo por conjugación y el espectro de la función invariante es su variedad de clase $G^\natural$. Para el mismo GSp_{2g}, la variedad de clase puede ser identificado con el conjunto de polinomios conformalmente palíndromos de grado $2g$, donde el factor conforme está dado. Los polinomios de Frobenius necesariamente viven en la imagen de $G^\natural(\mathbb{Q})$ en $GSp_{2g}^\natural(\mathbb{Q})$. Cuando G es estrictamente más pequeño que GSp_{2g}, se reduce drásticamente el conjunto de posibles polinomios de Frobenius para cualquier primo dado.

En el caso de curvas elípticas sobre $\mathbb{Q}$, las restricciones satisfacen para un polinomio de Frobenius de curvas elípticas con CM por D son como siguen. Primeramente, si $(D/p) = -1$ entonces $F_p(T) = 1 + pT^2$, tal como está ilustrado cinco veces por E_1 arriba. En segundo lugar, para $(D/p) = 1$, el discriminante de $F_p(T)$ debe ser D veces un cuadrado.

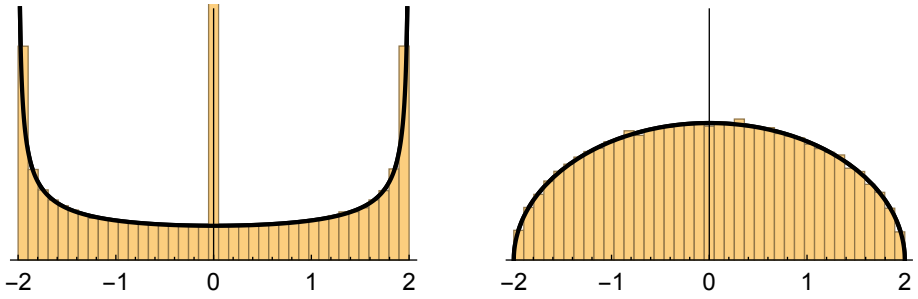
Para probar que una curva elíptica E sobre $\mathbb{Q}$ no tiene CM, no se debe usar el invariante j. Sólo se necesita mostrar que las condiciones mencionadas no son satisfechas. Por ejemplo, 5 y 13 son los primos menores p tales que $F_p(E_2, T)$ tiene un término lineal no nulo. Sus discriminantes módulo cuadrados son $d_5 = -1$ y $d_{11} = -7$. El hecho que $-1 \neq -7$ implica que $G = GL_2$. Proposición 19.1 de abajo explica cómo este simple cálculo tiene su análogo para $g \geqslant 2$.

16.7. Equidistribución arquimediana. La intersección de G con Sp_{2g} tiene una forma real compacta ST llamada el grupo de Sato-Tate de A. Como en §17.6, se puede pensar a ST como una versión no aritmética del grupo de Galois motívico: los giros de Tate han sido eliminados y el marco refinado de grupos reductivos ha sido reemplazado por los grupos compactos que son más familiares. Para curvas elípticas sobre $\mathbb{Q}$, existen sólo dos posibilidades para ST. Ellas son, ST es Sp_2 si E no tiene potencial CM, o sino es el normalizador $U_1.2$ de un toro U_1 en caso que sí lo tenga.

El grupo de Sato-Tate ST tiene una medida de probabilidad de Haar, la cual induce una medida de probabilidad μ_{ST} sobre el espacio de polinomios palíndromos $Sp_{2g}^\natural$. Para curvas elípticas E sobre $\mathbb{Q}$ las medidas en el u-intervalo $Sp_2^\natural = [-2, 2]$ para las dos posibilidades son las siguientes:

$$\mu_{U_1,2} = \frac{1}{2}\delta_0 + \frac{1}{2\pi\sqrt{4-u^2}}du, \qquad \mu_{Sp_2} = \frac{\sqrt{4-u^2}}{2\pi}. \tag{16.2}$$

Los siguientes gráficos consideran nuestros dos ejemplos, ubicando las primeras 100,000 trazas buenas de Frobenius en 39 compartimientos del mismo ancho. La barra del medio en el dibujo de la izquierda ha sido cortada, ya que debería ser nueve veces más alta. El acuerdo con las medidas de (18.2) es visualmente evidente.



En los primeros años de la década del 1960, Sato y Tate conjeturaron lo siguiente para el caso de curvas elípticas, con Sato inspirado por los datos que recién presentamos. Poco después, la siguiente conjetura general era de esperar, módulo el hecho que una definición rigurosa del grupo ST aún no había sido realizada.

Conjetura 16.1. Conjetura de Sato-Tate *Los polinomios buenos de Frobenius $F_p(A,T)$, considerados como puntos en $Sp_{2g}^\natural(\mathbb{R})$, están equidistribuidos con respecto a μ_{ST}.*

Una razón inicial para creer en esta conjetura fue que Deligne había probado un análogo con el cuerpo base $\mathbb{Q}$ reemplazado por $\mathbb{F}_p(t)$. También muchas personas habían encontrado evidencias numéricas para muchos ST sobre $\mathbb{Q}$, el cual es uno de los tópicos de la siguiente clase. El hecho de que la Conjetura 18.1 parezca verdadera es quizás la forma más rápida de ver la importancia de grupos de Galois motívicos.

La conjetura has sido largamente conocida para curvas elípticas con CM. El caso $g = 1$ fue probado completamente en una secuencia de artículos hace diez años, comenzando con [18].

Teorema 16.2. (Taylor et al.) *La conjetura de Sato-Tate es verdadera para $g = 1$.*

Su extensa demostración usa propiedades analíticas de no solo $L(E,s)$, sino también de funciones L $L(\mathrm{Sym}^k E, s)$ relacionadas a potencias simétricas.

16.8. Representaciones de Galois y equidistribución ℓ-ádica. Sea ℓ un número primo. Entonces $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ actúa en $H^1(A(\mathbb{C}),\mathbb{Q}_\ell)$ via la teoría de cohomología de étale. Como los ciclos de Hodge se comportan como ciclos algebraicos para variedades abelianas, lo cual fue probado por Deligne en la primera parte de [20], la imagen vive en $G(\mathbb{Q}_\ell)$.

Llevando la medida de probabilidad de Haar de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ hacia $GSp_{2g}^\natural(\mathbb{Z}_\ell)$ da una medida μ_ℓ. El Teorema de Densidad de Chebotarev nos dice que los polinomios característicos están definitivamente equidistribuidos con respecto a esta medida. Este hecho es obviamente un modelo para la conjetura general de Sato-Tate. Aunque en un sentido diferente, la situación ℓ-ádica es más complicada que la situación Arquimediana, pues existen muchas posibilidades para K_ℓ.

Otra conjetura que resalta la importancia fundamental esperada de los grupos de Galois motívicos es la conjetura de la imagen abierta.

Conjetura 16.3. (Conjetura de la imagen abierta) *Sea A una variedad abeliana sobre $\mathbb{Q}$ con grupo de Galois motívico G. Entonces, para todo número primo ℓ, la imagen K_ℓ de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ es un subgrupo abierto de $G(\mathbb{Q}_\ell)$.*

Con la idea de ser menos abstractos en el caso $G = GSp_{2g}$, la conjetura dice que la imagen tiene índice finito en el grupo $GSp_{2g}(\mathbb{Z}_\ell)$ de puntos enteros.

De las tres conjeturas que estamos destacando, la actual es la que está establecida con mayor generalidad.

Teorema 16.4. (Serre et al.) *La Conjetura de la imagen abierta es verdadera para $g = 1$. Es también cierta si* $\mathrm{End}(A_{\mathbb{C}}) = \mathbb{Z}$ *y g es impar.*

El primer enunciado fue probado en 1972 por el artículo más citado de Serre [29]. Para el segundo, la hipótesis implica que $G = GSp_{2g}$.

En el resto de esta subsección, damos una idea de cómo se ve en términos computacionales en las instancias más simples. Consideramos únicamente representaciones mód ℓ. Este es el primer y más importante paso para el caso ℓ-ádico completo. Estas representaciones mód ℓ provienen de las acciones de Galois en $H^1(A(\mathbb{C}), \mathbb{F}_\ell)$. Si A varía en una clase de isogenía, estas representaciones pueden cambiar. Sin embargo, sus semisimplificaciones son todas iguales.

Para curvas elípticas, ésto puede hacerse explícitamente para cualquier ℓ de manera uniforme. Nosotros tratamos aquí solo el caso $\ell = 2$ y 3, con Figura 18.8 dándonos una guía.

Mód 2. Las representaciones mód 2 de una curva elíptica $y^2 = x^3 + bx + c$ depende del polinomio cúbico $x^3 + bx + c$ vía $GL_2(\mathbb{F}_2) = S_3$. Patrones de factorización λ_p y trazas a_p son coordenadas como en las dos columnas de la izquierda.

(16.3)

λ_p	a_p	$GL_2(\mathbb{F}_2)$ masa	E_1	E_2
3	1	1/3		
21	0	1/2		50038
1	0	1/6	100000	49962

Cuando x^3+bx+c es irreducible, la distribución del par (λ, a_p) entre las tres posibilidades depende de las masas en las columnas del medio. Ninguno de nuestros ejemplos se ajusta a este patrón, como el 2-factor de polinomios de división:

$$x^3 - x = (x+1)x(x-1), \qquad x^3 + 6x - 7 = (x-1)(x^2 + x + 7).$$

The masses governing the two cases are not $(1/3, 1/2, 1/6)$ but rather $(0, 0, 1)$ and $(0, 1/2, 1/2)$. In el ejemplo, las representaciones mód 2 son diferentes, aunque sus semisimplificaciones son la misma, lo que significa que a_p es siempre pare. Las curva de dos componentes $E_1(\mathbb{R})$ está graficada en Figura 3 y los tres puntos de 2-torsión están sobre el eje real, con $x = -1$, 0, y 1. Para una curva con una componente, como $E_2(\mathbb{R})$, existe exactamente un punto real de 2-torsión, el cual en el caso de E_2 es racional.

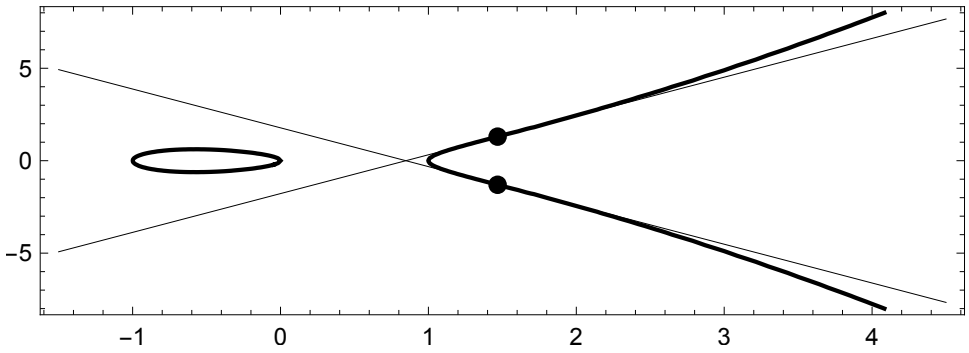


FIGURA 3. The curve $E_1(\mathbb{R})$. The two real 3-torsión points and their inflective tangents are highlighted.

Mód 3. Para ℓ un primo impar, hay relaciones de recursión clásicas que dan incluso polinomios $f_\ell(y)$ de grado ℓ^2-1 con raíces las y-coordenadas de los puntos de torsión en E de orden ℓ. Para abreviar, nosotros tratamos solo el caso $\ell = 3$, donde la geometría es particularmente atractiva.

Puntos distintos P, Q, y R sobre una curva elíptica $E : y^2 = x^3 + bx + c$ suman cero si y sólo si P, Q, y R viven sobre una línea. Por supuesto que, un punto P es un punto de 3-torsión si y sólo si $P + P + P = 0$. En este ejemplo, esta descripción geometrica de adición dice que P es un punto de 3-torsión si y sólo si es un punto de inflexión de la curva. Calculando puntos de inflexión de la forma que en un curso de cálculo de primer año, obtenemos que

$$f_3(y) = 27y^8 + 216cy^6 - 18\Delta y^4 - \Delta^2$$

es el polinomio de división buscado. Aquí no importa si $E(\mathbb{R})$ tiene una o dos componentes; siempre exactamente dos de los ocho puntos de 3-torsión son reales.

En los dos casos, las álgebras $\mathbb{Q}[y]/f(b_j, c_j, y)$ también son presentadas como $\mathbb{Q}[z]/g_j(z)$ para polinomios con coeficientes mucho más pequeños:

$$\begin{aligned} g_1(z) &= z^8 + 6z^4 - 3, & |\operatorname{Gal}_1| &= 16 & D_1 &= -2^{16}3^7, & d_1 &= -2^6 3^3 \\ g_2(z) &= z^8 + 4z^6 - 12z^2 - 12, & |\operatorname{Gal}_2| &= 48 & D_2 &= -2^{10}3^{11}, & d_2 &= -2^4 3^5. \end{aligned}$$

El tamaño del grupo de Galois $|\operatorname{Gal}_i|$, el discriminante D_j del álgebra $\mathbb{Q}[z]/f_j(z)$, y el discriminante d_j de $\mathbb{Q}[z]/f_j(\sqrt{z})$ son también indicados.

La siguiente tabla es análoga a (18.3), pero ahora para $\ell = 3$.

(16.4)

λ_p	$F_p(T)$	$GL_2(\mathbb{F}_3)$ masa	# for E_1	# for E_2
1^8	T^2+T+1	1/48	6253	2042
2^4	T^2-T+1	1/48	6246	2094
$3^2\,1^2$	T^2+T+1	1/6		16584
4^2	T^2+1	1/8	37463	12556
$2^3\,1^2$	T^2-1	1/4	25027	24952
8	T^2+T-1	1/8	12520	12545
8	T^2-T-1	1/8	12491	12541

Aquí, la última columna corresponde al número de primos entre 3, 5, ..., p_{100002} que tienen invariantes (λ_p, a_p). Como $\operatorname{Gal}_2 = GL_2(\mathbb{F}_3)$, la columna para E_2 es gobernada por la columna de masa impresa. Como Gal_1 es solo el subgrupo de 2-Sylow de $GL_2(\mathbb{F}_3)$, se rige por estadísticas diferentes. Uno puede correctamente suponer de la columna de E_1 que las frecuencias límites son $(1/16, 1/16, 0, 3/8, 1/4, 1/8, 1/8)$.

Para ℓ general, las clases de Frobenius pertenecen a $GL_2(\mathbb{F}_\ell)^\natural$, el conjunto de clases de conjugación del grupo $GL_2(\mathbb{F}_\ell)$. Notamos que el par de invariantes $(\lambda_p, F_p(T))$ determina estas clases completamente, donde ningún invariante por sí mismo es suficiente. En el caso $\ell = 3$, ambos invariantes determinan un conjunto cociente de siete elementos particular. Para λ_p, el problema es la repetición de 8's en su columna, mientras que para $F_p(T)$ el problema es la repetición de $T^2 + T + 1$.

Recordemos que un problema fundamental es caracterizar la imagen de $\mathrm{IsAb}_g(\mathbb{Q})$ en $\mathcal{L}_g(\mathbb{Q})$. El hecho que para qualquiera ℓ^e, los coefficientes de $L(A, s)$ son completamente determinados en $\mathbb{Z}/\ell^e$ por un cuerpo de números es una restricción muy fuerte.

16.9. Reducción mala en casos fáciles. Hicimos hincapié en §18.1 y§18.2 que la manera natural para clasificar variedades abelianas principalmente polarizadas es aumentando el conductor. Pero desde entonces no hemos dicho nada sobre reducción mala! En las dos subsecciones siguientes discutiremos brevemente este aspecto fundamental.

El estudio de la reducción mala de variedades abelianas es extremadamente complicado. In general, dados A sobre $\mathbb{Q}$ y un primo p, se tiene una descomposición de dimensión

$$g = g_{\text{good}} + g_{\text{mult}} + g_{\text{add}}.$$

El polinomio de Frobenius $F_p(A,T)$ tiene grado $2g_{\text{good}} + g_{\text{mult}}$. Raíces inversas correspondientes a la parte buena tienen el valor absoluto usual $\sqrt{p}$. De todas maneras, aquellos que corresponden a g_{mult} son raíces de la unidad. Abstractamente, los tres términos son respectivamente la dimensión de la parte buena, la parte toroidal, y la parte unipotente de la fibra especial del modelo de Néron para A.

In casos fáciles, las cantidad son calculables. Por ejemplo, en el marco hiperelíptico supongamos que $f(x)$ tiene polinomio discriminante divisible exactamente por p^k con $k \leqslant g$ y el polinomio reducido tiene la forma $a(x)b(x)^2$ con $b(x)$ de grado k. Entonces $(g_{\text{good}}, g_{\text{mult}}, g_{\text{add}}) = (g-k, k, 0)$. La parte buena de $F_p(T)$ viene desde la curva $y^2 = a(x)$ de género $g-k$, y la parte multiplicativa de $F_p(T)$ puede ser calculada desde las raíces de $b(x)$ y sus tangentes.

Escribiendo al conductor como $N = \prod p^{c_p}$, uno generalmente calcula los individuos c_p por separado. Se obtiene

$$c_p \geqslant g_{\text{mult}} + 2g_{\text{add}}.$$

La igualdad vale si y sólo si la ramificación es domesticada. Una condición suficiente para que la ramificación sea domesticada is que $p > 2g+1$. En el marco de la teoría de la ramificación, éste una propiedad simple, que se reduce al hecho que un grupo cíclico de orden p no puede actuar de manera no trivial sobre el espacio vectorial racional $H^1(A(\mathbb{C}), \mathbb{Q})$ de dimensión $2g$.

16.10. Reducción mala en casos difíciles. El famoso algoritmo de Tate determina las deseadas cantidades $F_p(A,T)$ y c_p directamente desde la ecuación de la curva elíptica. Un uso de polinomios de división es que, para un número primo p diferente de ℓ, la ramificación p-ádica en $\mathbb{Q}[y]/f_\ell(y)$ da información sobre el exponente $c_p = \text{ord}_p(N)$. Para esta aplicación, algunas veces es suficiente usar solo los dos primeros ℓ. En efecto, uno usa $\ell = 2$ para obtener información sobre los primos impares p, y luego uno usa $\ell = 3$ para resolver ambigüedades para $p \geqslant 5$ y obtener información sobre el caso más difícil $p = 2$.

Ejemplo 16.5. *Ejemplo de ramificación* 3*-ádica via representaciones mód* 2. Sea $y^2 = x^3 + bx + c$ con exponente conductor $c_3 = \text{ord}_3(N)$ y sea $x^3 + bx + c$ con exponente discriminante $\delta_3 = \text{ord}_3(D)$. Entonces, $c_3 \geqslant 3$ si y sólo si $\delta_3 \geqslant 3$; en este caso $c_3 = \delta_3$.

Ejemplo 16.6. *Ejemplo de ramificación* 2*-ádica via representaciones mód* 3. Sea $y^2 = x^3 + bx + c$ con exponente conductor $c_2 = \text{ord}_2(N)$ y sea $f_3(y)$ con exponente discriminante relativo $\delta_2 = \text{ord}_2(D/d)$. Supongamos que $\delta_2/4$ es la pendiente más larga en el cuerpo $\mathbb{Q}_2[y]/f_3(y)$, tal como ocurre en nuestros ejemplos. Entonces $c_2 = \delta_2/2$. En nuestro primer ejemplo se obtiene $c_2 = \text{ord}_2(D_1/d_1)/2 = 5$, mientras que en el segundo ejemplo se obtiene $c_2 = \text{ord}(D_2/d_2)/2 = 3$.

16.11. Funciones L como funciones analíticas de s. Definamos la siguiente modificación en la función Gamma estándar: $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$. La función L completa de una variedad abeliana g-dimensional es

$$\Lambda(A,s) := N^{s/2}\Gamma_C(s)^g L(A,s) \tag{16.5}$$

Como mencionamos previamente, el producto que define a $L(A,s)$ converge sólo para $\text{Re}(s) > 3/2$. Asimismo, nuevamente desde la década de 1960, se espera mucho más:

Conjetura 16.7. (Conjetura de la función L) *Para cualquier variedad abeliana A sobre $\mathbb{Q}$, $\Lambda(A,s)$ es una función entera, acotada en bandas verticales, y satisfaciendo*

$$\Lambda(A,s) = \pm\Lambda(A, 2-s). \tag{16.6}$$

La conjetura fue primeramente conocida para curvas elípticas con potencial CM. En los 1990s, la demostración para curvas elípticas fue muy famosa.

Teorema 16.8. (Wiles et al.) La Conjetura de la función L es verdadera para $g = 1$.

Su extensa demostración conecta curvas elípticas vía representaciones de Galois con formas modulares, y para las funciones L de formas modulares ya se sabía que tenían las propiedades analíticas deseadas.

Sea A una variedad abeliana sobre $\mathbb{Q}$ con álgebra de endomorfismos D con centro F. Sea $\dim_F(D) = d^2$. Entonces la función L $L(A, s)$ es la d-ésima potencia de una función que denotamos formalmente $L(A^{1/d}, s)$. Definimos $\Lambda(A^{1/d}, s) = N^{s/(2d)}\Gamma_{\mathbb{C}}(s)^{g/d}L(A^{1/d}, s)$. Entonces nuevamente se espera que Conjetura 18.7 sea cierta con A reemplazado por $A^{1/d}$. Más aún, podríamos ser más optimista y esperar que cualquier función que provenga de una variedad abeliana de esta manera satisfaga Conjetura 18.7. Esto sería una descripción de $\mathrm{IsAb}_g(\mathbb{Q})$ paralela a la descripción de Honda-Tate sobre $\mathrm{IsAb}_g(\mathbb{F}_q)$.

16.12. Ejercicios.

1. Realizar una más extensa búsqueda para curvas elípticas con $|a_1|$, $|a_2|$, $|a_3| \leqslant 1$ como antes, pero ahora con $|a_4|$, $|a_6| \leqslant 10$. ¿Cuántos de las 93 clases de isogenía con conductor $\leqslant 100$ se encontraron? ¿Cuántos de las 306 curvas se encontraron?
2. Explorar la sección de la LMFDB de curvas elípticas sobre $\mathbb{Q}$. Algunos posibles tópicos son:
   - ¿Cuáles conductores tienden una gran cantidad de clases de isogenía?
   - ¿Cuál es el significado de los enormes picos en las Z-función para la única curva de la base de datos con rango 4?
   - ¿Cuál es el conductor mínimo para el cual los trece invariantes j aparecen?
   - Confirmar en unos pocos casos que toda curva con conductor divisible exactamente por 2^4 o 2^6 es un giro cuadrático de una curva de conductor menor.
   - La curva $X_0(1200)$ tiene género 205. Notablemente, su Jacobiana es isógeno al producto de 205 curvas elípticas. ¿Cuántas clases de isogenía están involucradas? ¿Con cuáles multiplicidades?
3. Gross y Zagier probaron que todas las diferencias $j_D - j_{D'}$ con los j_D como en §18.4 se factorea en primos pequeños solamente. Por ejemplo, el código en *Magma* `Factorization(-3375+32768);` revela que la diferencia $j_{-7} - j_{-11}$ es $7 \cdot 13 \cdot 17 \cdot 19$. Intente adivinar rasgos de la fórmula general sin leer la referencia [24].
4. Los códigos de *Magma*
   ```
   E2 := EllipticCurve([6,7]);
   L2 := LSeries(E2);
   &+[(Coefficient(L2,NthPrime(j))/Sqrt(NthPrime(j)))^4 :
      j in [1..100000]]/100000;
   ```
   devuelven 1.995 . . . , mientras que el cuarto momento de la correspondiente medida es $m_4 = \int_{-2}^{2} \mu_{Sp_2} u^4 du = 2$. Éste es un ejemplo cuantitativo de cuán bien las sucesiones u_2, u_3, u_5, . . . encajan con la medida μ_{Sp_2}. Los m_k correctos son dados en la página de μ_{Sp_2} en la sección de Sato-Tate en la LMFDB. ¿Para cuáles k aseguran os primeros 100000 u_p el correcto m_k luego del redondeo?
5. El código
   ```
   F5T<T>:=PolynomialRing(FiniteField(5));
   E2 := EllipticCurve([6,7]);
   {*F5T!EulerFactor(E2,NthPrime(j)): j in [1..100000]*};
   ```

obtiene los primeros 100000 $F_p(E_2, T)$ como elementos de $\mathbb{F}_5[T]$. ¿Cuál subgrupo de $GL_2(\mathbb{F}_5)$ es la imagen de la representación mód 5? Repetirlo para E_1. ¿En qué lugar en la LMFDB está la respuesta?

6. *Magma* implementa para ℓ impares un polinomio de división de grado $(\ell^2-1)/2$ dando las coordenadas x de los puntos ℓ-división. El código

```
Qx<x>:=PolynomialRing(Rationals());
E1 := EllipticCurve([-1,0]);
DivisionPolynomial(E1,3);
```

devuelve este polinomio para la curva E_1 y $\ell = 3$. Repetirlo para $\ell = 5$, y utilice el "identifier" a [26] para obtener información sobre el comportamento 2-ádico de los dos polinomios. ¿Cómo comparan los pendientes 2-ádicos (dado en la columna "Galois slope content")? Repetirlo para E_2.

7. Vaya en la LMFDB de la página de E_1 hasta la página de su forma modular f_1, para apprender que $f_1 = q\prod_{n=1}(1-q^{4n})^2(1-q^{8n})^2 = \sum_{n=1}^{\infty} a_n q^n$, con los a_n exactamente los coefficientes de Dirichlet de $L(E_1, s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Escoje un número primo grande p y compute a_p de E_1. Independientemente, compute a_p de f_1. ¿Cómo comparan el tiempo de ejecución de los computaciones?

17. Variedades abelianas sobre $\mathbb{Q}$: ejemplos de superficies

En esta tercera clase continuamos la discusión de invariantes y clasificación, aunque ahora considerando con ejemplos del caso menos familiar de Jacobianas de curvas de género dos. Haremos contacto con cada una de las tres conjeturas mostradas en la clase anterior. Sin embargo, el punto principal es ilustrar cómo se ven las cosas desde un punto de vista computacional.

Como ejemplos explícitos de curvas, sean

(17.1)
$$C_1 : y^2 = (x-2)(x-1)(x+1)(x+2)\left(x^2-5\right), \quad \begin{matrix}\hat{\Delta}_1 & = 2^{24}3^4 5 \\ \Delta_1 & = 2^4 3^4 5\end{matrix}, \quad N_1 = 360 = 2^3 3^2 5,$$

(17.2)
$$C_2 : y^2 = x\left(x^2+1\right)\left(x^3-3x-4\right), \quad \begin{matrix}\hat{\Delta}_2 & = 2^{26}3^4 \\ \Delta_2 & = 2^6 3^4\end{matrix}, \quad N_2 = 2592 = 2^5 3^4.$$

La curva C_1 es especial porque no tiene solo la involución hiperelípticas $(x, y) \mapsto (x, -y)$, sino que además tiene la involución independiente $(x, y) \mapsto (-x, y)$. En contraste, veremos que C_2 tiene un comportamiento genérico.

17.1. Tablas de curvas con conductor pequeño. En general, consideremos una curva C de género dos presentada de la forma $y^2 + h(x)y = f(x)$, con $f(x) \in \mathbb{Z}[x]$ de grado seis $h(x) \in \mathbb{Z}[x]$ de grado $\leqslant 3$. Su discriminante es $\hat{\Delta} = 2^{10}|\mathrm{disc}(f + \frac{h^2}{4})|$. El discriminante Δ es el mínimo de todos estos $\hat{\Delta}$ y otros que provienen de presentaciones donde $f(x)$ tiene grado cinco (estos luego usualmente no son necesarios).

En general el conductor divide al discriminante: $N|\Delta$. La desigualdad $\mathrm{ord}_p(N) \leqslant \mathrm{ord}_p(\Delta)$ usualmente está cerca de ser una igualdad, tal como lo ilustran nuestros ejemplos. En particular, todos los primos que dividen exactamente a Δ, también dividen exactamente a N.

La LMFDB contiene los resultados de una extensa búsqueda [17] usando métodos muy eficientes para toda curva con $\Delta \leqslant 10^6$. La lista obtenida contiene 66158 curvas. La lista

comienza con

Conductor N	Número de género dos curvas en la LMFDB
169	1
196	1
249	2
256	1
277	2
294	2
295	2
324	1

Nuevamente la lista comienza con conductores determinando clases de isogenía. La primera repetición se da cuando $N = 576 = 2^6 3^2$.

Pero ahora la situación con respecto a la completitud está lejos de ser la configuración óptima de curvas de género 1. Primero, es probable que haya algunas curvas con Δ perdidas por la búsqueda. Mucho más en serio, hay casos con N debe ser menor que Δ. El artículo [17] da evidencia de que la lista puede estar completa con respecto a las clases de isogenía para $N \leqslant 1000$. El final de §19.3 nos muestra que a la clase isogenía de C_1 con $N = 360$ le faltan al menos cinco curvas. Los ejercicos da una clase de isogenía con $N = 1024$ también faltante.

17.2. Análogos de invariantes j. Sea

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

una curva de género dos con el polinomio $f(x) = cx^6 + \cdots$ teniendo raíces $\alpha_1, \ldots, \alpha_6$. Abreviamos $(\alpha_i - \alpha_j)^2$ por $[i, j]$. Entonces los invariantes de Igusa-Clebsch de la curva C explícitamente presentada son

$$\begin{aligned}
I_2 &= c^2\left([1,2][3,4],[5,6] + \text{the 14 like terms}\right),\\
I_4 &= c^4\left([1,2][2,3][3,1][4,5][5,6][6,4] + \text{the 9 like terms}\right),\\
I_6 &= c^6\left([1,2][2,3][3,1][4,5][5,6][6,4][1,4][2,5][3,6] + \text{the 59 like terms}\right),\\
I_{10} &= c^{10}\prod_{i<j}[i,j].
\end{aligned}$$

Cada I_k puede ser escrito como un polinomio en los coeficientes de $f(x)$, homogéneo de grado k.

Para estar a gusto con el resto de la literatura, uno debe conocer varias ligeras variantes. Por ejemplo, los invariantes de Igusa son

$$\begin{aligned}
J_2 &= I_2/8,\\
J_4 &= (4J_2^2 - I_4)/96,\\
J_6 &= (8J_2^3 - 160J_2J_4 - I_6)/576,\\
J_{10} &= I_{10}/4096.
\end{aligned}$$

La variedad de moduli compactada $\overline{M}_2$ para las curvas de género dos es el espectro proyectivo Proj$R$ del anillo graduado

$$R = \mathbb{Q}[I_2, I_4, I_6, I_{10}] = \mathbb{Q}[J_2, J_4, J_6, J_{10}].$$

La variedad M_2 en sí misma es el complemento de la hipersuperficie discriminante $I_{10} = 0$, o equivalentemente $J_{10} = 0$. Los invariantes de Igusa fueron introducidos ya que ellos se comportaban mejor cuando eran reducidos módulo 3 y 5. Cuando se complementa con un invariante similar J_8 se comportan bien cuando se reduce módulo 2.

El espacio M_2 es de dimensión 3 y singular. Sin embargo, se puede diseccionar inteligentemente en tres partes y volver a montar para crear el espacio afín ordinario de la siguiente manera. Definamos el invariante g por

$$(g_1,g_2,g_3)=\begin{cases}(J_2^5/J_{10}, & J_2^3/J_{10}, & J_2^2J_6/J_{10}) & \text{if } J_2\neq 0,\\ (0, & J_4^5/J_{10}^2, & J_4J_6/J_{10}) & \text{if } J_2=0 \text{ and } J_4\neq 0,\\ (0, & 0, & J_6^5/J_{10}^3) & \text{if } J_2=J_4=0.\end{cases} \tag{17.3}$$

Entonces vía (g_1,g_2,g_3), tenemos $M_2(K)=K^3$.

Tal como el invariante j, los invariantes g son números racionales típicamente de altura grande. Por ejemplo,

para C_1	para C_2
$g_1=28596971960000/81,$	$g_1=0,$
$g_2=1150492082200/81,$	$g_2=3125/3456,$
$g_3=6677950400/9,$	$g_3=-110/27.$

Nuevamente los denominadores son significativos, ya que reflejan que J_{10} es divisible por p si y sólo si $f(x)\in\mathbb{Z}[x]$ continúa teniendo seis raíces distintas en la línea proyectiva en característica p.

Es fácil calcular todos estes invariantes con *Magma*. Por ejemplo,

```
Qx<x>:=PolynomialRing(Rationals());
C2 := HyperellipticCurve([x*(x^2+1)*(x^3-3*x-4),0]);
G2Invariants(C2);
```

da el vector (g_1,g_2,g_3) de C_2 muy rapidamente.

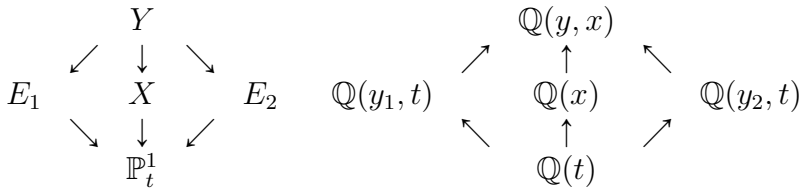
17.3. Una subvariedad clásica de A_2. Muchos anillos R surgen como anillos de endomorfismos de superficies abelianas que uno prácticamente puede enumerar. En consecuencia, hay muchas subvariedades naturales X_R de A_2, y la situación es mucho más complicada que la colección de subvariedades de dimensión cero X_D de A_1 tratada en §18.4. Discutimos solo una de las subvariedades más simples y clásicas, el de $R=\{(x,y)\in\mathbb{Z}^2 : x\equiv y\ (2)\}$. La ecuación para este X_R es ya muy complicada.

Sean E_1 y E_2 curvas elípticas sobre $\mathbb{Q}$ con todos los puntos de 2-torsion racionales. Se pueden escribir en la forma de Legendre como

$$\begin{aligned} y_1^2 &= t(t-1)(t-\lambda),\\ y_2^2 &= t(t-1)(t-\mu).\end{aligned}$$

Entonces, Legendre mostró que uno puede "pegar" $E_1=E_\lambda$ y $E_2=E_\mu$ en una curva de género dos como sigue.

A la izquierda tenemos un diagrama de curvas:



Aquí Y es el producto de las fibras de E_1 y E_2. Su cuerpo de funciones $\mathbb{Q}(Y)=\mathbb{Q}(t,y_1,y_2)$ es una extensión de grado cuatro del cuerpo base $\mathbb{Q}(t)$ con grupo de Galois que tiene cuatro elementos $(1,1)$, $(1,-1)$, $(-1,1)$, y $(-1,-1)$. El elemento (ϵ_1,ϵ_2) actúa por $y_1\mapsto\epsilon_1y_1$ y $y_2\mapsto\epsilon y_2$. La conducta de la ramificación presente nos dice que Y tiene género dos y el cociente $X:=Y/(-1,-1)$ con cuerpo de funciones $\mathbb{Q}(t,y_1y_2)$ tiene género cero.

Hay una coordenada x en X que lo identifica con la línea proyectiva $\mathbb{P}^1_x$ de tal manera que el mapeo a $\mathbb{P}^1_t$ toma la forma

$$t = \frac{\mu x^2 - \lambda}{x^2 - 1}.$$

Define

$$y = (-1+x)^2(1+x)^2(y_1+y_2).$$

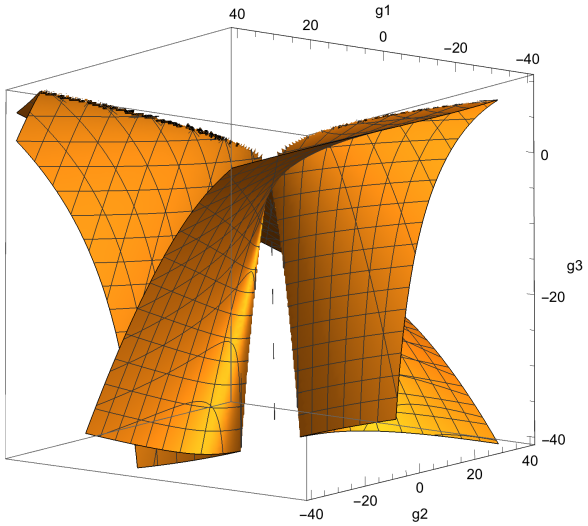
Eliminando variables obtenemos la curva de género dos deseada,

$$C_{\lambda,\mu}:\ y^2 = (\mu-\lambda)(x-1)(x+1)\left(\lambda-\mu x^2\right)\left(\lambda-\mu x^2+x^2-1\right). \tag{17.4}$$

Para obtener una ecuación para la subvariedad de M_2 correspondiente a esta construcción, calculamos los invariantes de Igusa (J_2, J_4, J_6, J_{10}) y buscamos una relación lineal entre los monomios en J_i de un grado dado. Estos monomios son polinomios gigantes en λ y μ. La primer relación lineal ocurre en grado 30, donde existen 47 monomios. Solo 29 de ellos están involucrados en la relación. Traduciendo a invariantes absolutos para el primer régimen de (19.3), la relación es

$$\begin{aligned}
&-51200000g_1^4 + 432g_1^5 - 28800g_1^4g_2 + 512000g_1^3g_2^2 - 8g_1^3g_2^3 + 512g_1^2g_2^4 - 8192g_1g_2^5\\
&+96000g_1^4g_3 - 11520000g_1^3g_2g_3 + 72g_1^4g_2g_3 - 4816g_1^3g_2^2g_3 + 84480g_1^2g_2^3g_3 - g_1^2g_2^4g_3\\
&+64g_1g_2^5g_3 - 1024g_2^6g_3 + 48g_1^4g_3^2 + 12960g_1^3g_2g_3^2 - 691200g_1^2g_2^2g_3^2 + 2g_1^3g_2^2g_3^2\\
&-136g_1^2g_2^3g_3^2 + 2304g_1g_2^4g_3^2 + 129600g_1^3g_3^3 - g_1^4g_3^3 + 72g_1^3g_2g_3^3 - 1080g_1^2g_2^2g_3^3\\
&-6912g_1g_2^3g_3^3 - 216g_1^3g_3^4 + 7776g_1^2g_2g_3^4 - 11664g_1^2g_3^5 = 0.
\end{aligned} \tag{17.5}$$

Por diversión, aquí tenemos un vistazo de la superficie $X(\mathbb{R})$ en el espacio real con coordenadas (g_1, g_2, g_3).



La curva C_1 fue construida por el método de esta subsección, con $(\lambda, \mu) = (-15, -3)$. En efecto, dividiendo ambos lados de la ecuación (19.4) de $C_{-15,-3}$ por 12^2 obtenemos la ecuación (19.1) de C_1. El primer factor E_{-15} es uno de las ocho curvas elípticas con conductor -15. Tres de estas curvas tiene 2-torsión partida, esta es E_λ con

$$\lambda \in \{-15, -9/16, 81\}.$$

El segundo factor E_{-3} es una de las seis curvas elípticas con conductor 24. Dos de estas curvas tienen 2-torsión partida, a saber E_μ con

$$\mu \in \{-3, 9\}.$$

Cuando se pegan las curvas elípticas de esta manera, las funciones L y los conductores se multiplican, así que $E_{-15,-3}$ tiene conductor $15 \cdot 24 = 360$. Cuando los factores de curvas

elípticas no son isógenas entre sí, la clase de isogenía se comporta multiplicativamente. Así la clase de isogenía $C_1 = E_{-15,-3}$ contiene exactamente $8 \times 6 = 48$ elementos. Al menos seis de estas 48 superficies abelianas tiene polarización principal, a saber las seis $E_{\lambda,\mu}$. Asimismo, la LMFDB actualmente tiene sólo C_1.

17.4. Polinomios de Frobenius y grupos de Galois motívicos. Evaluando (17.6) se obtienen polinomios de Frobenius buenos que ahora veremos. Los polinomios malos correctos son mostrados nuevamente en negrita. En el caso de C_1, todos los polinomios, buenos y malos, son conocidos por la construcción de pegar, como $F_p(C_1,T) = F_p(E_{-15},T)F_p(E_{-3},T)$. La columna $F_p(C_1,T)$ da $F_p(E_{-15},T)$ seguido de $F_p(E_{-3},T)$.

p	$F_p(C_1,T)$		$F_p(C_2,T)$
2	$(\mathbf{1+T+2T^2})$	$\mathbf{1}$	$\mathbf{1+T+2T^2}$
3	$(\mathbf{1+T})$	$(\mathbf{1+T})$	$\mathbf{1+2T+3T^2}$
5	$(\mathbf{1-T})$	$(\mathbf{1+2T+5T^2})$	$1+T+5T^3+25T^4$
7	$(1+7T^2)$	$(1+7T^2)$	$1+6T+18T^2+42T^3+49T^4$
11	$(1+4T+11T^2)$	$(1-4T+11T^2)$	$1-2T+6T^2-22T^3+121T^4$
13	$(1+2T+13T^2)$	$(1+2T+13T^2)$	$1+5T+24T^2+65T^3+169T^4$
17	$(1-2T+17T^2)$	$(1-2T+17T^2)$	$1-T-4T^2-17T^3+289T^4$
19	$(1-4T+19T^2)$	$(1+4T+19T^2)$	$1+30T^2+361T^4$
23	$(1+23T^2)$	$(1+8T+23T^2)$	$1+4T-2T^2+92T^3+529T^4$
29	$(1+2T+29T^2)$	$(1-6T+29T^2)$	$1-3T+32T^2-87T^3+841T^4$

Recordemos de §18.6 el formalismo de polinomios de Frobenius buenos $F_p(A,T)$ para una variedad abeliana A con grupo de Galois motívico G. Ellos viven en la imagen de $G^\natural(\mathbb{Q})$ en $GSp_{2g}^\natural(\mathbb{Q})$. Así que calculando secuencialmente $F_p(A,T)$ para más y más p, se obtiene una mejor cota inferior para G. Rápidamente se tiene un "buen pálpito" para G, el cual en la práctica es generalmente correcto. Por ejemplo, la columna $F_p(C_1,T)$ dice que la Jacobiana J_1 se parece al producto de dos curvas elípticas.

Proposición 17.1. *Sea A una variedad abeliana g-dimensional sobre $\mathbb{Q}$. Sean $F_p(A,T)$ y $F_q(A,T)$ dos polinomios de Frobenius con $\mathrm{Gal}(F_p(A,T)F_q(A,T))$ tan largo como sea posible, es decir, de orden $(2^g g!)^2$. Entonces, el grupo de Galois motívico de A es tan largo como es posible, a saber, GSp_{2g}.*

De hecho, si para un primo p se tiene que $|\mathrm{Gal}(F_p(A,T))| = 2^g g!$, entonces restan muy pocas posibilidades para G, por la classificación de subgrupos de grupos reductivos que contienen un toro maximal. Si para un segundo primo q, el subgrupo contiene un toro maximal completamente differente, la unica possibilidad es $G = GSp_{2g}$.

Es fácil de aplicar Proposición 19.1. Por ejemplo, $F_p(C_2,T)$ tiene grupo de Galois de orden 8 cuando $p \in \{5,11,13,17,23\}$. Ya los primeros dos de estos primos son suficientes, pues

```
Order(GaloisGroup(EulerFactor(C2,5)*EulerFactor(C2,11)));
```

devuelve 64.

17.5. Equidistribución arquimediana. Preparamos el escenario describiendo la equidistribución arquimediana en nuestros ejemplos. Las medidas de Sato-Tate en nuestros dos casos pueden ser escritos como densidades $f_{ST}dudv$. Las densidades son

$$f_{Sp_2\times Sp_2} = \frac{1}{2\pi^2}\sqrt{\frac{(-2u+v+2)(2u+v+2)}{u^2-4v+8}}, \tag{17.6}$$

$$f_{Sp_4} = \frac{\sqrt{(u^2-4v+8)\,(-2u+v+2)(2u+v+2)}}{4\pi^2}.$$

La equidistribución de clases de Frobenius $\mathrm{fr}_p = (u_p, v_p)$ es sabida en el primer caso, ya que se reduce a Teorema 18.1. No se conoce para el segundo. Los primeros cien fr_p en nuestros dos casos coinciden en la densidad de Sato-Tate, todas ilustradas en Figura 4.

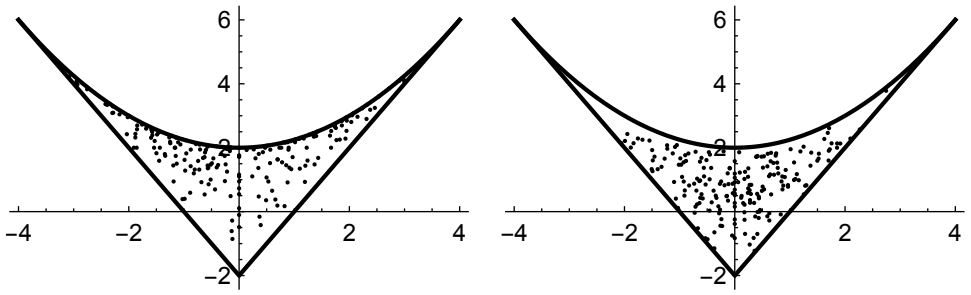


FIGURA 4. Puntos en el escudo $Sp_4^\natural$ representando el fr_p para los primeros cien primos buenos para C_1 (izquierda) y C_2 (derecha).

Algunas veces, como veremos pronto, uno se interesa solo en la distribución de a_1. La conjetura de Sato-Tate dice que estos son controlados por la medida de probabilidad inducida por μ_{ST} en $[-2g, 2g]$. Si la medida tiene una densidad, la cual es garantizada si ST es conexo, escribimos la densidad como ϕ_{ST}.

Para calcular la medida inducida en el eje u_1, hay que integrar las variables restantes. En nuestros casos integramos sobre v para obtener funciones en u:

$$\begin{aligned}\frac{24\pi^2\phi_{Sp_2\times Sp_2}}{u+4} &= \left(u^2+16\right)E\left(\frac{(u-4)^2}{(u+4)^2}\right) - 8uK\left(\frac{(u-4)^2}{(u+4)^2}\right)\\ \frac{240\pi^2\phi_{Sp_4}}{u+4} &= \left(u^4+224u^2+256\right)E\left(\frac{(u-4)^2}{(u+4)^2}\right)\\ &\quad - 8u\left(u^2+24u+16\right)K\left(\frac{(u-4)^2}{(u+4)^2}\right).\end{aligned} \tag{17.7}$$

Aquí, E y K son integrales elípticas completas clásicas. A pesar de su forma funcional complicada, el gráfico tiene una apariencia simple, como se muestra en Figura 5.

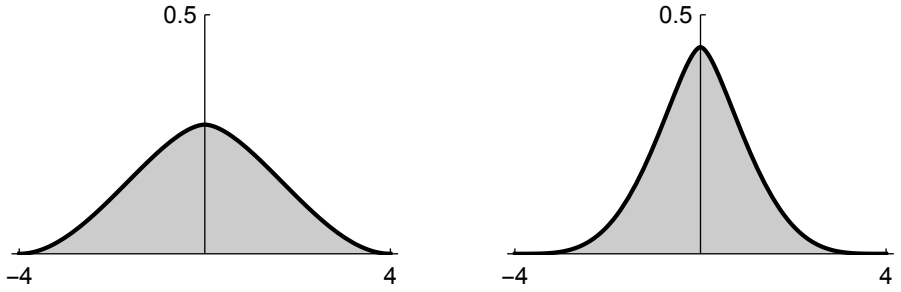


FIGURA 5. Medidas $\phi_{Sp_2\times Sp_2}$ y ϕ_{Sp_4} con varianza 2 y 1

La fórmula del carácter de Weyl da expresiones explícitas para $f_{Sp_{2g}}$ y $f_{Sp_2^g}$ para g general, similar en apariencia al caso $g = 2$ (19.6). De todas maneras, las funciones $\phi_{Sp_{2g}}$ y $\phi_{Sp_2^g}$ vuelve más complicadas cuando g crece. La ecuación diferencial lineal natural que ellos satisfacen tiene grado g y puntos singulares en $\{-2g, -2g+4, \ldots, 2g-4, 2g\}$ y ∞.

Rangos de endomorfismos vía el segundo momento. La dificultad de calcular $u_j = a_j/p^{j/2}$ en una clase de Frobenius $\mathrm{fr}_p = (u_1, \ldots, u_g)$ se aumenta rápidamente con j. Una situación típica cuando g es grande es que uno puede calcular una gran cantidad de u_1 pero ningún u_g. En esta situación, Proposición 19.1 no está disponible para ayudar a determinar los grupos de Galois motívicos G.

En este contexto se puede a veces hacer buenos pálpitos sobre G si uno asume la Conjetura de Sato-Tate. Escribiendo ahora u_p para la primera coordenada de fr_p, la conjetura asegura en particular que

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leqslant x} u_p^k = \int_{-2g}^{2g} \phi_{ST}(u) u^k du. \tag{17.8}$$

Calculando los radios finitos análogos para una x grande, uno puede intentar usar esta información para determinar algunos momentos m_k y luego ST mismo.

Los momentos para k impar son todos cero, y la atención se concentra en los momentos pares. El primer momento par no trivial m_2 es particularmente interesante, ya que es la dimensión de $\mathrm{End}(A)_{\mathbb{Q}}$. Luego, si $m_2 = 1$, existe solo la posibilidad de $\mathbb{Q}$. En general, escribiendo E_1, E_2, y E_4 para $\mathbb{R}$, $\mathbb{C}$, y $\mathbb{H}$ respectivamente, las posibilidades para $\mathrm{End}(A)_{\mathbb{R}}$ son

$$\bigoplus_i M_{j_i}(E_{d_i}) \tag{17.9}$$

con $\sum d_i j_i^2 = m_2$.

Clasicidad vía el cuarto momento. Se hace más difícil utilizar las clases de Frobenius para determinar con precisión m_k cuando k crece, ya que un análisis probabilístico suponiendo válida la Conjetura de Sato-Tate dice que la convergencia se vuelve más lenta. Sin embargo, uno aún puede identificar m_4 con confianza.

El cuarto momento es particularmente importante. Escribimos $G_{1,g}$, $G_{2,g}$, y $G_{4,g}$ para los grupos compactos Sp_{2g}, U_g, y $O_{g/2}$ en sus representaciones simplécticas naturales de dimensión $2g$. Candidatos fuertes para ST correspondiente al álgebra de endomorfismos (19.9) son

$$\prod_i G_{d_i,g_i}. \tag{17.10}$$

con $\sum_i g_i = g$. Tengamos en cuenta que si m_2 es grande admite una gran lista de posibilidades. Por ejemplo, $m_2 = 2$ permite muchos $Sp_{2g_1} \times Sp_{2g_2}$, y también U_g si g es par.

Un análisis relativamente fácil de los momentos, extendido en la discusión de los límites de Gauss que haremos a continuación, dice que

$$m_4 \geqslant 3m_2. \tag{17.11}$$

Supongamos, para hacer un enunciado limpio, que todos los g_i son al menos 2. Entonces, la alternativa de Larsen [27] nos dice que la igualdad vale si y sólo si G tiene el mismo grupo derivado que (19.10). "El mismo grupo derivado" es realmente necesario, ya que m_2 y m_4 no pueden distinguir entre U_g y SU_g, ni tampoco entre $O_{g/2}$ y $SO_{g/2}$. El caso más simple es el que se encuentra con mayor frecuencia en la práctica: *si* $(m_2, m_4) = (1, 3)$ *entonces* A *tiene grupo de Sato-Tate* Sp_{2g}.

Límites Gaussianos. La medida Gaussiana con promedio cero y varianza v en la línea u es $\mu_v = e^{-u^2/(2v)} du/\sqrt{2\pi v}$. Sus momentos pares son $m_k = v^{k/2}(k-1)!!$. Aquí, el doble factorial es como un factorial regular, excepto que uno baja por dos como en $7!! = 7\cdot5\cdot3\cdot1 = 105$. El grupo Sp_{2g} en su representación estándar de dimensión $2g$ tiene los mismos momentos para $k \leqslant g$ que μ_1, y entonces momentos más pequeños. Por ejemplo, los primeros momentos

pares para Sp_4 son $(m_2, m_4, m_6) = (1, 3, 14, \dots)$, lo cual es apenas inferior a los valores asintóticos $(1, 3, 15)$ alcanzados ya en $g = 3$. Del mismo modo, SU_g y $SO_{g/2}$ en sus representaciones estándares de dimensión $2g$ tienen momentos coincidiendo con μ_2 y μ_4 para $k \leqslant g - 1$.

En general la medida μ en $\mathbb{R}$ asociada con la representación de $G_1 \times G_2$ en $V_1 \oplus V_2$ es la convolución de las medidas μ_i asociadas con (G_1, V_1) y (G_2, V_2): $\mu = \mu_1 * \mu_2$. Las varianzas siempre se suman cuando convolucionamos y la convolución de dos Gaussianas es Gaussiana. La medida en $\mathbb{R}$ asociada a (G, V^m) es el reescalamiento por m de la medida asociada con (G, V), por lo que las varianzas aumentan por el factor m^2. Este dibujo muestra la densidad ϕ_G perteneciendo al grupo G de la forma (19.10) con mín(g_i) grande es muy cercana a una Gaussiana con promedio cero y varianza m_2.

Un ejemplo exótico en género dos. Describimos tres posibles grupos de Sato-Tate para curvas elípticas: Sp_2 y $U_1.2$ ocurren sobre $\mathbb{Q}$ y U_1 no lo hace. Para género dos, fue probado en [23] que son 34 las posibilidades que ocurren sobre $\mathbb{Q}$ y entonces 18 más possibilidades que solo ocurren sobre cuerpos de números más grandes . Cada uno de las 52 grupos tiene su propia página web en la sección de Sato-Tate de la LMFDB. Por supuesto, el número de posibilidades aumenta rápidamente con g.

Presentamos ahora un ejemplo de [23], el grupo llamado $J(O)$ allí . Como muchos de los 55 grupos, es construido a partir de un grupo finito G_1 y un grupo infinito G_2, cada uno en su propia representación 2-dimensional V_1 y V_2, y cada uno conteniendo la matriz escalar -1. El grupo de Sato-Tate es entonces $(G_1 \times G_2)/\{\pm(1, 1)\}$, actuando en el espacio 4-dimensional $V_1 \otimes V_2$.

En el caso que $ST = J(O)$, el grupo finito G_1 es $\tilde{S}_4 \subset Sp_2$, un cubrimiento doble de $S_4 \subset SO_3$, mejor pensado como rotaciones de un cubo en el 3-espacio. El grupo infinito es $G_2 = O_2$. Las medidas de probabilidad inducidas en el intervalo $[-2, 2]$ son

$$\begin{aligned} \mu_1 &= \frac{1}{48}\delta_{-2} + \frac{1}{8}\delta_{-\sqrt{2}} + \frac{1}{6}\delta_1 + \frac{3}{16}\delta_0 + \frac{1}{6}\delta_1 + \frac{1}{8}\delta_{\sqrt{2}} + \frac{1}{48}\delta_2 \\ \mu_2 &= \frac{1}{2}\mu_0 + \frac{dy}{2\pi\sqrt{4 - y^2}} \end{aligned}$$

Mientras que el producto semidirecto $O_2 = SO_2.2$ es un grupo diferente de la extensión no partida $U_1.2$, induce la misma medida en $[-2, 2]$.

Para esta construcción de producto tensoriales en general, el mapa natural envía un punto $(x, y) \in [-2, 2] \times [-2, 2]$ al punto $(u, v) = (xy, x^2 + y^2 - 2)$ en el escudo $Sp_4^\natural$. La medida $\mu_1 \times \mu_2$ avanza hacia la medida deseada μ_{ST}. En el caso $ST = J(O)$ uno obtiene

$$\mu_{J(O)} = \frac{3}{16}\delta_{p_2} + \frac{1}{6}\delta_{p_3} + \frac{1}{8}\delta_{p_4} + \frac{1}{48}\delta_{p_1} + \frac{3}{16}\nu_{V_2} + \frac{1}{6}\nu_{C_3} + \frac{1}{8}\nu_{C_4} + \frac{1}{48}\nu_{C_1}. \tag{17.12}$$

Así, la medida $\mu_{J(O)}$ tiene la mitad de su soporte sobre cuatro puntos especiales en la Figura 2, y la otra mitad en cuatro curvas especiales. Las ν_C son medidas de probabilidad. Son todas trasladadas de la medida con densidad $f(y) = 1/(\pi\sqrt{4 - y^2})$ sobre $[-2, 2]$ y cero afuera. Por consequencia, le medida unidimensional sobre $[-4, 4]$ es

$$\nu_{J(O)} = \frac{11}{16}\delta_0 + \frac{f(u)}{6} + \frac{f\left(u/\sqrt{2}\right)}{8\sqrt{2}} + \frac{f\left(u/2\right)}{96}. \tag{17.13}$$

La imagen de esta medida en la página web de $J(O)$ en la LMFDB es redibujada en Figura 6. Desde un punto de vista inocente, es sorprendente que uno podría mirar cientos de curvas y ver sólo una distribución siempre de tipo Gaussiano de Figura 5, y luego de repente encontrarse con $\nu_{J(O)}$ desde la inofensiva curva $y^2 = x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$.

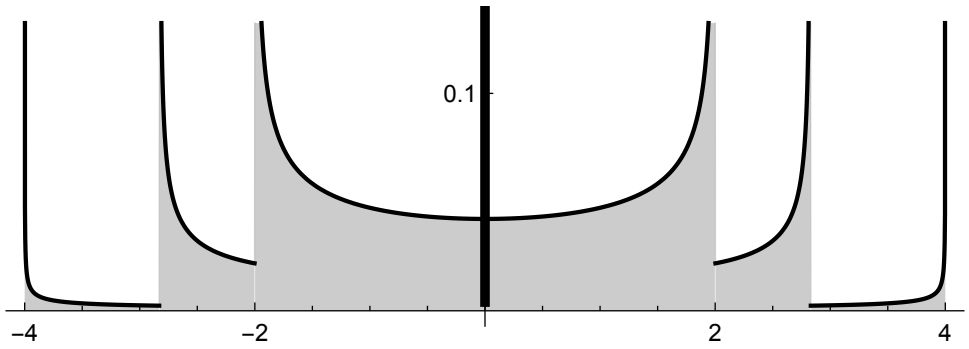


FIGURA 6. La medida Sato-Tate $\nu_{J(O)}$ de (19.13), con masa 11/16 a 0 y la masa restante dada por una densidad discontinua.

La receta para momentos es aún más fácil. Supongamos μ_{G_1} y μ_{G_2} en el intervalo $[-2,2]$ tienen momentos m'_k y m''_k respectivamente. Entonces los momentos de ν_{ST} en $[-4,4]$ son $m_k = m'_k m''_k$. Siempre, todos los momentos impares se anulan. En nuestro ejemplo, los momentos pares son

(17.14)

			m_2	m_4	m_6	m_8
G_1	=	$\tilde{S}_4$	1	2	5	15
G_2	=	O_2	1	3	10	35
ST	=	$J(O)$	1	6	50	525

Los momentos para G_1 y G_2 son calculados por métodos diagramados simples en el último ejercicio. Los momentos para ST están dados en la página web de $J(O)$ en la LMFDB.

17.6. Representaciones de Galois mód ℓ. Para curvas hiperelípticas $y^2 = f(x)$ la representación mód 2 está dada con la curva. A saber, el grupo de Galois $\mathrm{Gal}(f(x))$ está en S_{2g+2} y se tiene una inclusión

$$S_{2g+2} \to GSp_{2g}(\mathbb{F}_2).$$

Para $g = 1$ y $g = 2$, esta inclusión es suryectiva, reflejando el hecho que curvas elípticas y curvas de género dos son siempre hiperelípticas. Para $g = 3$, las 28 bitangentes sobre una curva cuártica le permiten a uno obtener la representación mód 2 nuevamente, aunque para $g \geqslant 4$ fórmulas explícitas parecen fuera del alcance para curvas generales.

Para $g \geqslant 2$ y $\ell \geqslant 3$, solo hay un caso para el cual uno tiene polinomios universales. Este caso único es el primer caso, $g = 2$ y $\ell = 3$. Un polinomio de grado 80 par para $y^2 = x^5 + bx^3 + cx^2 + dx + e$ es

(17.15)

$$f_3(b,c,d,e;x) = x^{80} + 15120\,b\,x^{76} + 2620800\,c\,x^{74} + (419237280\,d - 35394408\,b^2)\,x^{72} + \cdots$$

Expandido como un elemento de $\mathbb{Z}[b,c,d,e,x]$, tiene 1673 términos.

Tal como enfatizamos en el caso de género uno, representaciones mód ℓ tienen diferentes propósitos. Uno de ellos es dar acceso independiente a polinomios de Frobenius reducidos

a $\mathbb{F}_\ell[T]$. Nuestros dos casos son muy degenerados:

λ_p	$F_p(T) \in \mathbb{F}_2[T]$	$GSp_4(\mathbb{F}_2)$ mass	C_1	C_2
1^6	$(1+T)^4$	1/720	49977	16569
$2\,1^4$	”	1/48	50023	50051
2^3	”	1/48		
$2^2\,1^2$	”	1/16		
$4\,2$	”	1/8		
$4\,1^2$	”	1/8		
$3\,1^3$	$(1+T)^2\,(1+T+T^2)$	1/18		33380
$3\,2\,1$	”	1/6		
3^2	$(1+T+T^2)^2$	1/18		
6	”	1/6		
$5\,1$	$1+T+T^2+T^3+T^4$	1/5		

La división de la tabla en cuatro bloques muestra muy claramente cómo un polinomio de Frobenius determina solo la parte semisimple de una clase de conjugación. Aunque la masa $GSp_{2g}(\mathbb{F}_\ell)$ se convierte en equidistribuida en el espacio de polinomios característicos $GSp_{2g}^\natural(\mathbb{F}_\ell)$ en el límite $\ell \to \infty$, existen notables discrepancias para ℓ pequeño. Los cuatro bloques en orden contienen respectivamente $35.\overline{5}\,\%$, $22.\overline{2}\,\%$, $22.\overline{2}\,\%$, y $20\,\%$ de la masa.

Otro propósito de representaciones mód ℓ, descriptas ya en §18.10, es el de analizar la reducción mal. Como un ejemplo de esto, aplicamos (19.15) a la curva C_2 buscando información sobre la reducción mala de C_2 en 2. Cambiando coordenadas en (19.2) vía $(x,y) \mapsto (-100/(15+x), -20y/(15+x)^3)$ para expresar C_2 como una ecuación de quinto grado, evaluamos (19.15) en $(b,c,d,e) = (7750, -117500, -9009375, 2418212500)$. La factorización en irreducibles en $\mathbb{Q}_2[x]$ tiene la forma $f_{8r}(x)f_{8u}(x)f_{64}(x)$. El factor mayor no tiene que ser estudiado y el sitio web de [26] dice que $f_{8u}(x)$ es no ramificado. Applicando este sitio web en una manera menos trivial muestra que $f_{8r}(x)$ tiene grupo de Galois D_2 de orden 16. Muestra también que el grupo de inercia es el grupo de cuaterniones de orden 8. El “Galois slope content” allí, $[2,2,5/2]^2$, indica la filtración de ramificación de D_2. En particular, la única possibilidad para la valuación 2-ádica de la conductor de C_2 es dos veces lo mayor pendiente, a saber $2 \cdot (5/2) = 5$.

17.7. Cálculos numéricos con funciones L. Para curvas de género dos con grupo de Sato-Tate genérico, Conjetura 18.7 es desconocida. Notablemente, uno puedo todavía calcular con una precisión muy alta. Dados los polinomios de Frobenius en (19.4), las posibilidades localmente permitidas por el conductor son 2^a3^b con $0 \leqslant a \leqslant 8$ y $0 \leqslant b \leqslant 5$, como in el caso de curvas elípticas. Usando *Magma*'s `CFENew` para examinar todas las posibilidades da los siguientes números.

$a\backslash bb$	0	1	2	3	4	5
..0	0.65071	0.53189	0.41151	0.29208	0.16978	0.02654
1	0.57620	0.45586	0.33611	0.21589	0.08433	0.10492
2	0.50034	0.38017	0.26069	0.13567	0.02104	0.37675
3	0.42438	0.30489	0.18337	0.04423	0.18654	3.82310
4	0.34890	0.22900	0.09975	0.07776	0.66956	0.62849
5	0.27357	0.14983	0.00069	0.30666	0.00000	0.23470
6	0.19678	0.06112	0.14992	1.69170	0.40104	0.07216
7	0.11473	0.05313	0.51913	0.79266	0.15720	0.04627
8	0.01843	0.25073	3.19710	0.27365	0.02061	0.15698

Estos números sugieren fuertemente que el conductor correcto es $2^5 3^4$. Los escépticos podrían probablemente considerar todavía a $2^5 3^2$ como una posibilidad. Se puede usar más precisión así:

```
ZT<T>:=PolynomialRing(Integers());
CFENew(LSeries(C2:
    LocalData:=[<2,5,1+T+2*T^2>,<3,2,1+2*T+3*T^2>],Precision:=30));
```

Este código devuelve

$$0.00069191183229691135350870962 1 \text{ para } 2^5 3^2 \text{ en } 0.39 \text{ segundos.}$$

Pero un cambio de $c_3 = 2$ a $c_3 = 4$ da

$$0.000000000000000000000000000000 \text{ para } 2^5 3^4 \text{ en } 1.26 \text{ segundos.}$$

Una prueba de Conjetura 18.7 espera progreso en las conexiones con formas automorficas. Pero cálculos significativos ya son possibles, incluso en mayores dimensiones g.

17.8. Ejercicios.

1. La curva

$$C_3 : y^2 + x^3 y = x^5 - 5x^3 - 10x^2 - 8x - 2 \tag{17.16}$$

   tiene conductor $40000 = 2^6 5^4$ y está en la LMFDB. ¿Su punto moduli (g_1, g_2, g_3) vive en la subvariedad $X_{1+2\mathbb{Z}^2}$ de (19.5)?.
2. La LMFDB reporta que el grupo de Sato-Tate ST de (19.16) es $J(C_4)$. Tiene dimensión uno y grupo componente $C_2 \times C_4$. Más aún, la componente conteniendo a Fr_p depende solo del símbolo del residuo cuadrático $(-8/p)$ y la clase de p en $\mathbb{F}_5^\times$. Identificar la medida $\mu_{J(C_4)}$ en el escudo $Sp_{2g}^\natural$. (El soporte consiste de tres puntos especiales con medida $1/2$, y entonces tres curvas, también con medida $1/2$. Mucha orientación adicional se da en la página de $J(C_4)$.)
3. Pegue $E_1 : y^2 = x(x-1)(x+1)$ a una segunda copia de la misma curva dada por $E_2 : y^2 = x(x-1)(x-2)$, usando (19.4) para obtenir una curve C_4. El discriminante de C_4 debería ser el número grande $\Delta = 2056589122535424 = 2^{16} 3^{22}$. ¿Porqué es `LocalData:=[<2,10,1>,<3,0,(1+T^2)^2>]` la información local correcta? Chequear que C_4 pasa `CFENew` a treinta decimales. (Notar que esta curva tiene grupo de Sato-Tate $C_{2,1}$ y ningún ejemplo de este grupo existe actualmente en la LMFDB. Notar también que hay un salto grande del gran discriminante Δ al pequeño conductor $N = 1024$.)
4. Consideremos la curva $C_5 := y^2 = x^6 - 1$. ¿Cuál es su discriminante? ¿Is isomorfo a C_4? ¿Parece su Jacobiana ser isógeno a la Jacobiana de C_4?
5. Los momentos de $\tilde{S}_4$ se calculan por el diagrama extendido de Dynkin de tipo $\tilde{E}_7$:

$$\begin{array}{ccccccccccccc} \mathbf{1} & — & 2 & — & 3 & — & 4 & — & 3 & — & 2 & — & 1 \\ & & & & & & \vert & & & & & & \\ & & & & & & 2 & & & & & & \end{array}$$

   A saber, m_k es el número de paseos de longitud k que empiezan y terminan al punto $\mathbf{1}$. Verifique que los valores dados en (19.14) sean correctos. Repitelo por $G_2 = O_2$ y el digrama extendido de Dynkin de tipo $\tilde{D}_\infty$:

$$\begin{array}{ccccccccccc} \mathbf{1} & — & 2 & — & 2 & — & 2 & — & 2 & — & \cdots \\ & & \vert & & & & & & & & \\ & & 1 & & & & & & & & \end{array}$$

   ¿Cuál es el significado de los números en los vértices?

Referencias

[1] O. Debarre, *Tores et variétés abéliennes complexes*. EDP Sciences, 1999.
[2] C. Birkenhake y H. Lange, *Complex Abelian varieties*. Springer-Verlag, 1992.
[3] G. Cornell y J. H. Silverman (ed.), *Arithmetic Geometry*. Springer-Verlag, 1986.
[4] G. van de Geer y B. Moonen, *Notes on Abelian varieties*. preliminary notes accessible on: http://www.mi.fu-berlin.de/users/elenalavanda/BMoonen.pdf
[5] R. Hartshorne, *Algebraic geometry*. Springer-Verlag, 1977.
[6] M. Hindry y M. Rebolledo, *Introducción a la teoría de las curvas elípticas*. Notas de curso para AGRA II, Cusco 2015. Accessible `https://webusers.imj-prg.fr/~harald.helfgott/agraweb/AGRAIIMarcMarusia.pdf`
[7] M. Hindry y J. Silverman, *Diophantine Geometry. An introduction*. .Springer-Verlag, 2000.
[8] J. Milne, *Abelian varieties*. In [3], 103–150.
[9] J. Milne, *Jacobian varieties*. In [3], 167–212.
[10] J. Milnor, *Curvatures of left invariant metrics on Lie groups*, Adv. Math. **21**:3 (1976), 293–329. DOI: 10.1016/S0001-8708(76)80002-3.
[11] D. Mumford, *Abelian varieties*. Oxford U. Press, 1970.
[12] D. Mumford, *Curves and Jacobians*. Univ. of Michigan, 1975.
[13] M. Rosen, *Abelian varieties over* $\mathbb{C}$. In [3], 76–102.
[14] J. Silverman, *Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
[15] J. Silverman, *Advanced Topics on the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.
[16] *Numerical tables on elliptic curves*. In "Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)", Lecture Notes in Math. **476**, 74–144, Springer, Berlin, 1975.
[17] A.R. Booker, J. Sijsling, A.V. Sutherland, J. Voight, D. Yasaki, *A database of genus-2 curves over the rational numbers*. LMS J. Comput. Math. **19**, 235–254 (2016). DOI 10.1112/S146115701600019X.
[18] L. Clozel, M. Harris, R. Taylor, *Automorphy for some l-adic lifts of automorphic mód l Galois representations*. Publ. Math. Inst. Hautes Études Sci. **108**, 1–181 (2008). DOI 10.1007/s10240-008-0016-1.
[19] J.E. Cremona, *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 1997.
[20] P. Deligne, J. S. Milne, A. Ogus, K-y Shih. *Hodge cycles, motives, and Shimura varieties*. Lecture Notes in Mathematics, 900. Springer-Verlag, Berlin-New York, 1982.
[21] S.A. DiPippo, E.W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*. J. Number Theory **73**, 426–450 (1998). DOI 10.1006/jnth.1998.2302.
[22] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73**, 349–366 (1983). DOI 10.1007/BF01388432.
[23] F. Fité, A.V. Kedlaya, K.S. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*. Compos. Math. **148**, 1390–1442 (2012). DOI 10.1112/S0010437X12000279.
[24] B.H. Gross, D.B. Zagier, *On singular moduli*. J. Reine Angew. Math. **355**, 191–220 (1985).
[25] T. Honda, *Isogeny classes of abelian varieties over finite fields*. J. Math. Soc. Japan **20**, 83–95 (1968). DOI 10.2969/jmsj/02010083.
[26] J.W. Jones, D.P. Roberts, *A database of local fields*. J. Symbolic Comput. **41**, 80–97 (2006). DOI 10.1016/j.jsc.2005.09.003.
[27] N.M. Katz, *Larsen's alternative, moments, and the monodromy of Lefschetz pencils*. In "Contributions to automorphic forms, geometry, and number theory", 521–560, Johns Hopkins Univ. Press, Baltimore, MD, 2004.
[28] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*. In "Effective methods in algebraic geometry (Castiglioncello, 1990)", 313–334, Progr. Math. **94**, Birkhäuser Boston, Boston, MA, 1991.
[29] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**, 259–331 (1972). DOI 10.1007/BF01405086.
[30] J. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2**, 134–144 (1966). DOI 10.1007/BF01404549.
[31] W.C. Waterhouse, *Abelian varieties over finite fields*. Ann. Sci. École Norm. Sup. (4) **2**, 521–560 (1969).

Université Paris Diderot Paris 7, France
E-mail address: `marc.hindry@imj-prg.fr`

Université Clermont Auvergne, France
E-mail address: `marusia.rebolledo@uca.fr`

University of Minnesota, Morris, Minnesota 56267, USA
E-mail address: roberts@morris.umn.edu