Publicaciones Matemáticas del Uruguay
Volumen 18, Diciembre 2023, Páginas 287–365
S 0797-1443

VARIEDADES ABELIANAS, UNA INTRODUCCIÓN

MARC HINDRY, MARUSIA REBOLLEDO, Y DAVID ROBERTS

Resumen. Variedades abelianas son grupos algebraicos que, al mismo tiempo, son variedades algebraicas proyectivas. El primer 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).

Índice

Versión final: 18 de mayo de 2019.
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.

Introducción

Variedades abelianas son grupos algebraicos que, al mismo tiempo, son variedades algebraicas proyectivas. El primer 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, pues 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 una descripción aritmética de variedades abelianas sobre un cuerpo finito $\mathbb{F}_q$ y sobre el cuerpo racional $\mathbb{Q}$.

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 la 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 sección corresponde directamente a partes particulares de la base de datos.

Se puede encontrar referencias generales sobre variedades abelianas complejas en [1, 7, 12, 14], variedades abelianas y jacobianas sobre un cuerpo cualquiera en [4, 7, 9, 10, 12, 13]. Para variedades abelianas con dimensión 1, es decir curvas elípticas en [6, 15, 16]. Se reúne material más avanzado sobre variedades abelianas en [27, 30, 35, 37, 38], información computacional y base de datos sobre curvas elípticas y variedades abelianas de dimensión 2 en [18, 19, 20, 22, 28, 34].

Agradecimientos. Los tres autores desean expresar su gratitud a los organizadores de la escuela y en particular a Emilio Lauret por su apoyo lingüístico. También agradecen al referí anónimo por sus observaciones precisas.

David Roberts fue apoyado por la subvención DMS-1601350 de la NSF.

Parte 1. Variedades abelianas complejas

Definición 0.1. Una *variedad abeliana* es un grupo algebraico conexo que es también una variedad proyectiva.[1]

[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.

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.

Ejemplo 0.2. Vieron, en el curso de teoría de Galois, que las curvas algebraicas definidas por una ecuación afín de la forma $y^2 = x^3 + ax + b$ con $4a^3 + 27b^2 \neq 0$ tienen una estructura de grupos algebraicos. Así estas curvas, llamadas *curvas elípticas* son variedades abelianas de dimensión 1.

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. Luego, vamos a examinar si todos los toros complejos son variedades abelianas complejas. Las referencias principales para esta parte son: [1, 12, 7, 14] y [9].

1. Toros complejos

1.1. 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 (Proposición 1.3) 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: [12].

1.1.1. 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 $V = Lie(T) = \mathrm{Tan}_e(T)$ el espacio tangente a T en e ; es el álgebra de Lie asociada a T. Es un espacio vectorial de dimensión igual a la dimensión de T como variedad compleja.

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 cero) de $\mathrm{Tan}_0(\mathbb{C})$ sobre v.[3]

Definición 1.1. 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 implícitas, se deduce que la aplicación exp es un difeomorfismo local en un entorno de $0 \in V$ hacia un entorno de $e \in T$.

Lema 1.2. *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 $x = \exp(v_1) \ldots \exp(v_n)$.*

[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 $\mathbb{P}^n(\mathbb{C})$.

[3]Se puede pensar en λ_v como en la geodésica sobre T que parte de e y tiene dirección v.

Demostración. Como exp es un difeomorfismo local en 0, $\exp(V)$ 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 $\langle \exp(V)\rangle$ es un abierto de T. Como también es cerrado[4], la conexidad de T implica $\langle \exp(V)\rangle = T$. □

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

$$F \circ \exp_{T_1} = \exp_{T_2} \circ (dF)_e, \tag{1.1}$$

es decir el siguiente diagrama conmuta:

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

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

Proposición 1.3. *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;*[5]
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[6]. 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.

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 $\mathrm{End}(V)$, entonces es constante. En consecuencia, tenemos para todo $x \in T$, $(df_x)_e = (df_e)_e = \mathrm{id}_V$.

Se deduce de (1.1) 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 (Lema 1.2), entonces T es conmutativo.

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

[5]o suryectivo, o exhaustivo, como el lector prefiera.

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

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 todo $t \in \mathbb{C}, x, y \in V$. 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 difeomorfismo 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 1.4. *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.

1.2. Cuando un toro complejo es una variedad abeliana. En Subsección 1.1, 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.

Ejemplo 1.5. Consideramos un toro $\mathbb{C}/\Lambda$ de dimensión 1, o sea Λ es un retículo de $\mathbb{C}$. Denotamos por $\wp_\Lambda$ la *función de Weierstrass* definida por

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) \quad (z \in \mathbb{C}).$$

Entonces $u_\Lambda : z \mod \Lambda \mapsto (1 : \wp_\Lambda(z) : \wp'_\Lambda(z))$ define una inmersión holomorfa de $\mathbb{C}/\Lambda$ en $\mathbb{P}^2(\mathbb{C})$. Además la imagen de $\mathbb{C}/\Lambda$ en $\mathbb{P}^2(\mathbb{C})$ tiene ecuación $y^2 = 4x^3 - g_2(z)x - g_3(z)$ donde g_2, g_3 han sido definidas por ejemplo en el curso de teoría de Galois en este volumen, es decir es una curva elíptica sobre $\mathbb{C}$. Recíprocamente, para toda curva elíptica E sobre $\mathbb{C}$, existe un retículo Λ de $\mathbb{C}$ tal que la aplicación u_Λ de antes define un isomorfismo de grupos de Lie del toro $\mathbb{C}/\Lambda$ en $E(\mathbb{C})$. Es el famoso *teorema de uniformización*. Entonces, en dimensión 1 las nociones de toros, variedades abelianas y curvas elípticas coinciden.

Pero lamentablemente, no es verdad en dimensión > 1. Teorema 1.8 da condiciones necesarias y suficientes para que un toro complejo de dimensión $g > 1$ sea una variedad abeliana. Daremos las líneas principales de la demostración en las subsecciones 2.3.1 y 2.3.3.

Sea V un $\mathbb{C}$-espacio vectorial de dimensión g. 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 1.6. *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 1.7 (Forma de Riemann)**.** Diremos que una forma hermitiana $H : V \times V \to \mathbb{C}$ 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 1.8. *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.*

Ejemplo 1.9 (Curvas elípticas)**.** Vimos en Ejemplo 1.5 que los toros de dimensión 1 son todos curvas elípticas (entonces variedades abelianas). Eso es confirmado por el teorema precedente. En efecto, sea $\Lambda = Z\lambda_1 + \mathbb{Z}\lambda_2$ con $\Im(\lambda_1/\lambda_2) > 0$ y consideramos la forma hermitiana sobre $\mathbb{C} \times \mathbb{C}$ definida por

$$H(z, w) = \frac{z\bar{w}}{\Im(\lambda_1\bar{\lambda_2})} \quad ((z, w) \in \mathbb{C} \times \mathbb{C})).$$

Se puede verificar que H es una forma de Riemann no degenerada (ejercicio).

Ejemplo 1.10. Consideramos el toro $A_\tau = \mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$ donde $\tau \in M_g(\mathbb{C})$ es una matriz simétrica tal que $\Im(\tau)$ es definida positiva. Entonces

$$H(z, w) = {}^t z\Im(\tau)^{-1}\bar{w} \quad ((z, w) \in \mathbb{C}^g \times \mathbb{C}^g)$$

define una forma de Riemann no degenerada sobre T_τ (ejercicio). Entonces A_τ es una variedad abeliana.

Ejemplo 1.11 (Variedades abelianas con multiplicación compleja)**.** Sea $K/\mathbb{Q}$ una *extensión 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 $\mathbb{C}^g/f(\mathcal{O})$. Se puede demostrar que $K = K^+(\xi)$ con $\xi \in \mathcal{O}_K$ tal que $-\xi^2$ es un elemento totalmente positivo en K^+ y para todo $k \in \{1, \ldots, g\}$, $\Im(\varphi_k(\xi)) > 0$. Definimos una forma a valores reales, $\mathbb{R}$-bilineal antisimétrica por

$$E(z, w) = \sum_{k=1}^{g} \varphi_k(\xi)(\bar{z}_k w_k - z_k \bar{w}_k), \qquad (z, w \in \mathbb{C}^g). \tag{1.2}$$

La forma $E(iz, w)$ es simétrica, definida positiva. Se puede además demostrar que para todos $x, y \in K$, tenemos

$$E(f(x), f(y)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi\tilde{x}y) \tag{1.3}$$

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).

La variedad abeliana así obtenida es dicha *a multiplicación compleja por $\mathcal{O}$, de tipo CM (K, Φ)*.

1.3. Morfismos e isogenías. Para que una aplicación entre dos toros $f : T_1 = V_1/\Lambda_1 \to T_2 = V_2/\Lambda_2$ sea un *morfismo*, queremos que respecte las estructuras de grupos de Lie, es decir que sea una aplicación holomorfa y un morfismo de grupos. De hecho, tenemos el lema:

Lema 1.12. *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 $\mathbb{C}$-afín $\tilde{f} : V_1 \to V_2$ 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. Ver [7, Lema A.5.1.1, p. 93] o [3, Teorema I.2.3, p. 7]. □

Definición 1.13. 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 1.14. Si $\varphi : T_1 \to T_2$ es una isogenía, entonces $\dim(T_1) = \dim(T_2)$.

Ejemplo 1.15 (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, $\ker[n] = (1/n)\Lambda/\Lambda \cong \Lambda/n\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. Así tenemos una inyección $\mathbb{Z} \hookrightarrow \mathrm{End}(T)$.

Ejemplo 1.16 (Dimensión 1)**.** Consideramos un toro de dimensión 1: $E = \mathbb{C}/\Lambda$ con Λ un retículo de $\mathbb{C}$. Por Lema 1.12, el anillo $\mathrm{End}(E)$ de los endomorfismos de E es isomorfo al conjunto R de los números complejos $\alpha \in \mathbb{C}$ tales que $\alpha\Lambda \subset \Lambda$. Todo retículo de $\mathbb{C}$ es homotético a un retículo de la forma $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, con $\tau \in \mathbb{C}, \Im(\tau) > 0$. Así, podemos suponer, sin pérdida de generalidad, que $\Lambda = \Lambda_\tau$ para un tal τ. Si $\alpha\Lambda \subset \Lambda$, entonces, en particular, existen $a, b, c, d \in \mathbb{Z}$ tales que $\alpha = a + b\tau$ y $\alpha\tau = c + d\tau$. Eso implica

$$\alpha^2 - (d + a)\alpha + (da - cb) = 0 \tag{1.4}$$

entonces α es un entero cuadrático. Además si $\mathbb{Z} \neq R$, $b \neq 0$ y tenemos

$$b\tau^2 + (a - d)\tau - c = 0 \tag{1.5}$$

Desde (1.4) y (1.5), deducimos que R es un orden del cuerpo cuadrático imaginario $\mathbb{Q}(\tau)$.

Así, para E curva elíptica sobre $\mathbb{C}$, $\mathrm{End}(E) \cong \mathbb{Z}$ o $\mathrm{End}(E)$ es un orden de un cuerpo cuadrático imaginario.

En el caso de una variedad abeliana de dimensión > 1, es más complicado.

Ejemplo 1.17 (Variedad abeliana CM)**.** Sea $K/\mathbb{Q}$ una extensión CM y $A = \mathbb{C}^g/f(\mathcal{O})$ una variedad abeliana CM por un orden $\mathcal{O}$ de K, de tipo CM (K, Φ) (ver Ejemplo 1.11). Entonces, hay una inmersión $\mathcal{O} \hookrightarrow \mathrm{End}(A); \alpha \mapsto f_\alpha$, donde f_α es inducida por la multiplicación por $f(\alpha)$ en $\mathbb{C}^g$: $f_\alpha : (z_1, \ldots, z_g) \in A \mapsto (\varphi_1(\alpha)z_1, \ldots, \varphi_g(\alpha)z_g) \in A$.

Más generalmente, el anillo $\mathrm{End}(A)$ 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 $\mathrm{End}_0(A)$. Decimos que un toro es *simple* si no tiene ningún subtoro no trivial. Se puede demostrar:

Proposición 1.18. *Si A es simple, entonces* $\mathrm{End}_0(A)$ *es un álgebra de división (un cuerpo que puede ser no conmutativo).*

Ver Sección 4 para una descripción más avanzada de $\mathrm{End}_0(A)$.

1.4. Descomposición salvo isogenía. 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 1.19. *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*.*

Teorema 1.20 y Corolario 1.21 que siguen, dan la descomposición de las variedades abelianas salvo isogenía. Aquellos requieren la existencia de una forma de Riemann no degenerada sobre el toro considerado.

Teorema 1.20 (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. Ver [7, Teorema A.5.1.7, p. 95]. Denotamos $A = V/\Lambda$ y $B = V_1/\Lambda_1$ donde $V_1 \subset V$ y $\Lambda_1 = \Lambda \cap V_1$. Sea H una forma de Riemann no degenerada asociada a A. Es natural considerar el ortogonal de B para esta forma: consideramos

$$V_2 := \{v \in V : H(v, v_1) = 0;\ \text{para todo } v_1 \in V_1\}$$

y $\Lambda_2 = \Lambda \cap V_2$. Se puede demostrar que:

$$V_2 = \{v \in V : E(v, v_1) = 0 \text{ para todo } v_1 \in V_1\}$$

y $\Lambda_2 = \{v \in \Lambda : E(v, v_1) = 0;\ \text{para todo } v_1 \in V_1\} = \{v \in \Lambda : E(v, v_1) = 0;\ \text{para todo } v_1 \in \Lambda_1\}$ es un submódulo de Λ de rango igual a $rg(\Lambda) - rg(\Lambda_1)$ porque E es no degenerada y Λ_1 es un retículo (ejercicio). Entonces Λ_2 es un retículo de V_2 (pues de rango igual a $2\dim_{\mathbb{C}}(V_2)$) y $C := V_2/\Lambda_2$ es una subvariedad abeliana de A con forma de Riemann $H|_{V_2 \times V_2}$. Como $V_1 \oplus V_2 = V$, tenemos $B + C = A$ y $B \cap C$ finito. □

Corolario 1.21. *Toda variedad abeliana A es isógena a un producto de la forma $A_1^{n_1} \times \cdots \times A_s^{n_s}$ donde $A_1, \ldots, A_s$ 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. Se deduce de Teorema 1.20 y Proposición 1.18 por inducción. Ver [7, Corolario A.5.1.8, p. 96]. □

2. 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 1.8. En toda esta sección, denotamos por $T = V/\Lambda$ un toro complejo con V un $\mathbb{C}$-espacio vectorial de dimensión g y Λ un retículo de V. La elección de una base de V nos permite suponer que $V = \mathbb{C}^g$.

Deseamos determinar bajo que condiciones existe una inmersión holomorfa de T 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, una aplicación holomorfa u es una inmersión si y sólo si es inyectiva y si du es inyectiva en todo punto.

Es natural de considerar una aplicación u que provenga de $\tilde{u} = (u_0, \dots, u_n) : V \to \mathbb{C}^{n+1}\backslash\{0\}$ con $u_0, \dots, u_n$ holomorfas y sin cero común. Una tal aplicación induce $u : V/\Lambda \to \mathbb{P}^n(\mathbb{C})$, si para todo $(z, \lambda) \in V \times \Lambda, \tilde{u}(z + \lambda) \equiv \tilde{u}(z) \in \mathbb{P}^n(\mathbb{C})$ o sea si para todo (z, λ), existe un escalar $g_\lambda(z)$ tal que para todo $k \in \{0, \dots, n\}$, $u_k(z + \lambda) = g_\lambda(z)u_k(z)$. Eso motiva la definición de las funciones theta.

Referencias principales: [3, 7, 14].

2.1. Funciones theta y formas de Riemann.

2.1.1. Funciones theta. Para todo $t \in \mathbb{C}$, denotamos $\mathbf{e}(t) = \exp(2i\pi t)$. En lo que sigue, denotamos $V = \mathbb{C}^g$ y Λ un retículo de V.

Definición 2.1 (Función theta)**.** Una *función theta relativa a* Λ es una función meromorfa[7] $\theta : V \to \mathbb{C}$ que satisface una ecuación de la forma

$$\theta(z + \lambda) = \mathbf{e}(f_\lambda(z)).\theta(z) \qquad ((z, \lambda) \in V \times \Lambda) \tag{2.1}$$

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 theta.

Observación 2.2. La ecuación (2.1) determina L de manera única, pero J es definido a menos de agregación de un entero.

Ejemplo 2.3. Toda función de la forma $z \mapsto \exp(F(z))$ donde F es un polinomio de grado total $\leqslant 2$ es una función theta llamada *trivial*. Más precisamente, si $F(z) = \varphi(z, z) + R(z) + S$ con φ una forma bilineal simétrica, R una forma lineal y S una constante, el tipo de $\exp(F)$ es $(\frac{1}{i\pi}\varphi(z, \lambda), \frac{1}{2i\pi}(\varphi(\lambda, \lambda) + R(\lambda))$ (ejercicio).

Ejemplo 2.4.

1. Sea Λ un retículo de $\mathbb{C}$. La función $\sigma : \mathbb{C} \to \mathbb{C}$ definida por:

$$\sigma(z) := z \prod_{\lambda \in \Lambda\backslash\{0\}} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right) \tag{2.2}$$

   es una función theta relativa a Λ llamada *función sigma de Weierstrass* (ver Ejercicio 6.1).

2. Sean a, b reales. La función definida por:

$$\theta(z) = \sum_{m \in \mathbb{Z}} \exp(i\pi\tau(m + a)^2 + 2i\pi(m + a)(z + b)) \tag{2.3}$$

   es una función theta relativa a $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$.

   Más generalmente, consideramos $\tau \in M_g(\mathbb{C})$ simétrica tal que $\Im(\tau)$ sea definida positiva y $\Lambda_\tau = \mathbb{Z}^g + \tau\mathbb{Z}^g$ el retículo de $\mathbb{C}^g$ como en Ejemplo 1.10. La función definida por

$$\theta(z) = \sum_{m \in \mathbb{Z}^g} \exp(i\pi {}^t m\tau m + 2i\pi {}^t mz) \tag{2.4}$$

   es una función theta relativa a Λ_τ llamada *función theta de Riemann* (ver Ejercicio 6.2).

[7]Cuidado: en algunas referencias, las funciones theta son definidas como holomorfas. Aquí permitimos que sean meromorfas.

2.1.2. Forma de Riemann asociada a una función theta. Sea θ una función theta de tipo (L, J) relativamente a Λ. La relación (2.1) implica que para todos $\lambda_1, \lambda_2 \in \Lambda, z \in V$, tenemos

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

de lo que deducimos

$$L(z, \lambda_1 + \lambda_2) = L(z, \lambda_1) + L(z, \lambda_2) \tag{2.5}$$

$$L(\lambda_1, \lambda_2) \equiv J(\lambda_1 + \lambda_2) - J(\lambda_1) - J(\lambda_2) \quad (\text{mód } \mathbb{Z}) \tag{2.6}$$

$$L(\lambda_1, \lambda_2) \equiv L(\lambda_2, \lambda_1) \quad (\text{mód } \mathbb{Z}) \tag{2.7}$$

De (2.5), 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

$$E(z, w) = L(z, w) - L(w, z) \quad ((z, w) \in V \times V) \tag{2.8}$$

es a valores reales, $\mathbb{R}$-bilineal alternada y, por (2.7), tiene valores enteras sobre $\Lambda \times \Lambda$. Además, para todo $(z, w) \in V \times V$, $E(iz, iw) = E(z, w)$ (ejercicio). Entonces, E define una forma de Riemann (Lema 1.6): $H_\theta(z, w) = E(iz, w) + iE(z, w)$.

Así, a una función theta θ le asociamos la forma de Riemann H_θ. Observamos que H_θ depende sólo de L donde (L, J) es el tipo de θ.

Decimos que dos funciones theta θ_1, θ_2 son *equivalentes* y lo denotamos $\theta_1 \sim \theta_2$, si θ_1/θ_2 es una función theta trivial.

Observación 2.5. Si dos funciones theta tienen mismo tipo (L, J) entonces son equivalentes.

Proposición 2.6.

1. *Sean dos funciones theta θ_1, θ_2, entonces $H_{\theta_1\theta_2} = H_{\theta_1} + H_{\theta_2}$.*
2. *Si θ es una función theta trivial entonces $H_\theta = 0$. Si θ_1, θ_2 son dos funciones theta equivalentes, entonces $H_{\theta_1} = H_{\theta_2}$.*

Demostración.

1. Para $i = 1, 2$, denotamos por (L_i, J_i) el tipo de θ_i. Entonces, $\theta_1\theta_2$ es una función theta de tipo $(L_1 + L_2, J_1 + J_2)$. Se deduce 1.
2. Desde Ejemplo 2.3, deducimos que si θ es trivial entonces $L = \frac{1}{i\pi}\varphi(z, w)$ es simétrica (con las notaciones del ejemplo), lo que implica $E_\theta = 0$. Así $H_\theta = 0$. De eso y de 1., también se deduce que si $\theta_1 \sim \theta_2$ entonces $H_{\theta_1} = H_{\theta_2}$.

□

2.1.3. Función theta normalizada. En la clase de equivalencia de una función theta hay una función theta particular que llamamos *normalizada*.

Lema 2.7. *Sea θ una función theta y $H = H_\theta$ la forma de Riemann asociada. Entonces existe una función theta $\widetilde{\theta}$ equivalente a θ tal que*

$$\widetilde{\theta}(z + \lambda) = \mathbf{e}\left(\frac{1}{2i}H(z, \lambda) + \frac{1}{4i}H(\lambda, \lambda) + K(\lambda)\right)\widetilde{\theta}(z) \qquad ((z, \lambda) \in V \times \Lambda) \tag{2.9}$$

donde $K : \Lambda \to \mathbb{R}$ y verifica

$$K(\lambda + \mu) - K(\lambda) - K(\mu) \equiv \frac{1}{2}E(\lambda, \mu) \quad (\text{mód } \mathbb{Z}). \tag{2.10}$$

Además, existe $c > 0$ tal que, para todo $z \in V$,

$$|\widetilde{\theta}(z)| \leqslant c. \exp\left(\frac{\pi}{2}H(z, z)\right). \tag{2.11}$$

La función $\tilde{\theta}$ es llamada *función theta normalizada asociada a* θ (o a H). La función ψ definida por $\psi(z) = \mathbf{e}(K(z))$ verifica

$$\psi(\lambda+\mu) = \psi(\lambda)\,\psi(\mu)\,\mathbf{e}\left(\frac{1}{2}E(\lambda,\mu)\right) \tag{2.12}$$

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

Demostración. Sea (L, J) el tipo de θ y $H = H_\theta$. Toda función θ_1 en la clase de equivalencia de θ tiene un tipo (L_1, J_1) donde $L_1(z,w) = L(z,w) + \frac{1}{i\pi}\varphi(z,w)$ con φ una forma bilineal simétrica (ver Ejemplo 2.3). Deducimos que $L_1(z,w) - L_1(w,z) = L(z,w) - L(w,z) = E(z,w)$ (lo que implica $H_{\theta_1} = H$ como en Proposición 2.6). Recíprocamente, si L_1 es tal que

$$L_1(z,w) - L_1(w,z) = E(z,w) \tag{2.13}$$

entonces $L_1 - L$ es una forma bilineal simétrica. Con $\varphi := i\pi(L_1 - L)$ y para toda forma lineal R, la función $\theta_1 = \theta_{L_1,R}$ definida por $\theta_1(z) = \exp(\varphi(z,z) + R(z))\theta(z)$ tiene tipo (L_1, J_1) con $J_1(\lambda) \equiv J(\lambda) + \frac{1}{2i\pi}(\varphi(\lambda,\lambda) + R(\lambda))$ (mód $\mathbb{Z}$). Como $E = \Im(H)$, la forma bilineal $L_1(z,w) = \frac{1}{2i}H(z,w)$ verifica (2.13). La función theta asociada $\theta_R(z) = \theta_{\frac{1}{2i}H(z,w),R}$ es de tipo $\left(\frac{1}{2i}H(z,\lambda), \frac{1}{4i}H(\lambda,\lambda) + K_R(\lambda)\right)$ con

$$K_R(\lambda) \equiv J(\lambda) - \frac{1}{2}L(\lambda,\lambda) + \frac{1}{2i\pi}R(\lambda) \quad (\text{mód } \mathbb{Z}).$$

Desde (2.6) se deduce que para toda forma lineal R, K_R verifica (2.10) (ejercicio).

Basta ahora elegir R tal que $K_R = K_0 + \frac{1}{2i\pi}R$ sea a valores reales. Desde (2.6), podemos suponer que $\Im(K_0)$ es $\mathbb{Z}$-lineal y extenderlo $\mathbb{R}$-linealmente a V. Entonces $R(z) = 2\pi(\Im(K_0(z)) - i\Im(K_0(iz)))$ define una forma lineal tal que $K_R(\lambda) \in \mathbb{R}$ para todo $\lambda \in \Lambda$.

Para terminar, (2.11) se deduce del hecho que la función $|\widetilde{\theta}(z)|\exp(-\frac{\pi}{2}H(z,z))$ es Λ-periódica y continua, entonces cotada. □

Corolario 2.8. *Si θ es entera, entonces H_θ es positiva (es decir $H_\theta(z,z) \geqslant 0$ para todo $z \in V$). Además, para todo $z_0 \in V$, la función holomorfa $z \mapsto \theta(z_0 + z)$ es constante sobre el núcleo $N = \{z \in V; H_\theta(z,w) = 0, \forall w \in V\}$ de H_θ.*

Demostración. Consideramos θ holomorfa y $\widetilde{\theta}$ la función theta normalizada asociada. Supongamos que existe z_0 tal que $H_\theta(z_0,z_0) < 0$. Entonces (2.11) implica que la función holomorfa $t \in \mathbb{C} \mapsto (\widetilde{\theta}(tz_0))$ tiende hacia 0 cuando $|t|$ tiende hacia el infinito. Entonces por el teorema de Liouville, para todo $t \in \mathbb{C}$, $\theta(tz_0) = 0$. Como por continuidad $H(z,z) < 0$ en un vecino U de z_0, el argumento precedente aplicado a todo $z \in U$ implicaría que θ es idénticamente cero. Deducimos que H es positiva por contradicción.

Si $z \in N$ entonces

$$|\widetilde{\theta}(z_0+z)| \leqslant c\exp\left(\frac{\pi}{2}H(z_0+z,z_0+z)\right) = c\exp\left(\frac{\pi}{2}H(z_0,z_0)\right).$$

Aplicando de nuevo el teorema de Liouville a la función holomorfa $z \mapsto \widetilde{\theta}(z_0+z) - \widetilde{\theta}(z_0)$ nos da el segundo resultado. □

En particular, obtenemos la recíproca de Proposición 2.6:

Corolario 2.9. *La forma de Riemann H_θ es cero si y sólo si θ es trivial.*

2.2. Divisores. Recordamos:

Definición 2.10 (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 $\mathrm{Div}(X)$. Ver [3, 14].

Consideramos ahora $X = T = V/\Lambda$ un toro complejo, 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[8] por λ.

Observamos que si θ es una función theta relativamente a Λ, el divisor $(\theta) \in \mathrm{Div}(V)$ es Λ-periódico, entonces hay un divisor $D_\theta \in \mathrm{Div}(T)$ tal que $\pi^*(D_\theta) = (\theta)$. Si $(U_i)_{i\in I}$ es un recubrimiento de V constituido de abiertos Λ-pequeños[9], entonces D_θ puede ser descrito[10] por la familia $(\pi(U_i), \theta \circ (\pi|_{U_i})^{-1}))_{i\in I}$.

Teorema 2.11 (Poincaré)**.** *Para todo $D \in \mathrm{Div}(T)$, existe θ una función theta relativamente a Λ tal que $D_\theta = D$. Además, si D es efectivo, la función θ es holomorfa.*

Demostración. Ver [3, p. 43] o [17, Teorema 18, p. 35]. □

Dejamos como ejercicio la proposición siguiente:

Proposición 2.12. *El divisor D_θ es trivial si y sólo si θ es una función theta trivial. Entonces, la aplicación $\theta \mapsto D_\theta$ define un isomorfismo de grupos*

$$\{\textit{funciones theta}\}/\{\textit{funciones triviales}\} \cong \mathrm{Div}(T).$$

De Corolarios 2.8 y 2.9 y de Teorema 2.11, tenemos el siguiente resultado.

Corolario 2.13. *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 y es un morfismo de grupos de $\mathrm{Div}(T)$ en el grupo $\mathcal{R}(T)$ de las formas de Riemann sobre T. Si D es efectivo, θ es entera entonces H_D es positiva.*

[8]Si D' es dado por (U_α, f_α) entonces $t_\lambda^* D'$ es dado por $(U_\alpha + \lambda, f_\alpha(z - \lambda))$.

[9]Un abierto U es Λ-*pequeño* si no encuentra ningún de sus traslados por Λ.

[10]Esta familia es admisible porque desde la ecuación de θ, para todo λ, $\theta(z + \lambda)/\theta(z)$ no tiene cero ni polo sobre U_i para todo i.

2.3. Esbozo de prueba del criterio en Teorema 1.8. Si $\theta_0, \dots, \theta_n$ son funciones theta holomorfas sobre $V = \mathbb{C}^g$ relativamente a Λ, de mismo tipo y sin cero común, pues que satisfacen a la misma ecuación (2.1), la aplicación $(\theta_0, \dots, \theta_n) : V \to \mathbb{C}^{n+1}\backslash\{0\}$ induce una aplicación holomorfa de V/Λ en $\mathbb{P}^n(\mathbb{C})$ que denotaremos $(\theta_0 : \cdots : \theta_n)$.

Lema 2.14. *Si $u : T = V/\Lambda \longrightarrow \mathbb{P}^n(\mathbb{C})$ es una aplicación holomorfa, entonces existen $\theta_0, \dots, \theta_n$ funciones theta enteras normalizadas de mismo tipo tales que $u = (\theta_0 : \cdots : \theta_n)$.*

Demostración. Denotamos por $(x_0 : \cdots : x_n)$ las coordenadas en $\mathbb{P}^n(\mathbb{C})$. Salvo de una permutación de índices, podemos suponer que $u(T)$ no es contenida en el hiperplano $\mathcal{H}_0 = (x_0 = 0)$. Entonces el pullback por u de H_0 define un divisor efectivo[11] D sobre T.

Denotamos θ_0 la función theta normalizada asociada a D por Proposición 2.11. Como D es efectivo, θ_0 es una función entera. Denotamos $\tilde{u} : V \to \mathbb{C}^{n+1}\backslash\{0\}$ induciendo u y consideramos las funciones theta $\theta_j := \left(\frac{x_j \circ \tilde{u}}{x_0 \circ \tilde{u}}\right)\theta_0$ para $j = 1, \dots, n$. Pues como $\frac{x_j \circ \tilde{u}}{x_0 \circ \tilde{u}}$ es Λ-periódica, esas funciones theta son de mismo tipo que θ_0 (en particular son normalizadas de forma de Riemann H_{θ_0}). Además, son enteras, no tienen cero común y $u(z) = (\theta_0(z) : \cdots : \theta_n(z))$. □

2.3.1. Condición necesaria de Teorema 1.8. Supongamos que un toro complejo T es una variedad abeliana, i.e. que existe una inmersión holomorfa $u : T \to \mathbb{P}^n(\mathbb{C})$. Sean $\theta_0, \dots, \theta_n$ tales que $u = (\theta_0 : \cdots : \theta_n)$ como en Lema 2.14. La forma de Riemann H asociada a estas funciones theta enteras equivalentes es positiva (Corolario 2.8). 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 al 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.

2.3.2. Teorema de Riemann-Roch. Para terminar la prueba de Teorema 1.8, queremos construir una inmersión holomorfa de un toro T dotado de una forma de Riemann no degenerada en un espacio proyectivo. Por Lema 2.14, sabemos que tales inmersiones son dadas por funciones theta enteras de mismo tipo. En esta subsección, examinamos al espacio vectorial $Th(L, J)$ de las funciones theta *holomorfas* de tipo dado (L, J).

Decimos que (L, J) es un *tipo* si $L : V \times \Lambda \to \mathbb{C}$ es $\mathbb{C}$-lineal a izquierda, $J : \Lambda \to \mathbb{C}$ y verifican las propiedades (2.5),(2.6) y (2.7). A un tipo (L, J), extendiendo L a $V \times V$ por $\mathbb{R}$-linealidad a derecha, podemos asociar una forma $\mathbb{R}$-bilineal alternada E por (2.8). La forma H definida por $H(z, w) = E(iz, w) + iE(z, w)$ es una forma de Riemann (ver Subsección 2.1.2).

Observación 2.15. Recíprocamente si H es una forma de Riemann y $E = \Im(H)$, considerando $L(z, \lambda) = \frac{1}{2i}H(z, \lambda)$ y $J(\lambda) = \frac{1}{4i}H(\lambda, \lambda) + \frac{1}{4}E(\lambda, \lambda)$, entonces (L, J) es un tipo de forma de Riemann asociada H (ejercicio).

Recordamos que para una forma $\mathbb{R}$-bilineal alternada E a valores enteras sobre un $\mathbb{Z}$-módulo libre Λ de rango $2g$ que es no degenerada, existe una base $(\omega_1, \dots, \omega_{2g})$

[11] El hiperplano $\mathcal{H}_0$ puede ser descrito por la familia $(U_i, x_0/x_i)_{0 \leqslant i \leqslant n}$ donde $U_i = \mathbb{P}^n(\mathbb{C})\backslash(x_i = 0)$ y $D = u^*\mathcal{H}_0$.

dicha *base simpléctica* (o *base de Frobenius*) de Λ en la cual la matriz de E es de la forma

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

donde $\Delta = Diag(d_1, \ldots, d_g)$ con $d_1, \ldots, d_g$ enteros > 0 tales que $d_1 \mid \cdots \mid d_g$. Deducimos que $\det(E) > 0$. El *pfaffiano de* E es el entero: $\mathrm{Pf}(E) = \sqrt{\det(E)} = d_1 \ldots d_g$.

Teorema 2.16 (Teorema de Riemann-Roch para las variedades abelianas)**.** *Sea (L, J) un tipo. Supongamos que la forma de Riemann asociada H es no degenerada, y denotamos $E = \Im(H)$. Entonces, el espacio vectorial de las funciones theta holomorfas de tipo (L, J) tiene dimensión*

$$\dim_{\mathbb{C}}(Th(L, J)) = \mathrm{Pf}(E) > 0.$$

Demostración. Ver [17, Teorema 24, p. 45], [7, Teorema A.5.3.3, p. 104], [8, Teoremas 2.2 y 2.3, pp. 11–12]. □

Observación 2.17. Sea D un divisor efectivo sobre T y θ una función theta entera tal que $(\theta) = \pi^*(D)$. Denotamos (L, J) el tipo de θ. La aplicación $\vartheta \mapsto \vartheta/\theta$ define un isomorfismo entre $Th(L, J)$ y el espacio vectorial $\mathcal{L}(D) = \{f \in \mathcal{M}(T); D + (f) \geqslant 0\} \cup \{0\}$. Esto explica el nombre de Teorema 2.16.

2.3.3. Final de la prueba de Teorema 1.8. Supongamos que el toro T es dotado de una forma de Riemann no degenerada H.

De Observación 2.15, hay un tipo (L, J) de forma de Riemann H y por Teorema 2.16, $\dim_{\mathbb{C}}(Th(L, J)) > 0$. Denotamos $(\theta_0, \ldots, \theta_n)$ una base de $Th(L, J)$ y $D = D_{\theta_0} (= D_{\theta_i}$ para todo $i)$. Obtenemos una aplicación holomorfa $\Phi_D = (\theta_0 : \cdots : \theta_n) : T \to \mathbb{P}^n(\mathbb{C})$.

Definición 2.18. 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.

El fin de la prueba se deduce del siguiente resultado:

Teorema 2.19 (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 $\Phi_{3D} : T \to \mathbb{P}^n(\mathbb{C})$.*

Demostración. Ver [7, Teorema A.5.3.6, p. 105]. □

Observamos que, con Sección 2.3.1, el Teorema de Lefschetz demuestra:

Corolario 2.20. *Un divisor D sobre T es amplio si y sólo si H_D es una forma de Riemann no degenerada.*

3. Teorema de Appell-Humbert y variedad abeliana dual

3.1. Teorema de Appell-Humbert. Sea $A = V/\Lambda$ una variedad abeliana.

Recordamos que $\mathcal{R}(A)$ es el grupo de las formas de Riemann sobre A. Para $H \in \mathcal{R}(A)$ decimos que una función $\psi : V \to U(1)$ es un semi-carácter asociado a H si verifica (2.12) y denotamos

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

El conjunto $\mathcal{P}(A)$ es un grupo por la ley $(H_1, \psi_1).(H_2, \psi_2) = (H_1 + H_2, \psi_1\psi_2)$. Por Lema 2.7 y Teorema 2.11, a un divisor $D \in \mathrm{Div}(A)$ podemos asociarle una

función theta y entonces una función theta normalizada y un par $(H, \psi) \in \mathcal{P}(A)$. Consideramos la aplicación $\Psi : \mathrm{Div}(A) \to \mathcal{P}(A); D \mapsto (H_D, \psi_D)$ así definida.

Denotamos por $\mathrm{Pic}(A)$ el cociente de $\mathrm{Div}(A)$ por el subgrupo $\mathrm{Princ}(A)$ de los divisores principales, y $\mathrm{Pic}^0(A)$ el cociente por $\mathrm{Princ}(A)$ del subgrupo de los divisores D tales que $H_D = 0$. El *grupo de Néron-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 3.1 (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* $\mathrm{Pic}^0(A)$ *se identifica a* $\mathrm{Hom}(A, U(1))$ *y que induce* $NS(A) \cong \mathcal{R}(A)$*.*

Demostración. Dejamos al lector la verificación que Ψ es un morfismo de grupos. Sea $D \in \mathrm{Div}(A)$ tal que (H_D, ψ_D) sea trivial. Entonces la función normalizada $\widetilde{\theta}$ asociada a D es Λ-periódica, lo que implica que D es principal. Y también vale la recíproca. Entonces Ψ induce un morfismo inyectivo $\mathrm{Pic}(A) \to \mathcal{P}(A)$ que denotaremos todavía Ψ.

Demostramos que Ψ es sobreyectivo. Sea $(H, \psi) \in \mathcal{P}(A)$. Podemos escribir H como diferencia de dos formas de Riemann definidas positivas: $H = H_1 - H_2$ y para cada H_i, por Teorema 2.16, existe una función theta holomorfa normalizada θ_i de forma de Riemann H_i. La función theta meromorfa $\theta = \theta_1/\theta_2$ es normalizada y tiene forma de Riemann H. Denotamos por α su semi-carácter. Entonces $\psi/\alpha \in \mathrm{Hom}(\Lambda, U(1))$. Consideramos la función ϑ definida por $\vartheta(z) = \frac{\psi(z)}{\alpha(z)}\theta(z)$, extendiendo ψ/α en una función sobre V por $\mathbb{R}$-linealidad. La función ϑ es una función theta normalizada de forma de Riemann H y semi-carácter ψ. Así, $\Psi(D_\vartheta) = (H, \psi)$.

Deducimos que $\Psi : \mathrm{Pic}(A) \to \mathcal{P}(A)$ es un isomorfismo de grupos. Además, $H_D = 0$ si y sólo los semi-caracteres asociados a H_D son los elementos de $\mathrm{Hom}(\Lambda, U(1))$. Entonces $\Psi(\mathrm{Pic}^0(A))$ se identifica a $\mathrm{Hom}(\Lambda, U(1))$. Deducimos el resultado. □

3.2. Variedad abeliana dual. Denotamos por $\bar{V}^*$ el conjunto de las formas $\mathbb{C}$-antilineales 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 $\ell \mapsto \Im(\ell)$ 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 $\langle \ell, v \rangle := \Im(\ell(v))$, 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 3.2. 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 3.3. 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 3.4.

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

2. *la aplicación φ_D depende sólo de la clase de D en $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$;*
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 theta asociada a D, entonces $\pi^*(t_a^* D) = (\theta_a)$ donde $\theta_a(z) = \theta(z + a)$. Entonces $\pi^*(t_a^* D - D) = (\theta_a/\theta)$, es decir $t_a^* D - D = D_{\theta_a/\theta}$. Un cálculo muestra que la ecuación de la función theta normalizada equivalente a θ_a/θ tiene multiplicador $e(\frac{1}{2i}H(a,\lambda)) = e(E(a,\lambda))$, donde $H = H_D$ y $E = \mathrm{Im}(H)$. Esto demuestra que la función de Riemann asociada a θ_a/θ entonces a $t_a^* D - D$ es cero.

2. Si D es tal que $H_D = 0$, entonces la función theta normalizada asociada a θ_a/θ tiene multiplicador cero. Así, es Λ-periódica y deducimos que $t_a^* D - D$ es principal.
3. Observamos que con Teorema 3.1 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 theta 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 (ver Subsección 2.3.2), se puede demostrar que es un grupo finito de orden $\mathrm{Pf}(E)^2$.

□

Corolario 3.5. *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 3.3, Teorema 3.1 y la prueba de Proposición 3.4, 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 3.4,3., el núcleo de φ_H es finito, entonces $\varphi_H^{-1}(\widehat{\Lambda})/\Lambda$ es finito. Deducimos que un múltiplo de H^* es una forma de Riemann y es no degenerada porque H lo es. □

Proposición 3.6. *1. Tenemos $\widehat{\widehat{A}} = A$.*

2. *Un morfismo de toros* $f : A_1 \to A_2$ *induce un morfismo* dual $\hat{f} : \hat{A}_2 \to \hat{A}_1$ *y* $\hat{\hat{f}} = f$.
3. *El functor* $\hat{\ }$ *de la categoría de los toros es exacto.*

Demostración. Dejamos la prueba en ejercicio (o ver [1, §2.4]). □

3.3. Polarización.

Definición 3.7. Sea A una variedad abeliana. Una *polarización* sobre A es el dato de la clase de un divisor amplio en $NS(A)$, o de manera equivalente, es el dato 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, H) es *principalmente polarizada.*

Por Proposición 3.4, una polarización $[D]$ define una isogenía $\varphi_D : A \to \hat{A}$ de grado $\mathrm{Pf}(\Im(H_D))$. En particular, si la polarización es principal, la correspondiente isogenía es un isomorfismo.

Recíprocamente, una isogenía $\varphi : A \to \hat{A}$ es un φ_D con D un divisor amplio si y sólo si φ es inducida por una aplicación analítica $\Phi : V \to \bar{V}^*$ tal que la forma $H_\Phi : V \times V \to \mathbb{C}$ definida por $H(z, w) = \Phi(z)(w)$ es una forma hermitiana definida positiva.

Un morfismo (resp. una isogenía) $f : (A, H) \to (A, H')$ de variedades abelianas polarizadas es un morfismo (resp. una isogenía) $f : A \to A'$ tal que $[f^* D'] = [D]$ (donde $H' = H_{D'}$ y $H = H_D$), es decir si $f : A = V/\Lambda \to A' = V'/\Lambda'$ proviene de una aplicación $F : V \to V'$ tal que $H'(F(z), F(w)) = H(z, w)$ para todos z, w en V.

Ejemplo 3.8 (Dimensión 1)**.** Toda curva elíptica es principalmente polarizada. En efecto, si $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ con $\Im(\omega_1/\omega_2) > 0$, la forma real alternada $E = \Im(H)$ asociada a la forma de Riemann $H(z, w) = \frac{z\bar{w}}{\Im(\omega_1 \bar{\omega}_2)}$ tiene matriz $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ en la base (ω_1, ω_2) de Λ.

Ejemplo 3.9. Con las notaciones de Ejemplo 1.10, A_τ es principalmente polarizada.

En dimensión > 1, un importante ejemplo de variedad principalmente polarizada es dado por las jacobianas de curvas (ver Parte 2), pero no toda variedad abeliana es principalmente polarizada, aún si tenemos el resultado siguiente:

Proposición 3.10. *Toda variedad abeliana polarizada es isógena a una variedad abeliana principalmente polarizada.*

Demostración. Sea (A, H) una variedad abeliana polarizada, $A = V/\Lambda$. Consideramos una base simpléctica $(\omega_1, \ldots, \omega_{2g}$ de Λ con respecto a la forma alternada no degenerada $E = \Im(H)$. Con las notaciones de Subsección 2.3.2, consideramos el nuevo retículo de V dado por $\Lambda' = \mathbb{Z}\frac{1}{d_1}\omega_1 + \mathbb{Z}\frac{1}{d_g}\omega_g + \mathbb{Z}\omega_{g+1} + \ldots \mathbb{Z}\omega_{2g}$. Entonces, E toma todavía valores enteros sobre $\Lambda' \times \Lambda'$ y tiene matriz de determinante 1 en la base precedente de Λ'. Entonces el toro V/Λ' es una variedad abeliana principalmente polarizada e isógena a A. □

4. Endomorfismos de las variedades abelianas

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

Definición 4.1 (Involución de Rosati)**.** Para $u \in \mathrm{End}(A)$ consideramos

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

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

Así, si (A, H) es una variedad polarizada simple, $B := \mathrm{End}_0(A)$ 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 B y K_0 el subcuerpo de los elementos fijos por $\dagger_K$. Como $B \otimes_K \bar{K}$ es un álgebra de matrices, la dimensión de B sobre K es un cuadrado. Ademas, pues $\dagger$ es una anti-involución, $[K : K_0] \leqslant 2$. Denotamos

$$[B : K] = d^2, \quad [K : \mathbb{Q}] = e \leqslant 2[K_0 : \mathbb{Q}].$$

Teorema 4.3 (Clasificación de Albert)**.** *El cuerpo* K_0 *es un cuerpo de números algebraico totalmente real y el par* $(B, \dagger)$ *es de uno de los tipos siguientes:*

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

Tipo II: $K = K_0$ *y* B *es un álgebra de cuaterniones indefinida*[12] *sobre* K *(*$d = 2$*). La involución*$\dagger$ *es de la forma* $x^\dagger = ax^*a^{-1}$ *donde* $.^*$ *es la involución usual de* B *y* $a \in B$ *un elemento tal que* $a^2 \in K$ *con* a^2 *totalmente negativo.*

Tipo III: $K = K_0$ *y* B *es un álgebra de cuaterniones definida*[13] *sobre* K *(*$d = 2$*). En este caso* $x^\dagger = x^*$ *es la involución usual sobre* B.

Tipo IV: $[K : K_0] = 2$ *y* K *es un cuerpo CM*[14]*. En el caso donde* $K = B$*,* A *es una variedad abeliana CM por* K.

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

Observación 4.4. 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 más detalles el lector podrá consultar [12, p. 186] o [1, §5.5 y cap. 9].

5. Espacios de móduli

5.1. Matriz de periodos y condiciones de Riemann. Consideramos V un $\mathbb{C}$-espacio vectorial de dimensión g y Λ un retículo en V. Sea $\underline{e} = (e_1, \ldots, e_g)$ una $\mathbb{C}$-base de V y $(\omega_1, \ldots, \omega_{2g})$ una $\mathbb{Z}$-base de Λ. La matriz Π de los elementos ω_i en la base $\underline{e}$ es llamada *matriz de periodos.* Una vez fijadas la base $\underline{e}$ y $\underline{\omega}$, identificamos V a $\mathbb{C}^g$ y Λ a $\Pi\mathbb{Z}^{2g}$ y entonces $V/\Lambda \cong \mathbb{C}^{2g}/\Pi\mathbb{Z}^{2g}$.

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

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

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

Teorema 5.1. *El toro $T = V/\Lambda$ es una variedad abeliana si y sólo si existe una matriz $J \in M_2(\mathbb{Z})$ no degenerada alternada verificando las* condiciones de Riemann*:*

$$\Pi J^{-1}\,{}^t\Pi = 0 \tag{5.1}$$

$$i\Pi J^{-1}\,{}^t\overline{\Pi} > 0 \tag{5.2}$$

Presentamos la prueba del teorema precedente como un ejercicio (Ejercicio 6.6). Para una prueba completa (y entonces una solución al ejercicio), el lector puede referirse a [1, §4.2]. En Ejercicio 6.6, aparece que si V/Λ es una variedad abeliana, entonces la matriz J es la matriz en la base $\underline{\omega}$ de una forma alternada no degenerada con respecto a Λ (es decir $J = (E(\omega_i, \omega_j))_{1 \leqslant i,j \leqslant 2g}$).

Por ejemplo si $A = V/\Lambda$ es principalmente polarizada y si elegimos para $\underline{\omega}$ una base simpléctica relativamente a la polarización, entonces $J = \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$ y, con $\Pi = (\Pi_1\,\Pi_2)$ donde Π_1, Π_2 están en $M_g(\mathbb{C})$, las condiciones de Riemann se convierten en:

$$\Pi_2\,{}^t\Pi_1 = \Pi_1\,{}^t\Pi_2 \tag{5.3}$$

$$i\Pi_2\,{}^t\overline{\Pi_1} - i\Pi_1\,{}^t\overline{\Pi_2} > 0. \tag{5.4}$$

Se puede demostrar que Π_2 es invertible y un cambio de base manda la matriz de periodos $(\Pi_1\,\Pi_2)$ sobre $(\tau\ I_g)$ donde $\tau = \Pi_2^{-1}\Pi_1$ (ver Ejercicio 6.9, 1)). Las relaciones de Riemann dicen entonces que τ es simétrica de parte imaginaria $\Im(\tau)$ definida positiva. Este observación es el punto de inicio de la construcción del espacio de móduli para las variedades abelianas complejas como sigue en Subsección 5.2 y en Ejercicio 6.9.

5.2. Espacios de móduli. En esta subsección, nos interesamos en clasificar las variedades abelianas principalmente polarizadas salvo isomorfismo.

Ejemplo 5.2 (Dimensión 1)**.** Consideramos el *semi-plano de Poincaré* $\mathcal{H} = \{z \in \mathbb{C}; \Im(z) > 0\}$. El grupo $\mathrm{SL}_2(\mathbb{R})$ actúa sobre $\mathcal{H}$ por homografías: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).z = \frac{az+b}{cz+d}$. El cociente $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ tiene estructura de superficie de Riemann. La aplicación $\tau \mapsto \mathbb{C}/\Lambda_\tau$ define una correspondencia biyectiva entre los puntos de $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ y las clases de isomorfismo de curvas elípticas sobre $\mathbb{C}$ (ver [15, ap. C, §13]).

Vamos a enunciar un teorema análogo en dimensión $g \geqslant 1$. Denotamos por $\mathcal{A}_g(\mathbb{C})$ al conjunto de las clases de isomorfismos de variedades abelianas complejas principalmente polarizadas. Observamos que $\mathcal{A}_1(\mathbb{C})$ es simplemente el conjunto de las clases de isomorfismo de curvas elípticas complejas, pues son todas principalmente polarizadas. Denotamos por $\mathcal{H}_g$ el *semi-espacio de Siegel*, es decir el conjunto de las matrices $\tau \in M_g(\mathbb{C})$ simétricas tales que $\Im(\tau)$ sea definida positiva (lo que denotamos $\Im(\tau) > 0$ por brevedad).

Denotamos por $\mathrm{Sp}_{2g}(K) = \{M \in \mathrm{GL}_{2g}(K); MJ^tM = J\}$ donde

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Sea $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{R})$. Entonces

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\tau := (a\tau + b)(c\tau + d)^{-1} \tag{5.5}$$

define una acción (a la izquierda) de $\mathrm{Sp}_{2g}(\mathbb{R})$ sobre $\mathcal{H}_g$ (ver Ejercicio 6.8).

Teorema 5.3. *El cociente* $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g$ *tiene una estructura de variedad analítica compleja. La aplicación* $\tau \mapsto A_\tau = \mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$ *define una biyección de* $\mathcal{H}_g$ *hasta* $\mathcal{A}_g(\mathbb{C})$.

Ejercicio 6.9 demuestra la biyección. Ver [1, cap. 8] o [3, §VII.1] para la prueba completa, en un contexto aún más general.

6. Ejercicios

Ejercicio 6.1. Sea Λ un retículo de $\mathbb{C}$. Consideramos la función sigma de Weierstrass definida por

$$\sigma(z) := z \prod_{\lambda\in\Lambda\setminus\{0\}} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right). \tag{6.1}$$

1. Demostrar que $\left(\frac{\sigma'}{\sigma}\right)' = -\wp_\Lambda$ donde la función $\wp$ de Weierstrass es definida en Ejemplo 1.5.
2. Verificar que $\wp_\Lambda$ es Λ-periódica.
3. Deducir que σ es una función theta relativa a Λ.

Ejercicio 6.2. Sea $\tau \in M_g(\mathbb{C})$ simétrica tal que $\Im(\tau)$ sea definida positiva. Consideramos la función definida por

$$\theta(z) = \sum_{m\in\mathbb{Z}^g} \exp(i\pi {}^t m\tau m + 2i\pi {}^t mz) \tag{6.2}$$

1. Demostrar que para todo m, ℓ, k en $\mathbb{Z}^g$ y $z \in \mathbb{C}^g$, tenemos

$${}^t m\tau m + 2\,{}^t m(z + \ell + \tau k) = {}^t(m + k)\tau(m + k) + 2\,{}^t(m + k)z + 2\,{}^t m\ell - 2\,{}^t kz - {}^t k\tau k.$$

2. Deducir que para todo $z \in \mathbb{C}^g$ y todo ℓ, k en $\mathbb{Z}^g$,

$$\theta(z + \ell + \tau k) = \theta(z)\exp(-2i\pi\,{}^t kz - i\pi\,{}^t k\tau k)$$

y que θ es una función theta relativa a $\Lambda_\tau = \mathbb{Z}^g + \tau\mathbb{Z}^g$.

Ejercicio 6.3. Demostrar que toda función theta que no se anula es una función theta trivial.

Ejercicio 6.4. Consideramos el toro $A_\tau = \mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$ donde $\tau \in M_g(\mathbb{C})$ es una matriz simétrica tal que $\Im(\tau)$ es definida positiva (es decir un elemento de $\mathfrak{h}_g$). Demostrar que

$$H(z, w) = {}^t z\Im(\tau)^{-1}\bar{w} \qquad ((z, w) \in \mathbb{C}^g \times \mathbb{C}^g)$$

define una forma de Riemann no degenerada que induce una polarización principal sobre A_τ. [Indicación: verificar que $E(m+\tau n, h+\tau\ell) = {}^t nh - {}^t m\ell$ donde $E = \Im(H)$.]

Ejercicio 6.5. Demostrar que una matriz $\Pi \in M_{g,2g}(\mathbb{C})$ es una matriz de periodos de un toro complejo si y sólo si la matriz por bloques $\left(\begin{array}{c}\Pi\\ \hline \overline{\Pi}\end{array}\right)$ es invertible. *(Para una solución, ver* [1, Proposition 1.1.2, p. 9]*).*

Ejercicio 6.6 (Condiciones de Riemann). Adoptamos las notaciones de Subsección 5.1: sea Π una matriz de periodos de un toro complejo $T = V/\Lambda$ con respecto a una base $\underline{e}$ de V y una base $\underline{\omega}$ de Λ.

1. Consideramos una forma alternada no degenerada $E : \Lambda \times \Lambda \to \mathbb{Z}$, la extendemos a $\mathbb{C}^g = \Lambda \otimes \mathbb{R}$ y consideramos $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ definida por $H(z,w) = E(iz,w) + iE(z,w)$. Denotamos por J la matriz de E con respecto a la base $(\omega_1, \ldots, \omega_{2g})$ de Λ es decir $J = (E(\omega_i, \omega_j))_{1 \leqslant i,j \leqslant 2g}$.
   a) Verificar que de la definición de J, tenemos que para todos x, y en $\mathbb{R}^{2g}$,
   $$E(\Pi x, \Pi y) = {}^t x J y.$$
   b) Consideramos la matriz por bloques
   $$L := \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix}^{-1} \begin{pmatrix} iI_g & 0_g \\ 0_g & -iI_g \end{pmatrix} \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix}.$$
   Verificar que $\Pi L = i\Pi$.
   c) Deducir que $E(iz, iw) = E(z,w)$ para todos z, w en $\mathbb{C}^g$ si y sólo si ${}^t L J L = J$. (Indicación: como $\Lambda \otimes \mathbb{R} = V = \mathbb{C}^g$, se puede escribir $z = \Pi x$ y $w = \Pi y$ con x, y en $\mathbb{R}^{2g}$).
   d) Concluir que H es una forma hermitiana si y sólo si $\Pi J^{-1}\, {}^t\Pi = 0$.
   e) Demostrar que si H es una forma hermitiana, entonces tiene matriz $2i(\overline{\Pi} J^{-1}\, {}^t\Pi)^{-1}$. Deducir que H es una forma hermitiana definida positiva si y sólo si $i\Pi J^{-1}\, {}^t\overline{\Pi} > 0$.
2. Usar las preguntas precedentes para demostrar Teorema 5.1.

Ejercicio 6.7. Sean $A = V/\Lambda$ y $B = V'/\Lambda'$ dos variedades abelianas de dimensión respectiva g y g'. Sea $\Pi \in M_{g,2g}(\mathbb{C})$ (resp. $\Pi' \in M_{g',2g'}(\mathbb{C})$) una matriz de periodos de A (resp. B) con respecto a la elección de bases de V y Λ (resp. V', Λ'). Hacemos las identificaciones $A = \mathbb{C}^g/\Pi\mathbb{Z}^{2g}$ y $B = \mathbb{C}^{g'}/\Pi'\mathbb{Z}^{2g'}$. Supongamos que $f : A \to B$ es un morfismo de variedades abelianas. Denotamos por $F : \mathbb{C}^g \to \mathbb{C}^g$ el único isomorfismo tal que $F(\Lambda) \subset \Lambda'$ y F induce f. Denotamos por $M \in M_{g,g'}(\mathbb{C})$ la matriz de F y $R = M_{2g,2g'}(\mathbb{Z})$ la matriz de $F|_{\Lambda_\tau}$ con respecto a las bases precedentes. Demostrar que $M\Pi = \Pi' R$.

Ejercicio 6.8. Sea $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{R})$.

1. Demostrar que
   $$\overline{{}^t(c\tau + d)}(a\tau + b) - \overline{{}^t(a\tau + b)}(c\tau + d) = \tau - \overline{\tau} = 2i\Im(\tau).$$
2. Con lo que precede, demostrar que si v es tal que $(c\tau + d)v = 0$ entonces ${}^t\overline{v}\Im(\tau)v = 0$.
3. Deducir que $(c\tau + d)$ es invertible.
4. Denotamos $\tau' := (a\tau + b)(c\tau + d)^{-1}$. Demostrar que
   $$\overline{{}^t(c\tau + d)}(\tau' - {}^t\tau')(c\tau + d) = 0 \tag{6.3}$$
   $$\overline{{}^t(c\tau + d)}(\tau' - {}^t\overline{\tau'})(c\tau + d) = 2i\Im(\tau). \tag{6.4}$$
5. Deducir que (5.5) define una acción de $\mathrm{Sp}_{2g}(\mathbb{R})$ sobre $\mathcal{H}_g$.

Ejercicio 6.9.

1. Sea $A = V/\Lambda$ una variedad principalmente polarizada y $\underline{\omega}$ una base simpléctica relativamente a la polarización. Denotamos por $\Pi = (\Pi_1 \Pi_2)$ con $\Pi_k \in M_g(\mathbb{C})$ $(k = 1, 2)$, la matriz de periodos de $\underline{\omega}$ en una base $\underline{e}$ de V e identificamos A con $\mathbb{C}^g/\Pi\mathbb{Z}^{2g}$ como en subsección 5.1. Recordamos que Π_1, Π_2 verifican las condiciones de Riemann (5.3) y (5.4).

a) Demostrar que $(\omega_1, \ldots, \omega_g)$ es una $\mathbb{C}$-base del $\mathbb{C}$-espacio vectorial V. (Indicación: considerar W el $\mathbb{R}$ espacio vectorial generado por $\omega_1, \ldots, \omega_g$ y demostrar que $W \oplus iW = V$.) Deducir que Π_1 y Π_2 son invertibles.
b) Demostrar que $\tau := \Pi_2^{-1}\Pi_1 \in \mathcal{H}_g$.
c) Demostrar que la multiplicación por la matriz $\Pi_2^{-1} \in \mathrm{GL}_g(\mathbb{C})$ induce un isomorfismo de variedades abelianas polarizadas desde $\mathbb{C}^g/\Pi\mathbb{Z}^{2g} \cong A$ hasta $A_\tau = \mathbb{C}^g/\Lambda_\tau = \mathbb{C}^g/(\tau\, I_g)\mathbb{Z}^{2g}$.

2. Sea $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$, $\tau \in \mathcal{H}_g$ y $\tau' = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\tau = (a\tau + b)(c\tau + d)^{-1} \in \mathcal{H}_g$. Demostrar que

$$(\tau'\, I_g) = {}^t(c\tau + d)^{-1}(\tau\, I_g)\, {}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Deducir que la multiplicación por ${}^t(c\tau + d)^{-1}$ induce un isomorfismo de variedades abelianas (principalmente) polarizadas desde $A_\tau = \mathbb{C}^g/\Lambda_\tau$ hasta $A_{\tau'} = \mathbb{C}^g/\Lambda_{\tau'}$.

3. Sean τ, τ' en $\mathcal{H}_g$ tales que A_τ y $A_{\tau'}$ son isomorfas como variedades abelianas polarizadas. Denotamos por $F : \mathbb{C}^g \to \mathbb{C}^g$ el único isomorfismo tal que $F(\Lambda_{\tau'}) \subset \Lambda_\tau$ y F induce $f : A_{\tau'} \xrightarrow{\cong} A_\tau$. Denotamos por $M \in \mathrm{GL}_g(\mathbb{C})$ la matriz de F en la base canónica de $\mathbb{C}^g$ y $R \in M_{2g}(\mathbb{Z})$ la matriz de $F|_{\Lambda_\tau}$ en las bases simplécticas dadas por las matrices de periodos $(\tau\, I_g)$ y $(\tau'\, I_g)$ respectivamente. Recordamos que $M(\tau\, I_g) = (\tau'\, I_g)R$.

Demostrar que ${}^tR$ está en $\mathrm{Sp}_{2g}(\mathbb{Z})$ y que $\tau' = {}^tR.\tau$.

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 parte 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 (de línea) tal como están presentados por ejemplo en los dos primeros capítulos de* [5] *o la parte A de* [7]. *En la segunda sección de esta parte damos una breve descripción sobre las nociones de divisores y fibrados.*

7. Grupos algebraicos

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

Definición 7.1. 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 7.2. 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 $J = J_g = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ la matriz antisimétrica de tamaño $2g \times 2g$ y definimos

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

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 7.3. 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, 15, 16]) 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, 13]) 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 contraer[15] 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 7.4 (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, Lema A.7.1.1, p. 119] o [12, 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 1.3.

Teorema 7.5. *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. □

[15]Para verificar este punto, invocamos el criterio de Castelnuovo ([5, Teorema 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.

Teorema 7.6 (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, Corolario A.7.1.4, p. 120]. □

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.

8. Divisores de Weil y Cartier, fibrados de línea

En esta sección describimos sucintamente y sin demostraciones las varias nociones de divisores y fibrados (de línea) en geometría algebraica.

8.0.1. Divisores de Weil. Sea X una variedad algebraica, un *divisor de Weil* D es una combinación lineal de hipersuperficies con coeficientes enteros. En otros términos se puede escribir:

$$D = \sum_Z n_Z Z,$$

donde Z recorre las subvariedades de codimensión 1 de X y $n_Z \in \mathbb{Z}$, con la condición que los coeficientes n_Z sean casi todos nulos. Se define la adición de dos divisores, sumando los coeficientes. El divisor D es *efectivo* o *positivo* si para todos los coeficientes $n_Y \geqslant 0$. Se escribe $D_1 \geqslant D_2$ cuando $D_1 - D_2 \geqslant 0$. Los divisores de Weil de una variedad algebraica forman un grupo denotado $\mathrm{Div}(X)$.

Sea $f : X \to Y$ un morfismo dominante de variedades algebraicas, es decir que la imagen $f(X)$ no está contenida en ninguna hipersuperficie de Y. Para una hipersuperficie Z en Y, la imagen recíproca $Z' = f^{-1}(Z) = \{x \in X \mid f(x) \in Z\}$ es una hipersuperficie de X. Se define entonces $f^*Z = dZ'$ donde d es la multiplicidad. Observamos que la aplicación

$$f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X),$$

que es un homomorfismo de grupos, es bien definida solo cuando f es dominante.

Cuando $f \in K(X)^\times$ es una función racional (no nula), se puede definir el *divisor de la función* f como la diferencia de sus ceros con sus polos, o sea:

$$\mathrm{d}iv(f) := \sum_Y \mathrm{ord}_Y(f) Y,$$

donde $\mathrm{ord}_Y(f)$ es el orden de anulación de f según Y (es positivo si f se anula sobre Y y es negativo si f tiene un polo sobre Y). Tenemos

$$\mathrm{d}iv(fg) = \mathrm{d}iv(f) + \mathrm{d}iv(g)$$

y así los divisores $\mathrm{d}iv(f)$ forman un subgrupo $P(X)$ llamado el subgrupo de los divisores principales. Se nota $\mathrm{C}l(X)$ el cociente $\mathrm{Div}(X)/P(X)$.

Ejemplo 8.1. Escogemos $X = \mathbb{P}^n$, una hipersuperficie $Y \subset \mathbb{P}^n$ es definida por una ecuación $F = 0$, donde F es homogéneo de grado d. Se obtiene un homomorfismo *grado* de $\mathrm{Div}(\mathbb{P}^n)$ hacia $\mathbb{Z}$ que manda $Y = Z(F)$ sobre $d = \deg(F)$. Si Y' es definida por un polinomio F' de grado d, observamos que la función racional $f := F'/F$ tiene como divisor $\mathrm{d}iv(f) = Y' - Y$. Concluimos que $\mathrm{C}l(\mathbb{P}^n) \cong \mathbb{Z}$.

8.0.2. Divisores de Cartier. Para definir un *divisor de Cartier* sobre X escogemos un recubrimiento de abiertos $\{U_i\}_{i\in I}$ con funciones racionales $f_i \in K(U_i)^\times$ tales que $f_i f_j^{-1}$ no tenga polos ni ceros en $U_i \cap U_j$; o sea, tenemos que $f_i f_j^{-1} \in \mathcal{O}(U_i \cap U_j)^\times$. Identificamos dos datos $\{(U_i, f_i)\}_{i\in I}$ y $\{(V_j, g_j)\}_{j\in J}$ cuando $f_i g_j^{-1}$ es regular sin ceros sobre $U_i \cap V_j$; un *divisor de Cartier* es un tal dato $\{(U_i, f_i)\}_{i\in I}$ módulo esta equivalencia.

La adición de dos divisores de Cartier es definida por

$$\{(U_i, f_i)\}_{i\in I} + \{(V_j, g_j)\}_{j\in J} = \{(U_i \cap V_j, f_i g_j)\}_{(i,j)\in I\times J}$$

Un divisor de Cartier $D = \{(U_i, f_i)\}_{i\in I}$ es *efectivo* si las funciones f_i son regulares sobre U_i; el *soporte* $supp(D)$ de D es la unión de los ceros y polos de las funciones f_i. Un divisor de Cartier es *principal* si es de la forma $div(f) = (X, f)$. Los divisores principales forman un subgrupo de los divisores de Cartier. El grupo de clases de divisores de Cartier es denotado $\mathrm{C}aCl(X)$.

Cuando $f : X \to Y$ es un morfismo, definimos la imagen recíproca de $D = \{(U_i, f_i)\}_{i\in I}$ como

$$f^* D = \{(f^{-1}(U_i), f_i \circ f)\}_{i\in I},$$

en particular si $D = (Y, g)$, tenemos $f^*D = (X, g \circ f)$. Esta definición solo es correcta cuando $f(X)$ no está contenido en $supp(D)$ pero observamos que se puede fácilmente remplazar D por $D' \sim D$ tal que D cumpla la condición; de hecho basta remplazar $D = \{(U_i, f_i)\}_{i\in I}$ por $D' = \{(U_i, f_i f_j^{-1})\}_{i\in I}$ para mover el soporte fuera de U_j . Así se puede definir

$$f^* : \mathrm{C}aCl(Y) \to \mathrm{C}aCl(X).$$

Resumimos esto de la manera siguiente, $\mathrm{C}aCl$ es un funtor contravariante, pues tenemos claramente que si $f_1 : X \to Y$ y $f_2 : Z \to X$ son morfismos, $(f_1 \circ f_2)^* = f_2^* \circ f_1^*$.

Ejemplo 8.2. Escogemos $X = \mathbb{P}^n$, si $D = \{(U_i, f_i)\}_{i\in I}$ es un divisor de Cartier efectivo, podemos suponer que cada U_i es contenido en uno de los abiertos canónicos $V_j = \{x \in \mathbb{P}^n \mid x_j \neq 0\}$ y entonces podemos ver f_i como un polinomio en $x_0/x_j, \ldots, x_n/x_j$. Se demuestra fácilmente que la condición de recubrimiento implica que los f_i son las deshomogeneizaciones de un polinomio homogéneo F. Concluimos nuevamente que $\mathrm{C}aCl(\mathbb{P}^n) \cong \mathbb{Z}$. Si $\phi : \mathbb{P}^m \to \mathbb{P}^n$ es un morfismo dado por polinomios homogéneos $(F_0, \ldots, F_n)$ de grado d, la aplicación $\phi^* : \mathbb{Z} \cong \mathrm{C}aCl(\mathbb{P}^n) \to \mathrm{C}aCl(\mathbb{P}^m) \cong \mathbb{Z}$ es dada por $n \mapsto dn$ (Ejercicio).

8.0.3. Fibrados de línea. Como sólo usaremos "fibrados de línea", después de un tiempo hablaremos simplemente de "fibrados".

Un *fibrado* de línea sobre X es una familia continua de líneas parametrizada por X. Más precisamente es un morfismo $p : E \to X$ tal que

- La fibra $E_x := p^{-1}\{x\}$ es un espacio vectorial de dimensión 1.
- La fibración es localmente trivial, es decir, que se puede recubrir X con abiertos U_i sobre los cuales $E_{U_i} = p^{-1}U_i$ es trivial, existe isomorfismos ϕ_i que transforman p en la primera proyección $p_1 : U_1 \times \mathbb{A}^1 \to U_i$; en diagrama

$$\begin{array}{ccc} E_{U_i} & \xrightarrow{\phi_i} & U_i \times \mathbb{A}^1 \\ {\scriptstyle p}\downarrow & \swarrow_{p_1} & \\ U_i & & \end{array}$$

Sea $p : E \to X$ y $p' : E' \to X'$ dos fibrados de línea. Un homomorfismo de fibrados de línea es un morfismo $\phi : E \to E'$, combinado con un morfismo $\bar{\phi} : X \to X'$, tal que $\phi_x : E_x \to E'_{\phi(x)}$ sea lineal, y tal que ϕ, $\bar{\phi}$ conmuten con los morfismos definiendo los fibrados, es decir que el siguiente diagrama sea conmutativo

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ X & \xrightarrow{\bar{\phi}} & X' \end{array}$$

Generalmente se identifican dos fibrados isomorfos.

Ejemplo 8.3. La variedad $X \times \mathbb{A}^1$ con la primera proyección es un fibrado llamado *fibrado trivial*. Consideramos la aplicación cociente $\pi : \mathbb{A}^{n+1}\backslash\{0\} \to \mathbb{P}^n$ que define $\mathbb{P}^n$, podemos construir un fibrado sobre $\mathbb{P}^n$

$$E = \{(x, v) \in \mathbb{P}^n \times \mathbb{A}^{n+1} \mid v = 0 \text{ o } \pi(v) = x\} \to \mathbb{P}^n.$$

Este fibrado no es trivial, en la notación clásica de Serre es el fibrado $\mathcal{O}(-1)$.

Una *sección* de un fibrado $p : E \to X$ es un morfismo $s : X \to E$ tal que $p \circ s = id_X$. El conjunto de las secciones de un fibrado forman un espacio vectorial denotado $\Gamma(X, E)$ (o también $H^0(X, E)$). La propiedad más importante es que, para una variedad proyectiva X, el espacio $\Gamma(X, E)$ es de dimensión finita. Cuando $\Gamma(X, E) \neq \{0\}$ es de dimensión $n + 1$, se puede definir una aplicación racional $\Phi_E : X \cdots \to \mathbb{P}\Gamma(X, E) \cong \mathbb{P}^n$ por la fórmula $\Phi_E(x) = (s_0(x), \ldots, s_n(x))$, donde los s_i forman una base de $\Gamma(X, E)$.

La *suma* de dos fibrados de línea E y E' sobre X es definida como el morfismo $E'' \to X$ tal que las fibras sean el producto tensorial de las dos fibras $(E'')_x = E_x \otimes E'_x$. La imagen recíproca por un morfismo $\phi : Y \to X$ de un fibrado es el producto fibrado $f^*E = Y \times_X E$; al nivel de conjuntos, se puede describir como $\{(y, v) \in Y \times E \mid f(y) = p(v)\}$; las fibras de $p' : f^*E \to Y$ son tales que $(\phi^*E)_y = E_{\phi(y)}$. Se puede describir la construcción con el diagrama

$$\begin{array}{ccc} f^*E & \longrightarrow & E \\ {\scriptstyle p'}\downarrow & & \downarrow{\scriptstyle p} \\ Y & \xrightarrow{f} & X \end{array}$$

Notación 8.4. Para denotar la suma de dos fibrados $\mathcal{L}$ y $\mathcal{M}$ sobre X utilizaremos *dos* notaciones: $\mathcal{L} \otimes \mathcal{M}$ o $\mathcal{L} + \mathcal{M}$. De la misma manera denotamos $\mathcal{L}^{\otimes n}$ o $\mathcal{L}^n$ o $n\mathcal{L}$ la suma de $\mathcal{L}$ con si mismo n veces.

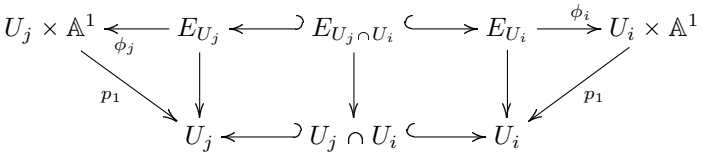
El *dual* de un fibrado $p : E \to X$ es el fibrado $\check{p} : \check{E} \to X$ tal que $\check{E}_x$ sea el dual (como espacio vectorial) de E_x.

Las clases de isomorfismo de fibrados de línea sobre X, con la suma (producto tensorial) forman un grupo llamado el *grupo de Picard* de X y denotado $\mathrm{Pic}(X)$; el inverso de E es su dual. La asociación $X \mapsto \mathrm{Pic}(X)$ es un funtor contravariante, a cada morfismo $f : Y \to X$, corresponde un homomorfismo de grupos $f^* : \mathrm{Pic}(X) \to \mathrm{Pic}(Y)$, y tenemos también $(f_1 \circ f_2)^* = f_2^* \circ f_1^*$.

Comparación de los grupos $\mathrm{C}l(X)$, $\mathrm{C}aCl(X)$ y $\mathrm{Pic}(X)$. Estos no son idénticos en general pero están estrechamente vinculados y, en muchos casos, isomorfos.

Describimos una correspondencia entre (clases de) divisores de Cartier y de Weil. A un divisor de Cartier $D = \{(U_i, f_i)\}_{i\in I}$ se asocia la familia de divisores de Weil principales $D_{U_i} = div(f_i)$ y se observa que la condición $f_i f_j^{-1} \in \mathcal{O}(U_i \cap U_j)^\times$ permite pegar estos divisores de Weil en un divisor de Weil global sobre X, que por tanto no es necesariamente principal. Se obtiene así una aplicación $\lambda : CaCl(X) \to Cl(X)$. Esta aplicación es siempre un homomorfismo pero no precisa ser ni inyectiva, ni sobreyectiva en general. Por ejemplo, cuando X es singular, puede existir hipersuperficies Y en X, pasando por un punto x, que no pueden ser definidas en una vecindad de x por una ecuación.

Describimos la correspondencia entre fibrados y (clases de) divisores de Cartier. Se puede reconstruir un fibrado pegando sus pedazos $E_{U_i} \cong U_i \times \mathbb{A}^1$ a través de los diagramas



es decir consideramos $\phi_j \circ \phi_i^{-1} : (U_j \cap U_i) \times \mathbb{A}^1 \to (U_i \cap U_j) \times \mathbb{A}^1$ que debe escribirse $(x, v) \mapsto (x, f_{ij}(x)v)$ con una función f_{ij} regular e invertible sobre $U_j \cap U_i$ (tales f_{ij} se llaman *funciones de transición* del fibrado E). Vemos que un divisor de Cartier $D = \{(U_i, f_i)\}_{i\in I}$ define un fibrado, escogiendo como funciones de transición $f_{ij} := f_i f_j^{-1}$. Recíprocamente, si $s : X \to E$ es una sección, s proporciona $U_j \xrightarrow{s} E_{U_i} \xrightarrow{\phi_i} U_i \times \mathbb{A}^1$ que tiene la forma $x \mapsto (x, f_i(x)$. Entonces una sección de E define una familia (U_i, f_i) y un divisor de Cartier. Se obtiene así una aplicación $\kappa : CaCl(X) \to \mathrm{Pic}(X)$.

Teorema 8.5. *Sea X una variedad (irreducible), el homomorfismo $\kappa : CaCl(X) \to \mathrm{Pic}(X)$ es un isomorfismo. Sea X una variedad (irreducible) lisa, el homomorfismo $\lambda : CaCl(X) \to Cl(X)$ es un isomorfismo.*

En el caso de una curva proyectiva lisa C, tenemos la aplicación *grado* que asocia a un divisor $D = \sum_{P\in C} n_P P$ su grado $\deg(D) = \sum_{P\in C} n_P$ y se obtiene una sucesión exacta

$$0 \longrightarrow \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0 \tag{8.1}$$

Cuando $C = \mathbb{P}^1$ tenemos $\mathrm{Pic}^0(C) = 0$ y $\mathrm{Pic}(C) = \mathbb{Z}$, pero cuando C no es una curva racional, el grupo $\mathrm{Pic}^0(C)$ no es trivial y además tiene una rica estructura, precisamente de variedad abeliana de dimensión el género de C. Esta sucesión exacta se generaliza a variedades de dimensión mayor de la forma siguiente. Si X es una variedad lisa proyectiva tenemos una sucesión exacta análoga

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{NS}(X) \longrightarrow 0 \tag{8.2}$$

donde $\mathrm{Pic}^0(X)$ es el subgrupo de los fibrados (o clases de divisores) que se puede deformar algebraicamente en el fibrado trivial, y $\mathrm{NS}(X)$ es el grupo de Néron-Severi. Dos características permanecen: el grupo $\mathrm{NS}(X)$ es un grupo de tipo finito (pero no es necesariamente isomorfo a $\mathbb{Z}$) y el grupo $\mathrm{Pic}^0(X)$ es el grupo de puntos de una variedad abeliana.

Terminamos este preliminar geométrico con una generalización del teorema clásico de Bézout *dos curvas planas proyectivas de grado d_1 y d_2 se intersectan en d_1d_2 puntos (contados con multiplicidades).*

Teorema 8.6. *Sea X una variedad lisa proyectiva de dimensión n. Existe una única aplicación multilineal simétrica:*

$$\begin{array}{ccc} \mathrm{Pic}(X) \times \cdots \times \mathrm{Pic}(X) & \to & \mathbb{Z} \\ (\mathcal{L}_1, \ldots, \mathcal{L}_n) & \mapsto & (\mathcal{L}_1 \cdots \mathcal{L}_n) \end{array}$$

tal que, si $\mathcal{L}_i$ corresponde a hipersuperficies Y_i que se intersectan transversalmente, el número $(\mathcal{L}_1 \cdots \mathcal{L}_n)$ es igual al número de puntos de $Y_1 \cap \cdots \cap Y_n$.

9. Fibrados de línea sobre variedades abelianas

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

Teorema 9.1 (Teorema del subibaja)**.** *Sean X, Y variedades y sea $\mathcal{L}$ un fibrado de línea 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 $i_x^*\mathcal{L}$ trivial, entonces existe $\mathcal{M}$, un fibrado de línea 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, Lema A.7.2.3, p. 123] o [12, Corolario 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 [12, p. 55]. □

Se deduce fácilmente el teorema siguiente

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 $\mathrm{Cubo}(\mathcal{L})$ al miembro izquierdo de la última igualdad. Aplicamos Teorema 9.2 mostrando que $\mathrm{Cubo}(\mathcal{L})$ restringido a $A \times A \times \{0\}$ es trivial; notando simetrías tendremos también que $\mathrm{Cubo}(\mathcal{L})$ 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

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

□

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 la fórmula $(f,g,h)^*(\mathrm{Cubo}(\mathcal{L})) = 0$. □

Aplicando Corolario 9.4 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 y simétrico $\mathcal{L}$, el número de intersección (ver Teorema 8.6) $(\mathcal{L})^g := (\mathcal{L}\cdot\cdots\cdot\mathcal{L}) > 0$ y calculamos $([n]^*\mathcal{L})^g = (n^2\mathcal{L})^g = n^{2g}(\mathcal{L})^g = \deg([n])(\mathcal{L})^g$. Como el fibrado $\mathcal{L}$ es amplio, $(\mathcal{L})^g > 0$ y concluimos. □

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 9.4 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, Proposiciones A.7.3.2 y A.7.3.3, p. 129]. □

Observamos que, sobre el cuerpo $\mathbb{C}$, las fórmulas precedentes se pueden demostrar fácilmente, representando un fibrado a través del teorema de Appell-Humbert (teorema 3.1).

10. Polarización, isogenía, variedad dual

10.1. Isogenías. 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 1.13.

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 tenemos $\deg(\alpha) = |(\ker \alpha)(\bar{K})|$; 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 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 $K(X)/\mathrm{Frob}_X^*(K(X^{(p)}))$ es una extensión finita *puramente inseparable* (de grado $p^{\dim X}$). Observamos que la diferencial $(d\,\mathrm{Frob}_X)_x : \mathrm{Tan}_x(X) \to \mathrm{Tan}_{\mathrm{Frob}_X(x)}(X^{(p)})$ 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 $\mathrm{car}(K) = 0$ o $\mathrm{car}(K) = p$ no divide n, entonces $\ker[n](\bar{K}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.*
- *Si $\mathrm{car}(K) = p$, 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 $p = \mathrm{car}(K)$ no divide n, porque entonces la diferencial es una aplicación inyectiva y la isogenía es separable. Cuando $n = p = \mathrm{car}(K)$ la diferencial es nula y se puede deducir que $[p]$ se factoriza a través del Frobenius, es decir existe una otra isogenía [16] $V : A^{(p)} \to A$ tal que $[p] = V \circ \mathrm{Frob}_A$. 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 $K(A) \to K(A^{(p)})$

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

que corresponde a un aplicación racional $V : A^{(p)} \to A$ tal que $V \circ \mathrm{Frob} = [p]$. Además el Teorema 7.6 nos dice que V es un morfismo. Tenemos $p^{2g} = \deg[p] = \deg V \deg \mathrm{Frob}_A = p^g \deg V$, 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 1.19) 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 7.6. 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 de línea sobre una variedad abeliana A, denotamos $K(\mathcal{L})$ el núcleo del homomorfismo $\phi_{\mathcal{L}} : A \to \mathrm{Pic}^0(A)$ dado por $\phi_{\mathcal{L}}(x) = t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$.

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

Demostración. Ver [7, Teorema A.7.2.10, p. 127] o [12, p. 77]. □

10.2. Variedad abeliana dual y polarizaciones. Enunciamos ahora la versión algebraica de la variedad abeliana dual (ver Subsección 3.2 sobre $\mathbb{C}$); se trata de formalizar la idea que el grupo $\mathrm{Pic}^0(A)$ es el grupo de puntos de una variedad abeliana.

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 $\widehat{A}$.*

Demostración. Ver [12, §III.13]. □

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

Para merecer el nombre de dual, tenemos la propiedad que $\widehat{\widehat{A}} \cong A$. En general $\widehat{A}$ no es isomorfa a A pero hay isogenías particulares llamadas *polarizaciones* $\lambda : A \to \widehat{A}$ 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 $\check{\lambda} = \lambda$ (donde $\check{\lambda}$ es definida en la línea siguiente).

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

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

Cuando α es una isogenía, $\check{\alpha}$ es también una isogenía (¡Cuidado! No es exactamente la misma isogenía *dual* que la isogenía definida sobre el cuerpo $\mathbb{C}$ en la primera parte).

Podemos ahora demostrar la versión algebraica del teorema de reducibilidad de Poincaré (sobre $\mathbb{C}$ ver Teorema 1.20).

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 $\phi_{\mathcal{L}} : A \to \widehat{A}$. Definimos C como el componente conexo del núcleo de $\check{\imath} \circ \phi_{\mathcal{L}}$. Tenemos $\dim C = \dim(\ker \check{\imath}) \geqslant \dim \widehat{A} - \dim \widehat{B} = \dim A - \dim B$. 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 10.9). Terminamos concluyendo que $s : B \times C \to A$ tiene un núcleo finito y en 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 (es decir, cuando $\mathrm{car}(K) = 0$ denotamos $\bar{K}$ la clausura algebraica de K, y cuando $\mathrm{car}(K) = p$, denotamos $\bar{K}$ la clausura algebraica separable de 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 las 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 $\check{a} \in \hat{A}[m]$, 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 $f \circ [m] = g^m$. Esta observación nos permite definir:

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

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 las propiedades siguientes

Teorema 11.2 (Emparejamiento[17] de Weil)**.** *Las aplicaciones $e_m : A[m] \times \hat{A}[m] \longrightarrow \mu_m$ son bilineales y cumplen:*

1. *El emparejamiento e_m es no degenerado (es decir de núcleo trivial a la derecha e 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*

$$e_{\ell^\infty} : T_\ell(A) \times T_\ell(\hat{A}) \to T_\ell(\mathbb{G}_m).$$

3. *(Galois equivariancia) Sea $\sigma \in G_K$ entonces*

$$e_m(\sigma(a), \sigma(\check{a})) = \sigma(e_m(a, \check{a})).$$

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

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 [12, pp. 185–186]. □

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}, el grupo de las similitudes simplécticas.

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

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

Relación 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 (11.2).

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 $\mathcal{L}$ amplio sobre A y la polarización asociada $\phi_{\mathcal{L}} : A \to \widehat{A}$ 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 [27, 37, 40])**.** *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) $\Theta_C := W_{g-1} = j_{g-1}(C^{g-1})$, que induce una polarización principal sobre J_C.*

Demostración. Ver [7, Teorema A.8.1.1, pp. 134–135]. □

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[18] 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 espacio dual $H^0(X(\mathbb{C}), \Omega^1_X)^* \cong \mathbb{C}^g$. Las *relaciones de Riemann* (ver [7, §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.*

Denotamos $J_X(\mathbb{C})$ este toro complejo; el vínculo 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

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

y extenderla a divisores.

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

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 $|J_C(\mathbb{F}_q)| = \prod_{i=1}^{2g}(\alpha_i - 1)$.*

Ver [7, ejercicio A.8.11, p. 150].

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, que 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

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

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 $I_X \in K[x_0, \dots, x_n]$, se define $\mathcal{I}_X = I_X \cap \mathcal{O}_K[x_0, \dots, x_n]$ 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 más 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 propiedad 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 módulo $\mathfrak{p}_v$ 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, Teorema C.1.4, p. 263]. □

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

Lema 13.4 (Análogo del lema 13.3 para $\mathbb{G}_m$)**.** *Sean 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 [15, Teorema VII.7.1]. La prueba se adapta al caso general, utilizando los modelos de Néron de una variedad abeliana [36]. □

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

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 (13.6). 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*

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

Sea $\mathcal{L}$ 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 $h_{\mathcal{L}} = h'_{\mathcal{L}} + O(1)$. [19]

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:*

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, Teoremas B.3.2 y B.3.6]. □

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

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 13.12 juntado con la proposición 13.11 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 cuadrática real $\hat{h}_{\mathcal{L},\mathbb{R}} : A(K)\otimes_{\mathbb{Z}}\mathbb{R} \to \mathbb{R}$ 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 (9.4) 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:*
$$A(K) = A(K)_{\mathrm{tor}} \oplus \mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_r$$
donde el grupo de torsión $A(K)_{\mathrm{tor}}$ 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 abeliano tal que $G/2G$ es 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 $q(nx) = n^2q(x)$ y el conjunto $\{x \in G \mid q(x) \leqslant 0\}$ seria infinito) y así podemos definir una semi-norma $|x| = \sqrt{q(x)}$. Sean $y_1, \dots y_m$ representantes de $G/2G$, denotamos $C = \max_i |y_i|$ 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

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

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 $G = \mathrm{Gal}(L/K)$ hacia $A[2]$. □

Paso 2. Supongamos ahora que K es tal que $A[2] \subset A(K)$. Se define un emparejamiento llamado *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 consiguiente $\lambda(P) \in A[2]$.

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)*

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

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 lugares 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 13.3. 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 13.3 concluimos que $\lambda(P, \sigma) = 0$ y, por consiguiente, σ actúa trivialmente sobre F. □

14. Ejercicios

1. Sea C una curva hiperelíptica y ι su involución canónica. Consideramos $L = \{(P, \iota(P)) \mid P \in C\}$. 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 e 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 [15, Teorema III.9.3]. El ejercicio siguiente muestra que el tercer caso puede 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 $|A(\mathbb{F}_q)| = \deg(Id_A - \mathrm{Frob}_A)$. 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 $\phi \circ (Id_A - \mathrm{Frob}_A) = (Id_B - \mathrm{Frob}_B) \circ \phi$, observar que un punto $x \in A$ pertenece a $A(\mathbb{F}_q)$ si y sólo si $\mathrm{Frob}_A(x) = x$ y probar que $Id_A - \mathrm{Frob}_A$ es una isogenía separable.]
5. Sea K cuerpo de característica $\neq 2$ y $f(x) = (x - a_1) \dots (x - a_{2g+1})$ un polinomio separable (es decir que los a_i son distintos). 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 12.4 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 13.3 y deducir que $|J_C(\mathbb{Q})_{\mathrm{tor}}|$ 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 dos variedades abelianas definidas sobre un cuerpo de números K y v un lugar 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 13.3 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 *la clasificación de variedades abelianas principalmente polarizadas* de una dimensión g dada sobre un cuerpo K dado por medio de *invariantes aritméticos explícitos*.

Sección 15 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 16 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 17 aún asume $K = \mathbb{Q}$, aunque entra en el caso mucho más complicado de $g \geqslant 2$. Explica que las conjeturas son conocidas sólo para casos especiales, pero que hay muchos cálculos que apoyan las conjeturas.

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. Esta parte apunta 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*. Esta parte del 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 relativamente fácil 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 $\mathrm{car}(K) > 3$, 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 de que ambas coordenadas sean 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,

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

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

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

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

15.3. El espacio de móduli A_g. La teoría profunda de los esquemas de móduli dice que existe un esquema de módulos gruesos A_g sobre $\mathbb{Z}$ para variedades abelianas. El mapa m en (15.1) envía $A \in \mathrm{PPAb}_g(K)$ a su punto móduli $m(A) \in A_g(K)$. 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 una curva elíptica E dada por (15.2). 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 $\mathrm{car}(K) \neq 2$ y $f(x) \in K[x]$ es separable de grado $2g + 1$ o $2g + 2$. Para un género dado g, considere los espacios de móduli 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 móduli son $(2g - 1, 3g - 3, g(g + 1)/2)$. Luego para $g = 2$, las dimensiones son $(3, 3, 3)$. Como explicaremos en la tercera sección de esta parte, $|H_2(\mathbb{F}_q)| = |M_2(\mathbb{F}_q)| = q^3$ 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 [34]. 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 una variedad abeliana sobre K'. Entonces uno tiene no solo Aut_K, sino también los grupos $\mathrm{Aut}(A_{K'})$ que pueden ser más grandes. 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 $\mathrm{Gal}(K^s/K) = \hat{\mathbb{Z}}$ 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 variedades abelianas de dimensión g sobre K. Una función sobre $\mathrm{Ab}_g(K)$ es llamada *invariante de isogenía* si proviene de una función sobre $\mathrm{IsAb}_g(K)$. 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, como describiremos, 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 $e \leqslant g$, como 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

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

Aquí estamos usando el símbolo del residuo cuadrático,

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

Existen maneras mucho más rápidas de calcular $|C(\mathbb{F}_{q^e})|$ que evaluando directamente el lado derecho de (15.6).

Funciones L desde distintos puntos de vista. Se 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 punto de vista, se 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 tercera opción, se puede 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 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 $\sqrt{q}$.

Como una cuarta manera, se 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 simplex curvilineal 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}. Notar que Sp_{2g} es un subgrupo maximal del grupo complejo $Sp_{2g}(\mathbb{C})$ y una forma interior del grupo real $Sp_{2g}(\mathbb{R})$.

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 $(\alpha, \bar{\alpha}, \alpha, \bar{\alpha})$, $(\alpha, \bar{\alpha}, 1, 1)$, y $(-1, -1, \alpha, \bar{\alpha})$ 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 $(-1, -1, 1, 1)$.

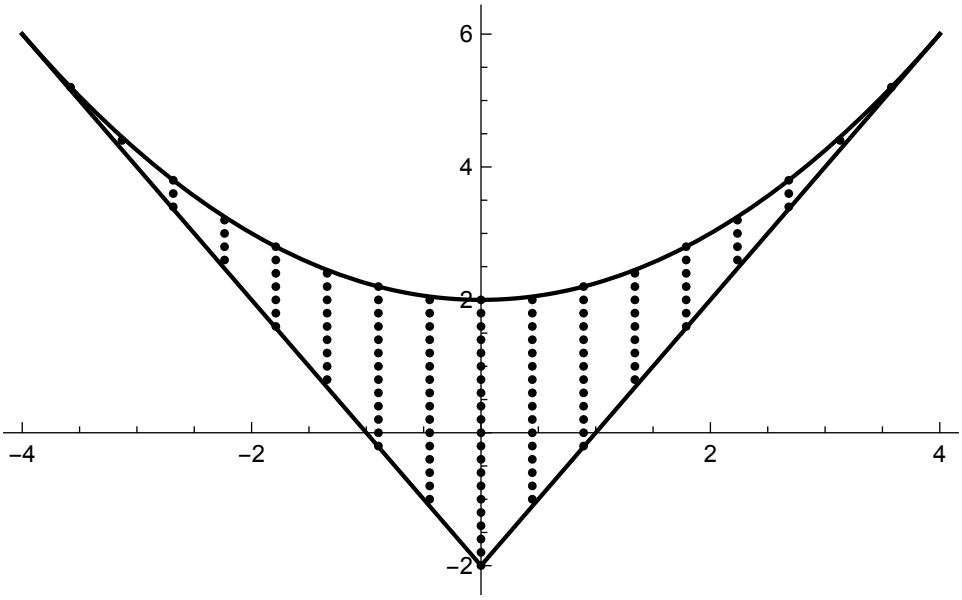


FIGURA 1. El simplex curvilineal $Sp_4^\natural$. Los 129 puntos $\mathrm{fr}_5 = (u_1, u_2) = (a_1/\sqrt{5}, a_2/5)$ corresponden a las 129 funciones L $1 + a_1 5^{-s} + a_2 5^{-2s} + a_1 5^{1-3s} + 5^{2-4s}$ en $\mathcal{L}_2(\mathbb{F}_5)$.

Como una quinta opción, se puede trasladar al lenguaje de *funciones L*, escribiendo

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

Éste es el 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 secciones. Tate probó en [37] la parte de la inyectividad del teorema y describió las obstrucciones. Honda probó en [30] para q general que la imagen es en efecto igual a todas las funciones L no obstruidas.

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 están 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 Figura 1 tienen ecuaciones que se pueden ver en (17.9) 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 ([24]) del volumen Euclidiano V_g de $Sp_{2g}^\natural$ para g arbitrario da

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

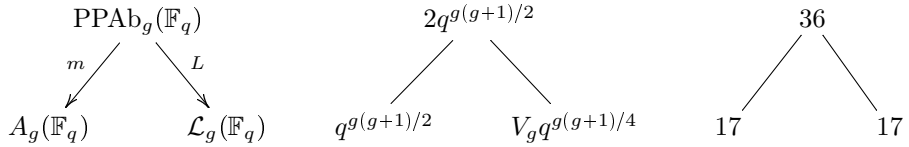
El j-ésimo factor es asintótico a $\sqrt{\pi/j}$, por lo que en particular V_g tiende a 0. Reescalando la j-ésima coordenada por $q^{j/2}$, obtenemos

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

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 revisado. 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. Estas fórmulas muestran que $\mathcal{L}_g(\mathbb{F}_q)$ es mucho más pequeño que los otros dos conjuntos.

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 [38]. 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 $\mathbb{Q}(\sqrt{d})$. 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	a	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 $1 + ap^{-s} + p^{1-2s}$. El correspondiente discriminante $D = a^2 - 4p$ y el número de clases $h(D)$ están dados a la derecha.

La parte derecha de (15.8) 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 motívicos 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 sección de esta parte definiendo grupos de Galois motívicos 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 secciones siguientes, como $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, estarán lejos de ser abelianos. Nuestro propósito principal con esta subsección es dar alguna idea de lo que son estos grupos, antes de ingresar al más sofisticado marco de la próxima sección.

Grupos de números de Weil. Dada $A \in \mathrm{IsAb}(\mathbb{F}_q)$, 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 números de Weil* de A y el grupo Θ es el *grupo de ángulos* 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 Π. El tamaño del subgrupo de torsión de Θ es generalmente t, pero excepcionalmente puede ser $2t$. Este último caso se da cuando por ejemplo $q = p^2$ por $p \in \{2, 3\}$ y $F_q(T) = 1 + pT + q$, donde $t = 2p$.

Rango angular en dimensión 2. Como un ejemplo que será de 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 $b \in \{-2, -1, 0, 1, 2\}$. Los polinomios $f_p(t)$ son productos de polinomios ciclotómicos. Por ejemplo, cuando $b = -1$, $1 - t^2 + t^4 = (1 + t + t^2)(1 - t + t^2) = \Phi_3(t)\Phi_6(t)$.

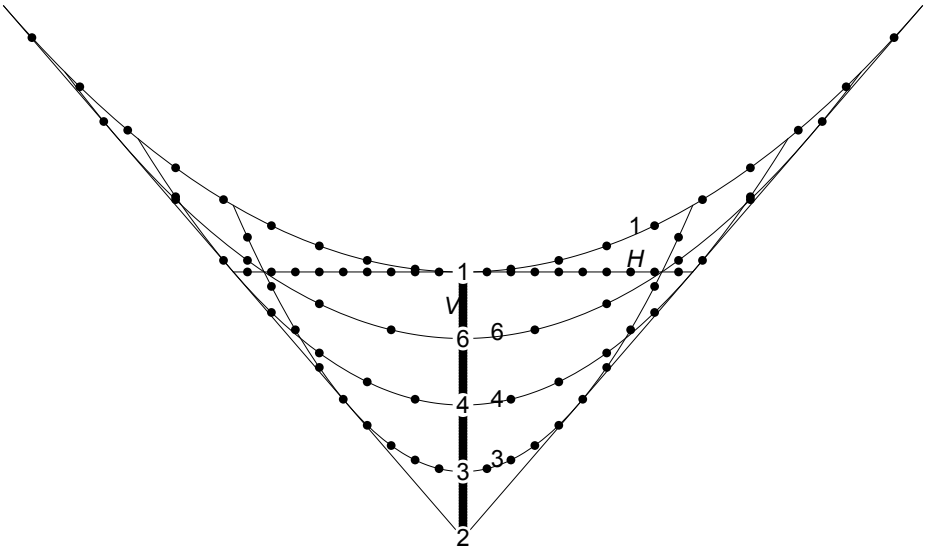


FIGURA 2. El espacio de clases $Sp_4^\natural$ de Figura 1, ahora con cinco puntos etiquetados p_i correspondientes al rango angular cero y seis curvas etiquetadas correspondientes a rango angular uno. Los 164 puntos de $\mathcal{L}_2(\mathbb{F}_{23})$ que tienen rango angular uno están también dibujados, 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 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 $p_k = (0, 4\cos^2(\pi/k) - 2)$.

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

Punto	$f_p(t)$
$p_2 = (0,-2)$	$(1-t)^2\,(1+t)^2$
$p_3 = (0,-1)$	$1-t^2+t^4$
$p_4 = (0,0)$	$1+t^4$
$p_6 = (0,1)$	$\Phi_3(t)\,\Phi_6(t)$
$p_1 = (0,2)$	$(1+t^2)^2$

Curva	$f_p(t)$	$g_p(t)$
$V_2:\ u=0$		$(t+1)^2\,(t^2-vt+1)$
$C_3:\ v=u^2-1$		$(t^2+t+1)\ \ (-tu^2+t^2+2t+1)$
$C_4:\ v=\frac{u^2}{2}$		$(t^2+1)\ \ (-\frac{tu^2}{2}+t^2+2t+1)$
$C_6:\ v=\frac{u^2}{3}+1$		$(t^2-t+1)\ \ (-\frac{tu^2}{3}+t^2+2t+1)$
$C_1:\ v=\frac{u^2}{4}+2$	$(t^2+\frac{ut}{2}+1)^2$	$(1-t)^2\,(-\frac{tu^2}{4}+t^2+2t+1)$
$H_4:\ v=2$	$(t^2+1)(t^2+ut+1)$	

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

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

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

Cuando usamos la ecuación de la curva para remover la variable, entonces $g_p(t)$ se factoriza en los casos listados en Cuadro 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 vía 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.

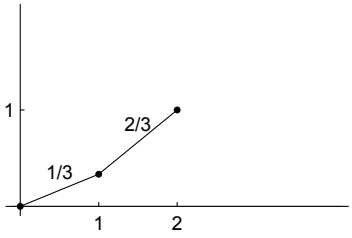
Sea ST el grupo dual de Θ. Aquí vemos Θ como un grupo discreto tal que ST es compacto. Su componente de la identidad ST^0 es el producto de r círculos. El grupo ST/ST^0 es isomorfo a $\mathbb{Z}/(\delta t)$. El grupo ST es el *grupo de Sato-Tate* de A.

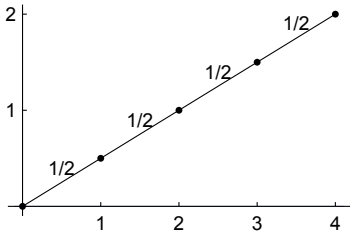
Para Π procedemos de manera similar. Sin embargo, esta vez, prestamos atención a la acción natural de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Sea G el grupo dual de Π, ahora considerado en el marco de grupos algebraicos conmutativos sobre $\mathbb{Q}$. La componente identidad G^0 satisface $G^0(\mathbb{C}) \cong (\mathbb{C}^\times)^{r+1}$. 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. Verificar que la curva elíptica (15.5) realmente tiene invariante j igual a j.
2. Construir el cuadro análogo a Cuadro 1 para $p = 5$.
3. Explorar la sección de la LMFDB sobre variedades abelianas sobre $\mathbb{F}_q$. Algunos posibles temas son:
   - ¿Cuán común es para A no ser una Jacobiana porque 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) es primitivo?
4. Los puntos $(u_1, \ldots, u_g)$ en $Sp^\natural_{2g}$ correspondientes al rango angular 0 son aquellos con coordenadas enteras. Usar la factorización de polinomios de Frobenius unitarizados $f_p(t) = 1 + u_1 t + \cdots + u_1 t^{2g-1} + t^{2g}$ en polinomios ciclotómicos para contar el número N_g de tales puntos vía funciones generatrices. (Se necesita considerar $\Phi_1(t) = t - 1$ y $\Phi_2(t) = t + 1$ de manera diferente que 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 del Teorema 15.1.
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 obstrucciones reales. Considera también los siguientes fenómenos que son visibles 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 $\mathbb{F}_{p^2}$ para $p \leqslant 7$, pero no en la página para superficies abelianas sobre $\mathbb{F}_{11^2}$.

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





7. El grupo de Galois G de un polinomio conformalmente palíndromo $F_q(T) = 1 + a_1 T + \cdots + a_1 q^{g-1} T^{2g-1} + q^g T^{2g}$ está en $2^g.S_g$, el grupo de orden $2^g g!$ que consiste en permutaciones de las raíces los cuales conmutan con la involución

$\alpha \mapsto q/\alpha$ sobre las raíces. Probar que si $g \geqslant 2$ y $G = 2^g.S_g$, entonces el rango angular de $F_q(T)$ es g.

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

Esta segunda sección 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, $(x, y) \mapsto (-x, iy)$, 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 genérica.

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 primos malos 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 la 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 vía representaciones módulo 2 al final de §16.10. De manera similar, los factores 2^c serán explicados allí vía representaciones 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 ([19]) 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 ([22]) 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.

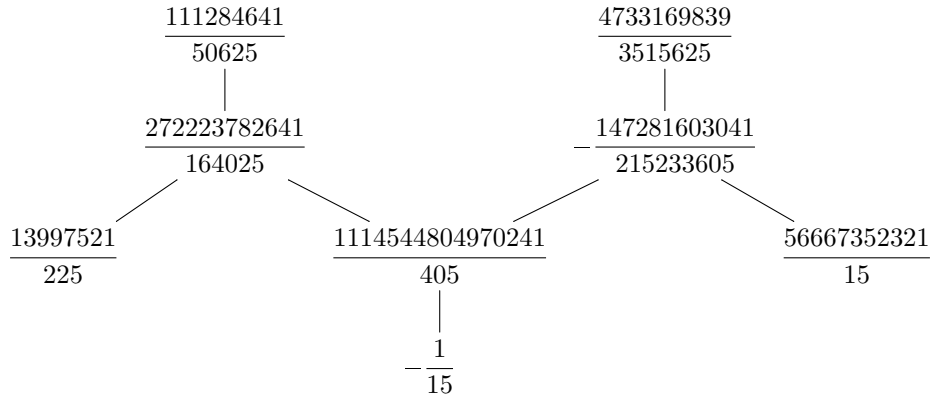
Conductor N	Número de curva elípticas	Número encontrado por una búsqueda muy rápida
11	3	1
14	6	1
15	8	1
17	4	1
19	3	1
20	4	1
21	6	1
24	6	1

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. La búsqueda consideró curvas elípticas en la "forma larga" estándar

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

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



La búsqueda encontró solo la curva con invariante j igual a $-1/15$. El diagrama ilustra que el tamaño de 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 de Teorema 16.8.

16.3. Funciones L como series de Dirichlet definidas por productos de Euler. Dada $A/\mathbb{Q}$ 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 sección 15 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 $T = p^{-s}$. 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 (16.1) convergen absolutamente en el semi-plano derecho $\Re(s) > 3/2$. Por el momento, asuntos analíticos no jugarán ningún papel, y uno puede considerar $L(A,s)$ como un paquete formal de cantidades $L_p(A,s)$, permitiendo las modificaciones en un número finito de primos malos que describiremos en §16.9. Sea $\mathcal{L}_g(\mathbb{Q})$ el conjunto de todos estos productos formales.

Faltings [27] generalizó la parte de la inyectividad en el Teorema de Honda-Tate, de tal manera que $\mathrm{IsAb}_g(\mathbb{Q}) \to \mathcal{L}_g(\mathbb{Q}) : A \mapsto L(A,s)$ 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 iguales! Uno de los propósitos de los grupos de Galois motívicos G, y de sus variantes fáciles, 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 un anillo de endomorfismos $\mathrm{End}(A)$ y un anillo de endomorfismos geométricos $\mathrm{End}(A_{\overline{K}}) \supseteq \mathrm{End}(A)$. 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 $\mathrm{End}(E_{\overline{\mathbb{Q}}})$ es genéricamente $\mathbb{Z}$, también puede ser un anillo cuadrático R con discriminante negativo D. En este caso, se dice que E tiene multiplicación compleja potencial por $\mathbb{Q}(\sqrt{D})$. 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

Ya que los invariantes j son $j_1 = 1728$ y $j_2 = 2048/3$, la curva E_1 tiene multiplicación compleja potencial por $\mathbb{Q}(i)$ mientras que E_2 es genérica.

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. Esto es un subgrupo del grupo simpléctico conforme GSp_{2g}. Existen un número de definiciones competentes para G, las cuales no se sabe si son equivalentes en general. Nosotros tomamos la de Parte I de [23], 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:	$\mathbb{Q}$	$\mathbb{Q}$	$GL_2(\mathbb{Q})$
CM potencial :	$\mathbb{Q}$	F	$N(F^\times)$
CM:	F	F	$F^\times$

Luego en el caso CM, G es un toro de dimensión dos. En el caso CM potencial, 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 del anillo de funciones invariantes es su variedad de clases $G^\natural$. Para el mismo GSp_{2g}, la variedad de clases puede ser identificada 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 $\mathrm{GSp}_{2g}^\natural(\mathbb{Q})$. 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 para los polinomios de Frobenius de curvas elípticas con CM potencial 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 multiplicado por un cuadrado.

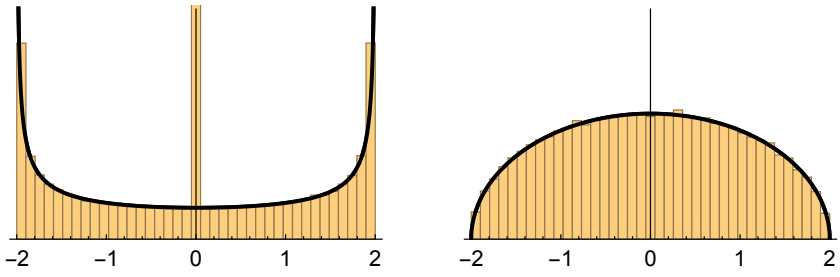
Para probar que una curva elíptica E sobre $\mathbb{Q}$ no tiene CM potencial, no se debe usar el invariante j. Sólo se necesita mostrar que las condiciones mencionadas no son satisfechas. Por ejemplo, 5 y 13 son los primos menores p tales que $F_p(E_2, T)$ tiene un término lineal no nulo. Sus discriminantes módulo cuadrados son $d_5 = -1$ y $d_{11} = -7$. El hecho que $-1 \neq -7$ implica que $G = GL_2$. La Proposición 17.1 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 §15.6, 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. El grupo ST es Sp_2 si E no tiene potencial CM. 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:

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

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 (16.2) 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 $Sp_{2g}^\natural$, 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 sección. El hecho de que la Conjetura 16.1 parezca verdadera es quizás la forma más rápida de ver la importancia de grupos de Galois motívicos.

La conjetura ya era conocida en los años sesenta para curvas elípticas con CM. El caso $g = 1$ fue probado completamente en una sucesión de artículos hace diez años, comenzando con [21].

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

La extensa demostración de este teorema usa propiedades analíticas de no solo $L(E,s)$, sino también de las funciones $L(\mathrm{Sym}^k E, s)$ 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 $H^1(A(\mathbb{C}), \mathbb{Q}_\ell)$ vía 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 [23], la imagen vive en $G(\mathbb{Q}_\ell)$.

Llevando la medida de probabilidad de Haar de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ hacia $\mathrm{GSp}_{2g}^\natural(\mathbb{Z}_\ell)$ 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 la imagen K_ℓ de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ en $G(\mathbb{Q}_\ell)$, y entonces muchas posibilidades para μ_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 $G = \mathrm{GSp}_{2g}$, la conjetura dice que la imagen tiene índice finito en el grupo $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ 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 [35]. Para el segundo, la hipótesis implica que $G = \mathrm{GSp}_{2g}$.

En el resto de esta subsección, damos una idea de cómo se ve en términos computacionales. 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 3 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 $GL_2(\mathbb{F}_2) = S_3$. Particiones de factorización λ_p y trazas a_p son coordenadas como en las dos columnas de la izquierda.

(16.3)

λ_p	a_p	masas genéricas	# para E_1	# para E_2
3	1	1/3		
2 1	0	1/2		50038
1^3	0	1/6	100000	49962

Cuando $x^3 + bx + c$ es irreducible con grupo de Galois S_3, 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, porque los polinomios $x^3 + bx + c$ son reducibles:

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

Las masas que gobiernan estos dos casos no son $(1/3, 1/2, 1/6)$ sino $(0, 0, 1)$ y $(0, 1/2, 1/2)$. En el ejemplo, las representaciones mód 2 son diferentes, aunque sus semisimplificaciones son la misma, lo que significa que a_p es siempre par. La 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.

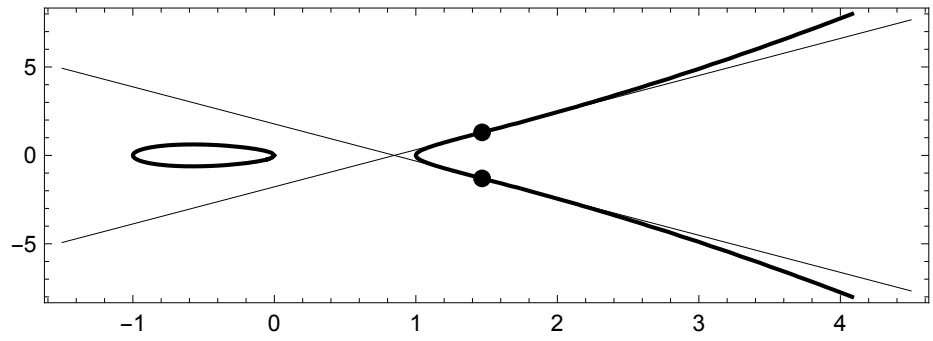


FIGURA 3. La curva $E_1(\mathbb{R})$. Se destaca los dos puntos 3-torsión reales y sus tangentes inflexivas.

Mód 3. Para ℓ un primo impar, hay relaciones de recursión clásicas que dan "polinomios de división" $f_\ell(y)$ de grado ℓ^2-1 con raíces las y-coordenadas de los puntos de torsión en E de orden ℓ. Para abreviar, 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 $P+P+P=0$. La descripción geométrica 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:

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

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

La siguiente tabla es análoga a (16.3), pero ahora para $\ell=3$.

(16.4)

λ_p	$F_p(T)$	masas genéricas	# para E_1	# para E_2
1^8	$1+T+T^2$	1/48	6253	2042
2^4	$1-T+T^2$	1/48	6246	2094
$3^2\,1^2$	$1+T+T^2$	1/6		16584
$6\ \ 2$	$1-T+T^2$	1/6		16686
4^2	$1\quad\ +T^2$	1/8	37463	12556
$2^3\,1^2$	$1\quad\ -T^2$	1/4	25027	24952
8	$1-T-T^2$	1/8	12520	12545
8	$1+T-T^2$	1/8	12491	12541

Aquí, las última columnas corresponde al número de primos entre $5, 7, \ldots, p_{100002}$ 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 $(1/16, 1/16, 0, 0, 3/8, 1/4, 1/8, 1/8)$.

Para ℓ general, las clases de Frobenius pertenecen a $GL_2(\mathbb{F}_\ell)^\sharp$, 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, pero ningún invariante por sí mismo es suficiente. En el caso $\ell=3$, el invariante λ_p determina un conjunto cociente de seis elementos mientras que $F_p(T)$ determina un conjunto cociente de siete elementos. Para λ_p, el problema es la repetición de 8 en su columna, mientras que para $F_p(T)$ los dos problemas son la repetición de $1+T+T^2$ y $1-T+T^2$.

Recordemos que un problema fundamental es caracterizar la imagen de $\operatorname{IsAb}_g(\mathbb{Q})$ en $\mathcal{L}_g(\mathbb{Q})$. El hecho que para cualquier ℓ^e, los coeficientes 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 §16.1 y §16.2 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. En 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.

En casos fáciles, las cantidades son calculables. Por ejemplo, en el marco hiperelíptico supongamos que el polinomio $f(x)$ tiene discriminante divisible exactamente por p^k con $k \leqslant g$ y el polinomio reducido a $\mathbb{F}_p[x]$ 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 moderada. Una condición suficiente para que la ramificación sea moderada es que $p > 2g+1$. En el marco de la teoría de la ramificación, esta condición proviene del 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 $\mathbb{Q}[y]/f_\ell(y)$ también 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 vía 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 vía 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 grande 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

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

Como mencionamos previamente, el producto que define a $L(A, s)$ converge sólo para $\mathrm{Re}(s) > 3/2$. 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 CM potencial. En los años noventa, la demostración para curvas elípticas fue muy famosa.

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

La larga demostración comienza en [39]. 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 16.7 sea cierta con A reemplazado por $A^{1/d}$. Más aún, podríamos ser más optimista y esperar que cualquier función que satisfaga Conjetura 16.7 provenga de una variedad abeliana de esta manera. 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 búsqueda más extensa de curvas elípticas con $|a_1|, |a_2|, |a_3| \leqslant 1$ como antes, pero ahora con $|a_4|, |a_6| \leqslant 10$. ¿Cuántas de las 93 clases de isogenía con conductor $\leqslant 100$ se encontraron? ¿Cuántas de las 306 curvas se encontraron?
2. Explorar la sección de la LMFDB de curvas elípticas sobre $\mathbb{Q}$. Algunos posibles temas son:
   - ¿Cuáles conductores tienen una gran cantidad de clases de isogenía?
   - ¿Cuál es el significado de los enormes picos en la función Z para la única curva en la base de datos con rango 4?
   - ¿Cuál es la cota de conductor mínima para la 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. Es de notar que su Jacobiana es isógena 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 §16.4 se factoriza en primos pequeños solamente. Por ejemplo, el código en *Magma* `Factorization(-3375+32768);` revela que la diferencia $j_{-7} - j_{-11}$ es $7 \cdot 13 \cdot 17 \cdot 19$. Intenta adivinar rasgos de la fórmula general sin leer la referencia [29].

4. El código de *Magma*
```
E2 := EllipticCurve([6,7]);
L2 := LSeries(E2);
&+[(Coefficient(L2,NthPrime(j))/Sqrt(NthPrime(j)))^4 :
   j in [1..100000]]/100000;
```
devuelven $1.995\ldots$, mientras que el cuarto momento de la correspondiente medida es $m_4 = \int_{-2}^{2} u^4 \mu_{Sp_2} = 2$. Este 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 los 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 utiliza el "identifier" a [32] para obtener información sobre el comportamiento 2-ádico de los dos polinomios. ¿Cómo comparan las pendientes 2-ádicas (dadas en la columna "Galois slope content")? Repetirlo para E_2.

7. Ve en la LMFDB de la página de E_1 hasta la página de su forma modular f_1, para aprender 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 coeficientes de Dirichlet de $L(E_1, s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Escoge un número primo grande p y compute a_p de E_1. Independientemente, computa 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 última sección continuamos la discusión de invariantes y clasificación, aunque ahora considerando ejemplos del caso menos familiar de Jacobianas de curvas de género dos. Haremos contacto con cada una de las tres conjeturas mostradas en la sección 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

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

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

La curva C_1 es especial porque no tiene solo la involución hiperelíptica $(x, y) \mapsto (x, -y)$, 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 y $h(x) \in \mathbb{Z}[x]$ de grado $\leqslant 3$. Su discriminante es $\hat{\Delta} = 2^{10}\,|\operatorname{disc}(f + \frac{h^2}{4})|$. El discriminante Δ es el mínimo de todos estos $\hat{\Delta}$ y otros que provienen de presentaciones donde $f(x)$ tiene grado cinco (estos usualmente no son necesarios).

En general el conductor divide al discriminante: $N|\Delta$. La desigualdad $\operatorname{ord}_p(N) \leqslant \operatorname{ord}_p(\Delta)$ 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 [20] 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 curvas de género dos 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 $\Delta \leqslant 10^6$ perdidas por la búsqueda. Mucho más en serio para las aplicaciones, hay muchas curvas con conductor N pequeño, que no aparecen porque su discriminante Δ es más que 10^6. El artículo [20] da evidencia de que la lista puede estar completa con respecto a las clases de isogenía para $N \leqslant 1000$. El final de §17.3 nos muestra que a la clase de isogenía de C_1 con $N = 360$ le faltan al menos cinco curvas. Los ejercicios da una clase de isogenía con $N = 1024$ también faltante.

17.2. Análogos de invariantes j. La fórmulas clásicas de esta subsección se dan con más información en la LMFDB. 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

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

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 móduli compactada $\overline{M}_2$ para las curvas de género dos es el espectro proyectivo $\operatorname{Proj} R$ 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

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

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 estos 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 rápidamente. Se tiene $A_2 = M_2 \coprod S$ donde S es el producto simétrico de dos copias de la línea j. Entonces para entender A_2, entender M_2 es el paso principal.

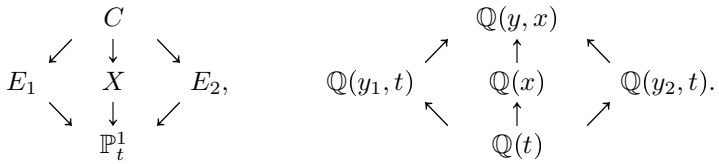
17.3. Una subvariedad clásica de A_2. Muchos anillos R surgen como anillos de endomorfismos de superficies abelianas que uno prácticamente puede enumerar. En consecuencia, hay muchas subvariedades naturales X_R de A_2, y la situación es mucho más complicada que la colección de subvariedades de dimensión cero X_D de A_1 tratada en §16.4. 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-torsión racionales. Se pueden escribir en la forma de Legendre como

$$y_1^2 = t(t-1)(t-\lambda), \qquad y_2^2 = t(t-1)(t-\mu). \tag{17.4}$$

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

A la izquierda tenemos un diagrama de curvas:



Aquí C es el producto fibrado de E_1 y E_2. Su cuerpo de funciones $\mathbb{Q}(C) = \mathbb{Q}(t, y_1, y_2)$ 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 $y_1 \mapsto \epsilon_1 y_1$ y $y_2 \mapsto \epsilon_2 y_2$. La conducta de la ramificación nos dice que C tiene género dos y el cociente $X := C/(-1,-1)$, con cuerpo de funciones $\mathbb{Q}(t, y_1 y_2)$, 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

$$t = \frac{\mu x^2 - \lambda}{x^2 - 1}. \tag{17.5}$$

Define

$$y = (-1+x)^2(1+x)(y_1 + y_2). \tag{17.6}$$

Eliminando las variables y_1, y_2 y t del sistema (17.4),(17.5),(17.6), obtenemos una ecuación estándar para C,

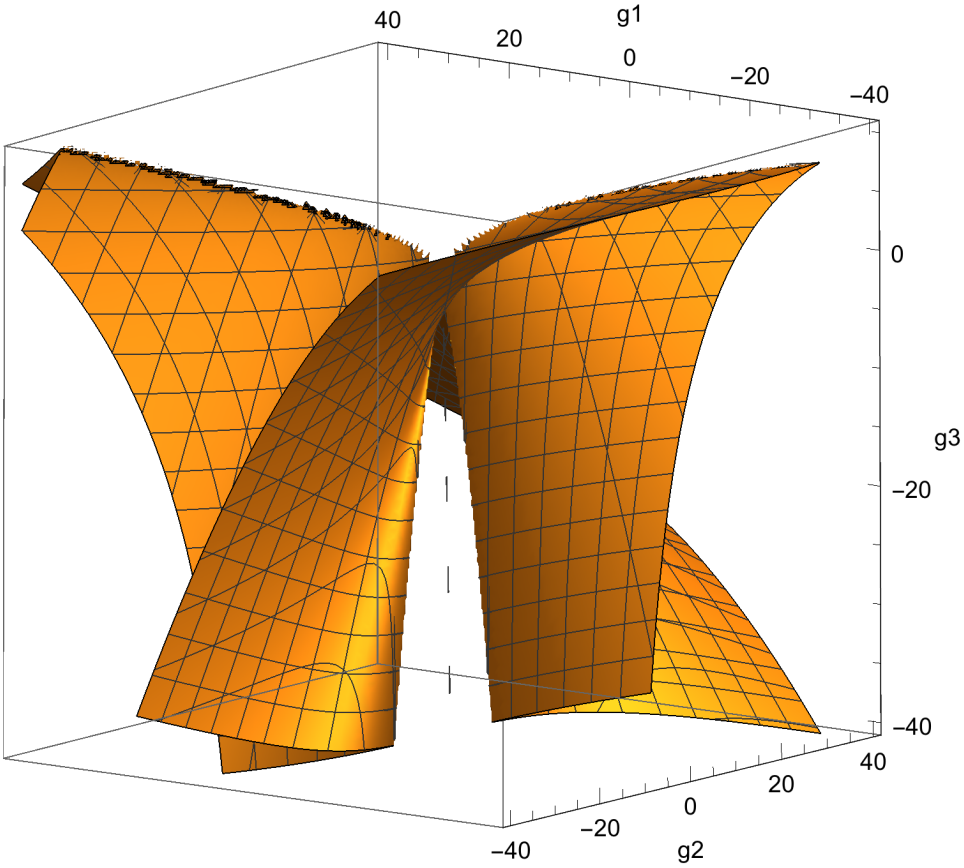
$$y^2 = (\mu - \lambda)(x-1)(x+1)\left(\lambda - \mu x^2\right)\left(\lambda - \mu x^2 + x^2 - 1\right). \tag{17.7}$$

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 primera 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 (17.3), la relación es

$$
\begin{aligned}
&-51200000g_1^4+432g_1^5-28800g_1^4g_2+512000g_1^3g_2^2-8g_1^3g_2^3+512g_1^2g_2^4\\
&-8192g_1g_2^5+96000g_1^4g_3-11520000g_1^3g_2g_3+72g_1^4g_2g_3-4816g_1^3g_2^2g_3\\
&+84480g_1^2g_2^3g_3-g_1^2g_2^4g_3+64g_1g_2^5g_3-1024g_2^6g_3+48g_1^4g_3^2+12960g_1^3g_2g_3^2\\
&-691200g_1^2g_2^2g_3^2+2g_1^3g_2^2g_3^2-136g_1^2g_2^3g_3^2+2304g_1g_2^4g_3^2+129600g_1^3g_3^3\\
&-g_1^4g_3^3+72g_1^3g_2g_3^3-1080g_1^2g_2^2g_3^3-6912g_1g_2^3g_3^3-216g_1^3g_3^4+7776g_1^2g_2g_3^4\\
&-11664g_1^2g_3^5=0.
\end{aligned}
\tag{17.8}
$$

Por diversión, aquí tenemos un vistazo de la superficie $X_R(\mathbb{R})$ 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 (17.7) de $C_{-15,-3}$ por 12^2, obtenemos la ecuación (17.1) 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, estas son 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 $C_{-15,-3}$ 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 de la Jacobiana de $C_1 = C_{-15,-3}$ contiene exactamente $8 \times 6 = 48$ elementos. Al menos seis de estas 48 superficies abelianas tiene polarización principal, a saber las seis $C_{\lambda,\mu}$. Asimismo, la LMFDB actualmente tiene sólo C_1.

17.4. Polinomios de Frobenius y grupos de Galois motívicos. Evaluando (15.6) 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 §16.6 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 $\mathrm{GSp}_{2g}^\natural(\mathbb{Q})$. 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.

En este contexto, hay una proposición general que es muy útil:

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 G de A es tan grande 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 clasificación de subgrupos de grupos reductivos que contienen un toro maximal. Si para un segundo primo q, el subgrupo contiene un toro maximal completamente diferente, la única posibilidad es $G = \mathrm{GSp}_{2g}$.

Es fácil de aplicar Proposición 17.1. 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

$$f_{Sp_2\times Sp_2} = \frac{1}{2\pi^2}\sqrt{\frac{(-2u+v+2)(2u+v+2)}{u^2-4v+8}}, \tag{17.9}$$
$$f_{Sp_4} = \frac{\sqrt{(u^2-4v+8)\,(-2u+v+2)(2u+v+2)}}{4\pi^2}.$$

La equidistribución de clases de Frobenius $\mathrm{fr}_p = (u_p, v_p)$ es parcialmente sabida en el primer caso, ya que por los dos factores se puede aplicar Teorema 16.1. Casi nada se conoce en el segundo caso. Los primeros cien fr_p en nuestros dos casos coinciden en la densidad de Sato-Tate, todas ilustradas en Figura 4.

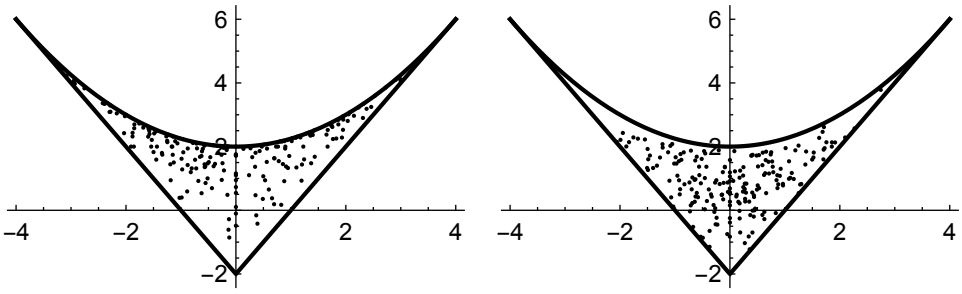


FIGURA 4. Puntos en el escudo $Sp_4^\natural$ representando el fr_p para los primeros cien primos buenos para C_1 (izquierda) y C_2 (derecha).

Algunas veces, como veremos pronto, uno se interesa solo en la distribución de a_1. La conjetura de Sato-Tate dice que estos números a_1 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 $v = u_2$ para obtener funciones en $u = u_1$:

$$\frac{24\pi^2\phi_{Sp_2\times Sp_2}}{u+4} = \left(u^2+16\right)E\left(\frac{(u-4)^2}{(u+4)^2}\right) - 8uK\left(\frac{(u-4)^2}{(u+4)^2}\right), \tag{17.10}$$
$$\frac{240\pi^2\phi_{Sp_4}}{u+4} = \left(u^4+224u^2+256\right)E\left(\frac{(u-4)^2}{(u+4)^2}\right)$$
$$- 8u\left(u^2+24u+16\right)K\left(\frac{(u-4)^2}{(u+4)^2}\right).$$

Aquí, E y K son integrales elípticas completas clásicas. A pesar de la formas funcionales complicadas de las ϕ_{ST}, los gráficos tienen una apariencia simple, como se muestra en Figura 5.

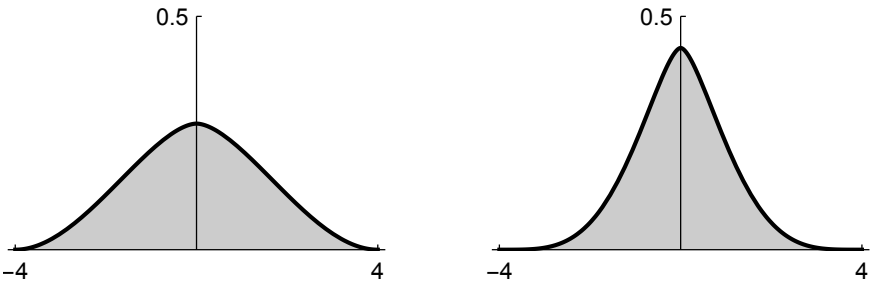


FIGURA 5. Densidades $\phi_{Sp_2\times Sp_2}$ y ϕ_{Sp_4} con varianza 2 y 1.

La fórmula del carácter de Weyl da expresiones explícitas para $f_{Sp_2^g}$ y $f_{Sp_{2g}}$ para g general, similar en apariencia al caso $g = 2$ (17.9). Sin embargo, las funciones $\phi_{Sp_2^g}$ y $\phi_{Sp_{2g}}$ se vuelven 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 anillos 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 se puede calcular una gran cantidad de u_1 pero ningún u_g. En esta situación, Proposición 17.1 no está disponible para ayudar a determinar el grupo de Galois motívico 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

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leqslant x} u_p^k = \int_{-2g}^{2g} \phi_{ST}(u) u^k du. \tag{17.11}$$

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 el rango de $\mathrm{End}(A)$. Luego, si $m_2 = 1$, existe solo la posibilidad de $\mathrm{End}(A) = \mathbb{Z}$. En general, escribiendo E_1, E_2 y E_4 para $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$ respectivamente, las posibilidades para $\mathrm{End}(A)_{\mathbb{R}} := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{R}$ son

$$\bigoplus_i M_{j_i}(E_{d_i}) \tag{17.12}$$

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 (17.12) son

$$\prod_i G_{d_i,g_i}. \tag{17.13}$$

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

$$m_4 \geqslant 3m_2. \tag{17.14}$$

Supongamos, para hacer un enunciado limpio, que todos los g_i son al menos 2. Entonces, la alternativa de Larsen [33] nos dice que la igualdad vale si y sólo si G tiene el mismo grupo derivado que (17.13). "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 $7!! = 7 \cdot 5 \cdot 3 \cdot 1 = 105$. 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 $(m_2, m_4, m_6) = (1, 3, 14)$, 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 (17.13) 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 [28] que son 34 las posibilidades que ocurren sobre $\mathbb{Q}$ y entonces 18 más posibilidades que solo ocurren sobre cuerpos de números más grandes. Cada uno de los 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 [28], el grupo llamado $J(O)$ allí. Como muchos de los 52 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

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

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 tensorial 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

$$\mu_{J(O)} = \frac{3}{16}\delta_{p_2} + \frac{1}{6}\delta_{p_3} + \frac{1}{8}\delta_{p_4} + \frac{1}{48}\delta_{p_1} + \frac{3}{16}\nu_{V_2} + \frac{1}{6}\nu_{C_3} + \frac{1}{8}\nu_{C_4} + \frac{1}{48}\nu_{C_1}. \tag{17.15}$$

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 consecuencia, le medida unidimensional sobre $[-4, 4]$ es

$$\nu_{J(O)} = \frac{11}{16}\delta_0 + \left(\frac{f(u)}{6} + \frac{f\left(u/\sqrt{2}\right)}{8\sqrt{2}} + \frac{f\left(u/2\right)}{96}\right)du. \tag{17.16}$$

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

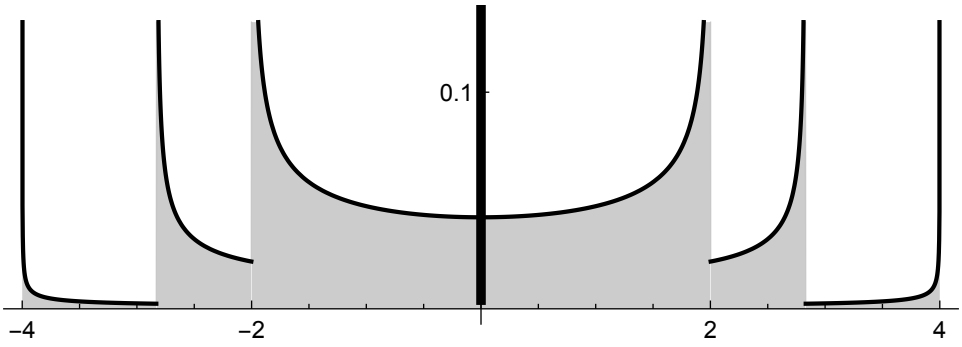


FIGURA 6. La medida Sato-Tate $\nu_{J(O)}$ de (17.16), con masa 11/16 a 0 y la masa restante dada por una densidad discontinua.

cientos de curvas y ver sólo distribuciones del tipo gaussiano de Figura 5, y luego de repente encontrarse con $\nu_{J(O)}$ desde la inofensiva curva $y^2 = x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$.

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

(17.17)

	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

$$S_{2g+2} \to \mathrm{GSp}_{2g}(\mathbb{F}_2).$$

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 $\ell = 3$. El método clásico para producir el polinomio de división se describe con detalles en [26]. El polinomio para $y^2 = x^5 + bx^3 + cx^2 + dx + e$ es par y comienza

$$f_3(b,c,d,e;x) = x^{80} + 15120\,b\,x^{76} + +2620800\,c\,x^{74} + (419237280\,d - 35394408\,b^2)\,x^{72} + \cdots \tag{17.18}$$

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 para $\ell = 2$. Las distribuciones de $(\lambda_p, F_p(T))$ para los primeros 10^5 primos buenos están en las dos últimas columnas:

λ_p	$F_p(T) \in \mathbb{F}_2[T]$	masas genéricas	# para C_1	#para 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		
$3\ 1^3$	$(1+T)^2\left(1+T+T^2\right)$	1/18		33380
$3\ 2\ 1$	”	1/6		
3^2	$\left(1+T+T^2\right)^2$	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 de $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ se convierte en equidistribuida en el espacio de polinomios característicos $\mathrm{GSp}^\natural_{2g}(\mathbb{F}_\ell)$ 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 §16.10, es el de analizar la mala reducción. Como un ejemplo de esto, aplicamos (17.18) a la curva C_2 buscando información sobre la reducción mala de C_2 en 2. Cambiando coordenadas en (17.2) vía $(x, y) \mapsto (-100/(15 + x), -20y/(15 + x)^3)$ para expresar C_2 vía un polinomio de quinto grado, evaluamos (17.18) 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 [32] dice que $f_{8u}(x)$ es no ramificado. Aplicando 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 posibilidad para la valuación 2-ádica de la conductor de C_2 es dos veces la 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 16.7 es desconocida. Notablemente, uno puede todavía calcular con una precisión muy alta. Hay un paquete muy útil en *Magma*, que viene de [25]. Nuestra curva C_2 da un ejemplo representativo. Dados los polinomios de Frobenius en (17.4), las posibilidades localmente permitidas por el conductor son 2^a3^b con $0 \leqslant a \leqslant 8$ y $0 \leqslant b \leqslant 5$, como en el caso de curvas elípticas. Usando `CFENew` de *Magma* para examinar todas las posibilidades da los siguientes números.

$a\backslash b$	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 enfáticamente que el conductor correcto es 2^53^4. Los escépticos podrían probablemente considerar todavía a 2^53^2 como una posibilidad. Se puede calcular con 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 nos da

$$0.00069191183229691135350870962 1 \text{ para } 2^53^2 \text{ en } 0.39 \text{ segundos.}$$

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

0.00000000000000000000000000000000 para $2^5 3^4$ en 1.26 segundos.

Una prueba de Conjetura 16.7 espera progreso en las conexiones con formas automorfas. Pero cálculos significativos ya son posibles, incluso en mayores dimensiones g.

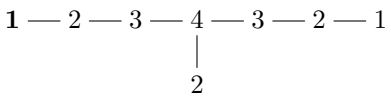
17.8. Ejercicios.

1. La curva

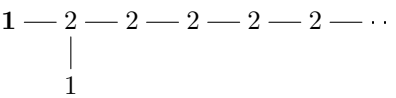
$$C_3 : y^2 + x^3 y = x^5 - 5x^3 - 10x^2 - 8x - 2 \tag{17.19}$$

tiene conductor $40000 = 2^6 5^4$ y está en la LMFDB. ¿Su punto móduli (g_1, g_2, g_3) vive en la subvariedad $X_{1+2\mathbb{Z}^2}$ de (17.8)?.

2. La LMFDB reporta que el grupo de Sato-Tate ST de (17.19) es $J(C_4)$. Tiene dimensión uno y grupo componente $C_2 \times C_4$. Más aún, la componente que contiene 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 $Sp^\natural_{2g}$. (El soporte consiste en 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 (17.7) para obtener una curva C_4. El discriminante de C_4 debería ser el número grande $\Delta = 2056589122535424 = 2^{16} 3^{22}$. ¿Por qué es `LocalData:=[<2,10,1>,<3,0,(1+T^2)^2>]` la información local correcta? Verifica que C_4 pasa `CFENew` a treinta decimales. (Fíjate que esta curva tiene grupo de Sato-Tate $C_{2,1}$ y ningún ejemplo de este grupo existe actualmente en la LMFDB. Pon atención también que hay un salto grande del gran discriminante Δ al pequeño conductor $N = 1024$.)
4. Consideremos la curva C_5 dada por $y^2 = x^6 - 1$. ¿Cuál es su discriminante? ¿Es isomorfo a C_4? ¿Parece su Jacobiana ser isógena a la Jacobiana de C_4?
5. Los momentos de $\tilde{S}_4$ se calculan por el diagrama extendido de Dynkin de tipo $\tilde{E}_7$:



A saber, m_k es el número de paseos de longitud k que empiezan y terminan al punto **1**. Verifica que los valores dados en (17.17) sean correctos. Repítelo para $G_2 = O_2$ y el diagrama extendido de Dynkin de tipo $\tilde{D}_\infty$:



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

Referencias

[1] C. Birkenhake y H. Lange, *Complex Abelian varieties*. Springer-Verlag, second edition, 2004.
[2] G. Cornell y J. H. Silverman (ed.), *Arithmetic Geometry*. Springer-Verlag, 1986.
[3] O. Debarre, *Tores et variétés abéliennes complexes*. EDP Sciences, 1999.
[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] G. R. Kempf, *Complex abelian varieties and theta functions*. Universitext, Springer-Verlag, Berlin, 1991.
[9] J. Milne, *Abelian varieties*. In [2], 103–150.
[10] J. Milne, *Jacobian varieties*. In [2], 167–212.
[11] 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.
[12] D. Mumford, *Abelian varieties*. Oxford U. Press, 1970.
[13] D. Mumford, *Curves and Jacobians*. Univ. of Michigan, 1975.
[14] M. Rosen, *Abelian varieties over* $\mathbb{C}$. In [2], 76–102.
[15] J. Silverman, *Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
[16] J. Silverman, *Advanced Topics on the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.
[17] H. P. F. Swinnerton-Dyer, *Analytic theory of abelian varieties*. London Mathematical Society Lecture Note Series, No. 14. Cambridge University Press, London-New York, 1974.

REFERENCIAS MÁS ESPECIALIZADAS

[18] The LMFDB Collaboration – *The L-function and Modular Forms Data Base*, `http://www.lmfdb.org`, 2013.
[19] *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.
[20] 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.
[21] 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.
[22] J.E. Cremona, *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 1997.
[23] 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.
[24] 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.
[25] T. Dokchitser, *Computing special values of motivic L-functions* Experiment. Math. **13**, no. 2, 137–149 (2004).
[26] T. Dokchitser and C. Doris, *3-torsion and conductor of genus 2 curves*. Arxiv 1706.06162 (2018).
[27] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73**, 349–366 (1983). DOI 10.1007/BF01388432.
[28] 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.
[29] B.H. Gross, D.B. Zagier, *On singular moduli*. J. Reine Angew. Math. **355**, 191–220 (1985).
[30] T. Honda, *Isogeny classes of abelian varieties over finite fields*. J. Math. Soc. Japan **20**, 83–95 (1968). DOI 10.2969/jmsj/02010083.
[31] J-I. Igusa, *Arithmetic variety of moduli for genus two*. Ann. of Math. **72** (1960) 612–649.
[32] 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.
[33] 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.
[34] 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.
[35] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**, 259–331 (1972). DOI 10.1007/BF01405086.

[36] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*. Annals of Math. **88**, 492–517 (1968).
[37] J. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2**, 134–144 (1966). DOI 10.1007/BF01404549.
[38] W.C. Waterhouse, *Abelian varieties over finite fields*. Ann. Sci. École Norm. Sup. (4) **2**, 521–560 (1969).
[39] A. Wiles, *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) **141**, no. 3, 443–551 (1995).
[40] Yu. G. Zarhin, *A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction*. Invent. Math. **79** (1985), 309–321.

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

Université Clermont Auvergne, France
Email address: marusia.rebolledo@uca.fr

University of Minnesota, Morris, Minnesota 56267, USA
Email address: roberts@morris.umn.edu