El método de Dem'janenko-Manin

José Cuevas Barrientos

Resumen. En ésta charla, veremos la prueba del teorema de Dem'janenko-Manin, una aplicación de Manin a curvas modulares y se mencionará una generalización en forma del teorema de especialización de Silverman.

1. Preliminares

1.1. Homomorfismos entre curvas elípticas. Para la aplicación de Manin, será necesario los siguientes resultados elementales:

Lema 1.1.A: Sean $E_1\colon y^2 = f_1(x)$ y $E_2\colon y^2 = f_2(x)$ un par de curvas elípticas sobre un cuerpo k. Toda isogenia $\alpha\colon E_1 \to E_2$ se puede escribir en *forma estándar*

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

donde $u, v, s, t \in k[x]$ son polinomios y los pares (u,v) y (s,t) son coprimos.

Demostración: Escribamos

$$\alpha(x,y) = \big(r_1(x,y), r_2(x,y)\big),$$

donde $r_1, r_2 \in k(x,y)$ son funciones racionales. Escribamos $r_1(x,y) = A(x,y)/B(x,y)$, donde $A, B \in k[x,y]$ son polinomios coprimos; empleando reiteradas veces que $y^2 = f_1(x)$, podemos escribir

$$r_1(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{1}$$

Ahora bien, como α es una isogenia, entonces para $P \in E_1(k^{\mathrm{alg}})$ tenemos que $\alpha(-P) = -\alpha(P)$, así que, comparando coordenadas, vemos que $r_1(x,-y) = r_1(x,y)$, es decir, r_1 es una función par en la variable y, por lo que $p_2(x) = p_4(x) = 0$.

Similarmente, $r_2(x,-y) = -r_2(x,y)$, por lo que r_2 es impar en la variable y, así que si escribimos r_2 en la forma (1), tendremos que $p_1(x) = p_3(x) = 0$, como se quería probar. □

Proposición 1.1: Sea k un cuerpo, sea E una curva elíptica sobre k y sean $\alpha, \beta \in \operatorname{End}_k(E)$ un par de (k-)endomorfismos. Sea $m := \max\{\deg\alpha, \deg\beta\}$ y supongamos que α y β coinciden en $\geq 4m+2$ puntos fuera de $\ker\alpha \cap \ker\beta$. Entonces $\alpha = \beta$.

Fecha: 29 de noviembre de 2024.

Demostración: Tras escoger una ecuación de Weierstrass para E, escribamos

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y \right)$$

en forma estándar, donde $u(x), v(x) \in k[x]$ son coprimos y $v(x)$ es mónico.

Como la función $P \mapsto x(P)$ tiene grado 2, vemos que conocemos el valor de $u(x)/v(x)$ en $\geq 2\deg\alpha + 1$ puntos. Supongamos que $u_1(x), v_1(x)$ fuesen otro par de polinomios coprimos de grado $\leq \deg\alpha$ cuyas evaluaciones coincidan, entonces $u(x)v_1(x) - u_1(x)v(x)$ sería un polinomio de grado $\leq 2\deg\alpha$ con $\geq 2\deg\alpha + 1$ raíces; así que u, v están únicamente determinados y, por tanto, la coordenada x de α lo está.

Aplicando el mismo argumento para β, concluimos que $\alpha(P) = \pm\beta(P)$ para todo $P \in E(k^{\mathrm{alg}})$. Ergo, $\alpha + \beta$ o $\alpha - \beta$ es un endomorfismo con núcleo infinito, es decir, $\alpha = \pm\beta$. Finalmente, sean $P_1, \dots, P_n$ con $n \geq 4m + 2$ los puntos distintos fuera de los núcleos en donde α y β coinciden. Como $n > 4m \geq 4$, vemos que es imposible que $\alpha(P_j) \in E[2](k^{\mathrm{alg}})$ para todo j, por lo que $\alpha(P_j) \neq -\alpha(P_j)$ para algún j y, por tanto, $\alpha = \beta$. □

1.2. La traza (de variedades abelianas) y el teorema de Lang-Néron. Para las demostraciones recomendamos el libro clásico de Lang **[3]**. Otra exposición en lenguaje esquemático es la de Conrad **[2]**.

Definición 1.2 (Chow): Sea K/k una extensión *primaria* de cuerpos (i.e., tal que la extensión $K \cap k^{\mathrm{alg}}/k$ sea puramente inseparable), y sea A_K una variedad abeliana sobre la extensión K. Se dice que una variedad abeliana B_k sobre el cuerpo base k, junto con un K-homomorfismo $\tau\colon B_K := B_k \times_k \operatorname{Spec} K \to A_K$ es la ***K/k-traza*** de A si posee la siguiente propiedad universal: para toda variedad abeliana B'_k sobre k con un K-homomorfismo $\varphi\colon B'_K \to A_K$, existe un único k-homomorfismo $\tilde{\varphi}\colon B'_k \to B_k$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} & B'_K \arrow[dl, dashed, "\exists!\tilde{\varphi}_K"'] \arrow[d, "\varphi"] \\ B_K \arrow[r, "\tau"] & A_K. \end{tikzcd}$$

Es claro que, si existe la traza, es única (salvo k-isomorfismo) y Chow probó que en efecto:

Proposición 1.3: Sea K/k una extensión primaria, y sea A una variedad abeliana sobre K. Entonces existe la K/k-traza de A y se denota por $\operatorname{Tr}_{K/k}(A)$.

La principal aplicación de la traza es el siguiente resultado. Para el enunciado, recuerde que una extensión de cuerpos K/k se dice ***regular*** si es puramente transcendente (i.e., si $K \cap k^{\mathrm{alg}} = k$) y es separable (i.e., posee una base de transcendencia $\Gamma \subseteq K$ tal que la extensión algebraica $K/k(\Gamma)$ es separable).

Teorema 1.4 (Lang-Néron): Sea K/k una extensión regular finitamente generada de cuerpos y sea A una variedad abeliana sobre K. Entonces, el grupo cociente $A(K)/\operatorname{Tr}_{K/k}(A)(k)$ es finitamente generado.

Corolario 1.4.1 (tesis de Néron): Sea K un cuerpo finitamente generado (sobre su cuerpo primo) y sea A una variedad abeliana sobre K. Entonces el grupo $A(K)$ es finitamente generado.

Demostración: Basta recordar que la traza será una variedad abeliana sobre el cuerpo primo k, en el cual $\operatorname{Tr}_{K/k}(A)(k)$ será finitamente generado por el teorema de Mordell-Weil; así concluimos tras aplicar el teorema de Lang-Néron. □

2. El teorema de Dem'janenko-Manin

Lema 2.1.A: Sean A, B un par de variedades abelianas sobre un cuerpo global K y sea $D \in \operatorname{Pic} B$ un divisor muy amplio y simétrico. La aplicación

$$H := \operatorname{Hom}_K(A, B) \longrightarrow \mathbb{Z}, \qquad \psi \longmapsto \deg \psi^* D \tag{2}$$

es cuadrática y se extiende en $H_{\mathbb{R}} := H \otimes_{\mathbb{Z}} \mathbb{R}$ a una forma cuadrática definida positiva.

Demostración: Basta notar que la función (2) es cuadrática por el teorema del cuadrado sumado al hecho de que D es simétrico. Además, en H toma valores estrictamente positivos, luego es claro que en $H_{\mathbb{R}}$ se extiende a una forma definida positiva. □

También será necesario el siguiente lema de álgebra (bi)lineal:

Lema 2.1.B: Sean E_1, E_2 un par de $\mathbb{R}$-espacios de producto interno, sea $\Lambda \leq E_1$ un reticulado (i.e., un $\mathbb{Z}$-submódulo de $\operatorname{rang}_{\mathbb{Z}} \Lambda = \dim_{\mathbb{R}} E_1$) y sean $\{\varphi_i : E_1 \to E_2\}_{i=1}^{\infty}$ una sucesión de aplicaciones lineales tales que para todo $f, g \in \Lambda$ con $f \neq 0$ se cumpla que

$$\lim_n \frac{|\varphi_n(g)|}{|\varphi_n(f)|} = \frac{|g|}{|f|}.$$

Entonces φ_n es inyectivo para n suficientemente grande.

Demostración: Fijemos $f \in \Lambda$ no nulo; por hipótesis $\varphi_n(f) \neq 0$ para n suficientemente grande y podemos multiplicarlos por un escalar de modo que $|\varphi_n(f)| = |f|$. Así, por hipótesis, para todo $g \in \Lambda$ se tiene que $\lim_n |\varphi_n(g)| = |g|$. En particular, aplicándolo para $g := a + b$, donde $a, b \in \Lambda$ son elementos cualesquiera, y despejando, obtenemos que

$$\lim_n \varphi_n(a) \cdot \varphi_n(b) = a \cdot b.$$

Finalmente, sea $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_m)$ una $\mathbb{Z}$-base ordenada de Λ, se comprueba entonces que

$$\lim_n \det[\varphi_n(\boldsymbol{e}_i) \cdot \varphi_n(\boldsymbol{e}_j)]_{i,j} = \det[\boldsymbol{e}_i \cdot \boldsymbol{e}_j]_{ij} \neq 0,$$

de modo que $\det[\varphi_n(\boldsymbol{e}_i) \cdot \varphi_n(\boldsymbol{e}_j)]_{i,j}$ es no nulo para n suficientemente grande y, por tanto, $\varphi_n(\boldsymbol{e}_1), \dots, \varphi_n(\boldsymbol{e}_m)$ son $\mathbb{R}$-linealmente independientes. □

En el siguiente teorema, diremos que un conjunto de morfismos $f_1, \dots, f_m : X \to G$ hacia un grupo algebraico conmutativo son *independientes* si $\sum_{j=1}^m a_j f_j = 0$ (como morfismos) para $a_j \in \mathbb{Z}$ solo cuando cada $a_j = 0$.

Teorema 2.1 (Dem'janenko-Manin): Sea X una curva proyectiva, geométricamente irreducible y suave sobre un cuerpo numérico K. Sea $P_0 \in X(K)$ un punto racional y sean $f_1, \dots, f_m \colon X \to A_K$ un conjunto de K-morfismos hacia una variedad abeliana A tales que $f_1(P_0) = \cdots = f_m(P_0) = 0$. Si $f_1, \dots, f_m$ son independientes, entonces para todos salvo finitos $P \in X(K)$ se cumple que $f_1(P), \dots, f_m(P) \in A(K)$ son $\mathbb{Z}$-linealmente independientes.

Demostración: Sea $H := \operatorname{Hom}_K(\operatorname{Jac} X, A)$ el grupo de homomorfismos de variedades abelianas sobre K. Mediante el morfismo de Abel-Jacobi con centro $P_0 \in X(K)$, se verifica que H está en biyección con los K-morfismos $f \colon X \to A$ tales que $f(P_0) = 0$. Como cada $\varphi \in H$ manda puntos racionales en puntos racionales, los cuales en ambos casos son grupos abelianos finitamente generados, se verifica que $H \cong \mathbb{Z}^r$ para algún $r \geq m$ (¿por qué es libre de torsión?). Definamos $H_{\mathbb{R}} := H \otimes_{\mathbb{Z}} \mathbb{R}$. Mediante el morfismo de Abel-Jacobi identificamos f_j con $\tilde{f}_j \in H \subseteq H_{\mathbb{R}}$.

Elijamos un encaje cerrado $X \hookrightarrow \mathbb{P}^N_K$ correspondiente a una clase $C \in \operatorname{Pic} X$, y sea $D \in \operatorname{Pic} A$ una clase de un divisor muy amplio simétrico, correspondiente a un encaje $g \colon A \hookrightarrow \mathbb{P}^M_K$. Por el lema 2.1.A, vemos que $|\psi|^2 := \deg(\psi^* D)$ determina una forma cuadrática sobre $H_{\mathbb{R}}$, mientras que D determina la forma cuadrática $|a|^2 := \hat{h}_{A,D}(a)$ para $a \in A(K)$ y, por tanto, una forma cuadrática sobre $V_{\mathbb{R}} := A(K) \otimes_{\mathbb{Z}} \mathbb{R}$ por cambio de base.

Más aún, para cada $P \in X(K)$, tenemos el homomorfismo de evaluación $\operatorname{ev}_P \colon H \to A(K)$ el cual, mediante cambio de base, se extiende a un homomorfismo $\Phi_P \colon H_{\mathbb{R}} \to V_{\mathbb{R}}$. Supongamos ahora, por contradicción, que existen infinitos puntos $\{P_n\}_{n=1}^{\infty} \subseteq X(K)$, entonces tenemos una sucesión de homomorfismos $\Phi_n := \Phi_{P_n}$.

Como $\operatorname{NS}(X) = 1$, entonces $C \in \operatorname{Pic} X$ conforma una $\mathbb{Q}$-base de $\operatorname{NS}(X) \otimes \mathbb{Q} \cong \mathbb{Q}$, de modo que

$$\forall f \in H \qquad f^* D \equiv \lambda(f) C \pmod{\operatorname{Pic}^0(X) \otimes \mathbb{Q}}$$

para algún $\lambda(f) \in \mathbb{Q}$. En particular, tomando deg a ambos lados con $d := \deg C$ se tiene que

$$\lambda(f) = \frac{1}{d} \deg(f^* D) = \frac{1}{d} |f|^2.$$

Luego, para $P \in X(K)$ se sigue que

$$\begin{aligned} |f(P)|^2 = \widehat{h}_{A,D}(f(P)) &= h_{X, f^* D}(P) + O_f(1) \\ &= \frac{1}{d} |f|^2 h(P) + O_f(1) + o(h(P)), \end{aligned}$$

donde $h(P) := h_{X,C}(P)$. Finalmente, como la sucesión $\{P_n\}_{n \in \mathbb{N}}$ es infinita y de puntos racionales, necesariamente $h(P_n) \to \infty$ por el teorema de Northcott, de modo que se confirma que

$$\lim_n \frac{|f(P_n)|^2}{h(P_n)} = \frac{1}{d} |f|^2,$$

por lo que se concluye por el lema 2.1.B. $\square$

Observación 2.1.1: Uno puede relajar X a suponer que es una variedad proyectiva, geométricamente irreducible y suave con $\operatorname{rang} \operatorname{NS}(X) = 1$; en cuyo caso, lo único que cambia en la demostración es usar la variedad Albanese $\operatorname{Alb}(X)$ en lugar del jacobiano $\operatorname{Jac}(X)$. Vid. **[10]**.

Como consecuencia, tenemos lo siguiente:

Corolario 2.1.2: Sea X una variedad proyectiva, geométricamente irreducible y suave sobre un cuerpo numérico K con $\operatorname{rang} \operatorname{NS}(X) = 1$. Si existe una variedad abeliana A sobre K y K-morfismos $f_1, \dots, f_m \colon X \to A$ independientes con $m > \operatorname{rang} A(K)$, entonces $X(K)$ posee finitos puntos racionales.

Corolario 2.1.3: Sea X una variedad proyectiva, geométricamente irreducible y suave sobre un cuerpo numérico K con $\operatorname{rang} \operatorname{NS}(X) = 1$. Si existe una variedad abeliana A tal que $\operatorname{rang} \operatorname{Hom}_K(C, A) > \operatorname{rang} A(K)$, entonces $X(K)$ posee finitos puntos racionales.

3. Aplicaciones: torsión de curvas elípticas

La siguiente aplicación es de Manin.

Teorema 3.1: Sea K un cuerpo numérico y sea p un número primo. Existe un natural $n = n(p, K) \geq 1$ tal que $X_0(p^m)$ solo tiene finitos puntos K-racionales para $m \geq n$.

Demostración: Sea n_p el mínimo entero tal que la curva modular $X_0(p^{n_p})$ tenga género $p_g \geq 1$, y sea $A := \operatorname{Jac}(X_0(p^{n_p}))$ su variedad jacobiana. Para cualesquiera enteros $m \geq n$ tenemos los morfismos algebraicos

$$f_i \colon X_0(p^m) \longrightarrow X_0(p^n), \qquad (0 \leq i \leq m - n)$$

dado sobre puntos complejos por mandar $[z] \mapsto [p^i z]$. Así, para $m \geq n_p$, sean $f_i \colon X_0(p^m) \to X_0(p^{n_p})$ susodichos morfismos y sea $j \colon X_0(p^{n_p}) \hookrightarrow A$ el morfismo de Abel-Jacobi con centro en la cúspide $[\infty]$.

Sea $\omega \in H^0(A, \Omega^1_{A/\mathbb{C}})$ una forma diferencial de A invariante por traslaciones, entonces veremos que las formas dadas por *pullbacks* $f_i^* j^* \omega$ son $\mathbb{C}$-linealmente independientes. Para ello, expandamos en términos de la variable $q = e^{2\pi \mathrm{i} z}$:

$$j^*\omega = cq^N \,\mathrm{d}q + \cdots, \qquad c \neq 0,$$

(esta expansión de Fourier o bien puede verla como una expansión de Taylor en la cúspide, o bien puede verla por la identificación entre formas cuspidales de peso 2 y diferenciales holomorfos.) Como f_i transforma q en q^{p^i}, tenemos que

$$f_i^* j^* \omega = c(q^{p^i})^N \,\mathrm{d}(q^{p^i}) + \cdots = c p^i q^{N p^i + (p^i - 1)} \,\mathrm{d}q + \cdots$$

y como los órdenes de $f_i^*\omega$ en q son distintos (por tanto, su orden de anulamiento en $[\infty] \in X_0(p^m)$ lo es), vemos que necesariamente los $f_i^*\omega$ son $\mathbb{C}$-linealmente independientes.

Así pues, los morfismos f_i son independientes. Para $m \geq n_p + \operatorname{rang} A(K)$ (donde $\operatorname{rang} A(K)$ es finito por el teorema de Mordell-Weil), vemos que hay $m - n_p + 1 > \operatorname{rang} A(K)$ morfismos independientes, así que aplicamos el teorema de Dem'janenko-Manin. $\square$

Observación 3.1.1: En la demostración, hemos visto que $m \geq n_p$, donde n_p es el mínimo tal que $p_g(X_0(p^{n_p})) \geq 1$. Podemos calcular explícitamente el valor de

n_p:

p	2	3	5	7	11	13	17	$\cdots$
n_p	5	3	3	2	1	2	1	$\cdots$
p^{n_p}	32	27	125	49	11	169	17	$\cdots$

Y en particular, podemos ver que $p^{n_p} \geq 11$.

Corolario 3.1.2: Sea K un cuerpo numérico y sea p un número primo. Existe un natural $m = m(p, K) \geq 1$ tal que toda curva elíptica E sobre K no posee puntos K-racionales de torsión de periodo p^m.

Demostración: Esto se sigue de la interpretación de $X_0(N)$ como espacio de *moduli* (vid. §1.1 y §1.3 de Rohrlich [**8**]): los puntos K-racionales de $Y_0(N)$ están en correspondencia con clases de K^{alg}-isomorfismo $(E, \mathcal{C})$, donde E es una curva elíptica sobre K y $\mathcal{C} \leq E[N](\mathbb{C})$ es un subgrupo de torsión cíclico de orden N, llamado el *distinguido*, el cual es $\mathrm{Gal}(K^{\mathrm{alg}}/K)$-estable (aquí, los isomorfismos mandan el subgrupo distinguido en el otro).

Sean (E_1, P_1) y (E_2, P_2) dos pares en la misma clase de equivalencia, es decir, E_1, E_2 son curvas elípticas sobre K con un punto $P_i \in E_i(K)$ de periodo p^m, y con un K^{alg}-isomorfismo que manda P_1 en P_2. Esto es lo mismo que tener un K^{alg}-automorfismo σ de una curva E que fija a un punto $P \in E(K)$ de periodo p^m; luego σ y Id_E son isogenias de grado 1 que coinciden en $p^m \geq 6$ puntos, por lo que son iguales (Prop. 1.1). Así que si $[E_1, \mathcal{C}_1] = [E_2, \mathcal{C}_2]$, escogiendo el generador apropiado, vemos que hay un único K^{alg}-isomorfismo φ entre ellos. Para cada $\sigma \in \mathrm{Gal}(K^{\mathrm{alg}}/K)$, vemos que necesariamente $\varphi^\sigma = \varphi$, por lo que φ es un K-isomorfismo.

En conclusión, hay a lo sumo finitas curvas elípticas sobre K con un punto K-racional de periodo p^m, para algún $m \gg 0$. Agrandando un poco el m, podemos asegurar que ninguna curva elíptica sobre K posea un punto de periodo p^m. □

Esto conlleva a la siguiente pregunta de Ogg: ¿para un cuerpo numérico K, cuántas posibilidades para la torsión de las curvas elípticas sobre K? Como el subgrupo de torsión de una curva elíptica es un grupo abeliano finito, uno puede emplear el teorema de clasificación para verificar que hay finitos grupos si y solo si la cardinalidad de la torsión está acotada. En efecto:

Teorema 3.2 (Merel [7], 1996): Sea K un cuerpo numérico. Existe un entero $N = N(K) > 1$ tal que para toda curva elíptica E sobre K, se cumple que $|E(K)_{\mathrm{tors}}| \leq N$.

Para $\mathbb{Q}$, Beppo Levi en 1908 había conjeturado *cuáles* grupos eran exactamente aquellos de torsión. Esto fue reconjeturado por Nagell y Ogg, y probado por Mazur:

Teorema 3.3 (B. Mazur [5] y [6], 1978): Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces su grupo de torsión $E(\mathbb{Q})_{\mathrm{tors}}$ es uno de los siguientes:

$$C_m \quad (1 \leq m \leq 10 \text{ o } m = 12), \qquad C_2 \times C_{2v} \quad (1 \leq v \leq 4).$$

Además, B. Levi ya conocía familias explícitas de curvas elípticas donde cada grupo de la lista anterior aparecía.

Las demostraciones de ambos teoremas pasan por la relación entre modularidad y variedades abelianas, y requieren de un preliminares no triviales sobre formas modulares. Más precisamente, Mazur prueba que los puntos $\mathbb{Q}$-racionales de las curvas modulares $X_1(p)$ para $p \geq 11$ son solo las cúspides.

4. El teorema de especialización de Silverman

En **[11],** Silverman dio una generalización al método de Dem'janenko-Manin. Antes de presentar el enunciado vamos a indicar exactamente cuál es la innovación de Silverman en su artículo: en el teorema de Dem'janenko-Manin, *a priori*, la curva X y la variedad abeliana A no están demasiado relacionadas entre sí; la situación para Silverman consiste en pensar que tienes una variedad que es (genéricamente) abeliana $\mathcal{A}$ relativa a otro esquema algebraico S sobre un cuerpo k (éste a su vez, no requiere ser un cuerpo numérico). Dado un punto S-valuado $P \in \mathcal{A}(S)$, podemos pensar que, sobre cada $s \in S$ hay un $P_s \in \mathcal{A}_s$, y la pregunta a tratar por Silverman está en cómo varían las alturas al verlos en esta familia.

Ahora formalizaremos los resultados:

Definición 4.1: Un ***cuerpo semiglobal*** es un par (K, M_K), donde K es un cuerpo y M_K es un conjunto no vacío de valores absolutos no triviales tales que:

CSG1. Para todo $\alpha \in K^\times$ se cumple que $|\alpha|_v = 1$ para todos salvo finitos lugares $v \in M_K$.

CSG2. Todo $\alpha \in K^\times$ satisface la ***fórmula del producto***:

$$\prod_{v \in M_K} |\alpha|_v = 1.$$

De no haber ambigüedad obviaremos el conjunto M_K.

Por ejemplo, $\mathbb{Q}$ junto a los valores absolutos $|\,|_\infty$ y $|\,|_p$ para todo primo p conforma un cuerpo semiglobal. Más generalmente, dado un esquema X regular en codimensión 1, siempre podemos formar un cuerpo semiglobal $K(X)$.

Situación 4.2: Sea k un cuerpo semiglobal, sean $\mathcal{A}, S$ un par de variedades proyectivas suaves sobre k, denotemos por $\xi \in S$ al punto genérico, y sea $\pi\colon \mathcal{A} \to S$ un k-morfismo plano cuya fibra genérica $\mathcal{A}_\xi$ es una variedad abeliana sobre $\Bbbk(\xi) = K(S)$. Vamos a denotar por S^0 el conjunto de puntos esquemáticos $s \in S$ tales que la fibra $\mathcal{A}_s$ sea una variedad abeliana (sobre $\Bbbk(s)$).

Sea $s \in S^0(k^{\mathrm{alg}})$, entonces s es de buena reducción para $\mathcal{A}_{K(S)}$ y, por la propiedad de los modelos de Néron, se tiene la siguiente ***función de especialización***:

$$\sigma_s\colon \mathcal{A}(K(S)) \xrightarrow{\ \sim\ } \mathcal{A}(\mathscr{O}_{S,s}) \longrightarrow \mathcal{A}_s(k^{\mathrm{alg}}).$$

Teorema 4.3: En la situación 4.2 supongamos que $\mathrm{NS}(S)$ es cíclico. Sea $P \in \mathcal{A}(S)$ una sección o punto valuado tal que $n \cdot P \in \mathcal{A}(S)$ también sea una sección para n suficientemente grande. Dado $D \in \operatorname{Pic} \mathcal{A}$ sea $h_{\mathcal{A}_\xi, D_\xi}$ la altura en $\mathcal{A}_\xi\big(K(S)^{\mathrm{alg}}\big)$, entonces

$$\lim_{\substack{h(s)\to\infty \\ s\in S^0(k^{\mathrm{alg}})}} \frac{h_{\mathcal{A}_s,D_s}(P(s))}{h_S(s)} = h_{\mathcal{A}_\xi,D_\xi}(P(\xi)).$$

Teorema 4.4 (especialización de Silverman, 1982): En la situación 4.2, supongamos que $\mathrm{NS}(S)$ es cíclico y que toda sección racional es un morfismo. Sea $\Gamma \leq \mathcal{A}_\xi(K(S))$ un subgrupo finitamente generado con $\Gamma \cap \mathrm{Tr}_{K(S)/K}\,\mathcal{A}_\xi(K) = 0$. Entonces el conjunto de $s \in S^0(k^{\mathrm{alg}})$ tales que la función de especialización σ_s no es inyectiva en Γ tiene altura acotada. En particular, si k es un cuerpo global, existen (solo) finitos puntos cerrados $s \in S^0$ de grado acotado tales que σ_s no es inyectivo en Γ.

Asumiendo el teorema anterior, podemos probar nuevamente el teorema de Dem'janenko-Manin:

Demostración: Sea X una curva proyectiva y suave sobre K, y sea A una variedad abeliana sobre K. Consideramos $S = X$ y $\mathcal{A} := A \times_K X$, en donde, en este caso, $\mathcal{A}_s = A$ para todo punto K-racional, $S^0 = X$ y $\mathcal{A}_\xi = A_{K(X)}$ es el cambio de base; en particular

$$\mathrm{Tr}_{K(X)/K}\, A_{K(X)} = A_K.$$

Así $\Gamma \leq A(K(X))$ es un subgrupo finitamente generado de secciones $X \to \mathcal{A} = A \times_K X$ y la condición de que $\Gamma \cap A(K) = 0$ equivale a exigir que Γ esté generado por finitos morfismos $\mathbb{Z}$-linealmente independientes.

Como Γ consiste de morfismos independientes, la especialización σ_x en un $x \in X(\mathbb{Q}^{\mathrm{alg}})$ corresponde a la evaluación, los cuales darán puntos distintos salvo en finitos valores de x. Así, si X tuviese infinitos puntos K-racionales, para infinitos de ellos σ_x sería inyectiva, lo cual es absurdo. □

Comentarios sobre la literatura

En éste artículo hemos optado por la simple definición de un *cuerpo semiglobal*, pero está tratada en mayor detalle y con otros nombres en el resto de la literatura técnica. Por ejemplo, Gubler les llama *M-cuerpos*, mientras que Yaakov y Hrushovski les llaman *cuerpos globalmente valuados*. La noción más general, sin embargo, es la de *curvas adélicas* en §3.1 de Chen y Moriwaki **[1]**.

La demostración del método de Dem'janenko-Manin aquí expuesta es la que aparece en §5.2 del libro de Serre **[10]**, mientras que en §12.2 de Lang **[4]** aparece la generalización mediante el teorema de Silverman. Para probar el teorema de especialización de Silverman hacen falta varios resultados, algunos bastante importantes, como una cota de Silverman-Tate para la variación de la altura de una sección $P \in \mathcal{A}(S)$ entre sus especializaciones y una comprensión de alturas sobre cuerpos de funciones.

Se puede leer acerca del trabajo de B. Levi en la conjetura de Ogg en el artículo expositivo **[9]**.

Referencias

1. Chen, H. y Moriwaki, A. *Arakelov Geometry over Adelic Curves Lecture Notes in Mathematics* **2258** (Springer-Verlag, 2020).

2. Conrad, B. Chow's K/k-image and K/k-trace and the Lang-Néron theorem. *L'enseignement math.* **52,** 37-108. doi:10.5169/seals-2226 (2006).
3. Lang, S. *Abelian Varieties* (Interscience, 1959).
4. Lang, S. *Fundamentals of Diophantine Geometry* (Springer-Verlag, 1983).
5. Mazur, B. Modular curves and the Eisenstein ideal. *Publ. Math. IHÉS* **47,** 33-186. http://www.numdam.org/item/PMIHES_1977__47__33_0/ (1977).
6. Mazur, B. Rational Isogenies of Prime Degree. *Invent. math.* **44,** 129-162. doi:10.1007/BF01390348 (1978).
7. Merel, L. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. math.* **124,** 437-449. doi:10.1007/s002220050059 (1996).
8. Rohrlich, D. E. *Modular Curves, Hecke Correspondences, and L-functions* en *Modular Forms and Fermat's Last Theorem* (eds. Cornell, G., Silverman, J. H. y Stevens, G.) (Springer-Verlag, 2000), 41-100.
9. Schappacher, N. y Schoof, R. Beppo Levi and the Arithmetic of Elliptic Curves. *The Mathematical Intelligencer* **18,** 57-69. doi:10.1007/bf03024818 (1996).
10. Serre, J.-P. *Lectures on the Mordell-Weil theorem* (Friedrick Vieweg & Son, 1997).
11. Silverman, J. H. Heights and the specialization map for families of abelian varieties. *J. reine angew. Math.* **342,** 197-211. doi:10.1515/crll.1983.342.197 (1982).

Correo electrónico: josecuevasbtos@uc.cl
URL: josecuevas.xyz

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