# Teorema de Chabauty

Rocío Sepúlveda

## 1. Introducción

Trabajaremos sobre el campo $\mathbb{Q}$. Las curvas se asumirán suaves, proyectivas y geometricamente integrales.

Sea $X$ una curva sobre $\mathbb{Q}$ de género $\geq 2$. La Conjetura de Mordell [**5**] nos dice que $X(\mathbb{Q})$ es finito y éste fue demostrado en 1983 por G. Faltings [**3**]. Sin embargo, Chabauty en 1941 inspirado por una idea análoga de T. Skolem [**6**] en el contexto de puntos enteros sobre subvariedades de un tori, tuvo la idea de usar $\mathbb{Q}_p$ para un primo fijo $p$ en vez de $\mathbb{R}$ que ya revisamos que falla con la charla anterior de Matías Alvarado (se terminaba deduciendo que $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ posee una vecindad de algún punto conocido en $X(\mathbb{R})$, así que es infinito).

> Si tenemos tiempo aparte de revisar el trabajo de Chabauty, podemos ver lo interés de su teorema: Coleman en 1985 [**2**] encontró gracias al trabajo de Chabauty una cota para la cantidad de puntos $\mathbb{Q}$ racionales de la cuva $X$. Es interesante ya que la demostración de Faltings no es efectiva, la demostración no entrega un algoritmo para poder encontrar los puntos $X(\mathbb{Q})$, sin embargo, existe el método Chabauty-Coleman que permite calcularlo en algunas curvas de manera individual.

## 2. Preliminares

**2.1. Álgebras de Lie** Recordemos de la charla anterior que un grupo de Lie $p$-ádico es un grupo dotado con estructura de *Manifold* analítico $p$-ádico son la multiplicación y el inverso son analíticos.

En el apunte realizado por Matías Alvarado se realiza la construcción de un álgebra de Lie a partir de un Grupo de Lie, éste se realiza restringiendo el espacio de campos vectoriales $\mathfrak{X}(G)$ a sólo los campos vectoriales invariantes por la izquierda y considerando un isomorfismo como grupos entre $T_e(G)$ y $\mathfrak{X}(G)^{\text{inv}}$, y al espacio tangente $T_e(G)$ se le dota por un operador llamado *conmutador* y éste se le denomina al álgebra de Lie $G$ denotado por $\text{Lie}(G)$.

**2.2. El Jacobiano** Sea $J$ el Jacobiano de $X$. Este es una variedad abeliana de dimensión $g$ sobre $\mathbb{Q}$. Supongamos que conocemos un punto $O \in X(\mathbb{Q})$.

Entonces tenemos el encaje

$$\iota\colon X \to J, P \mapsto [P - O], \tag{2.1}$$

donde $[D]$ denota la clase de equivalencia de un divisor $D$. Así, podemos identificar $X$ con su imagen:

$$X \subset J, \qquad X(\mathbb{Q}) = X \cap J(\mathbb{Q}).$$

Esto es extra :
La estrategia para determinar $X(\mathbb{Q})$ es

1. Primero calcular $J(\mathbb{Q})$.
2. Luego determinar cuales puntos en $J(\mathbb{Q})$ están en $X$.

Aunque $J(\mathbb{Q})$ no es necesariamente finito, el Teorema de Mordell-Weil dice que $J(\mathbb{Q})$ es un grupo abeliano finitamente generado así que, *a priori*, puede ser descrito dando los generadores explícitamente (representados por sus divisores) y sus relaciones. «Calcular $J(\mathbb{Q})$» significa calcular los generadores y las relaciones.

*Observación* 1. De aquí en adelante, asumiremos que $J(\mathbb{Q})$ ha sido calculado.

**2.3. Estructura de** $J(\mathbb{Q}_p)$ Algunos hechos de esta parte están en citar [**1,** III §7.6.], o bien, en los apuntes de Matías Alvarado.

Para otorgarle de estructura a la variedad Jacobiana, se hace notar que como es variedad algebraica está definida localmente como ceros de polinomios y se utiliza el Teorema de la Función Implícita en su versión no arquimediana. Para ver que el Jacobiano es un grupo de Lie necesitamos ver que el mapeo multiplicación y mapeo inversa son analíticos. En esto estoy con dudas, pero creo que lo intuitivo es que, para la inversa, es usar el hecho de que es un isomorfismo.

Recordemos de la charla pasada en que el profesor Pastén dio un ejemplo básico del mapeo logaritmo $\mathrm{Log} : \mathbb{G}_m \to \mathbb{Q}_p$, $z \mapsto \int_0^z \frac{dt}{t}$. Queremos generalizar eso

**Teorema 1:** *Si $\iota\colon X \to J$ es la incrustación de $X$ en su Jacobiana, entonces $\iota^*\colon H^0(J, \Omega^1_J) \to H^0(X, \Omega^1_X)$*

*Demostración.* Ver Prop. III.2.2 en [**4**]. □

Así podemos deducir que la dimensión del Jacobiano es igual al género de la curva $X$.

Sea $J_{\mathbb{Q}_p}$ una variedad definida por las mismas ecuaciones de $J$, pero considerándolo sobre $\mathbb{Q}_p$ en vez de $\mathbb{Q}$. Sea $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ el espacio vectorial de 1-formas regulares de dimensión $g$ sobre $\mathbb{Q}_p$ en $J_{\mathbb{Q}_p}$.

Suponga que $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Se puede definir

$$\eta_J : J(\mathbb{Q}_p) \to \mathbb{Q}_p, \qquad Q \mapsto \int_0^Q \omega_J$$

Luego se obtiene la siguiente aplicación bilineal

$$J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) \to \mathbb{Q}_p, \qquad (Q, \omega_J) \mapsto \int_0^Q \omega_J.$$

Esta induce un homomorfismo $\log\colon J(\mathbb{Q}_p) \to H^(J, \Omega^1)^{dual}$. Y log es un difeomorfismo local.

**Lema 2:** *Si $\omega \neq 0$ es una forma diferencial del primer tipo sobre $J$, entonces la restricción de $\omega$ en la curva $X$ es $\neq 0$.*

**Teorema 3 (Chabauty):** *Sea $X$ una curva de género $g \geq 2$ sobre $\mathbb{Q}$. Sea $J$ el Jacobiano de $X$. Sea $p$ un primo. Si $\operatorname{rang} J(\mathbb{Q}) < g$. Entonces $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ es finito (por tanto, lo es $X(\mathbb{Q})$).*

*Demostración.* Note que $J(\mathbb{Q}_p)$ es un grupo de Lie $p$-ádico compacto sobre $\mathbb{Q}_p$ de dimensión $g = \dim J$. Como el grupo es localmente isomorfo a su álgebra de Lie, existe un abierto $U$ de $J(\mathbb{Q}_p)$ isomorfo, como un grupo de Lie, a $O_{\mathbb{Q}_p} \times \ldots \times O_{\mathbb{Q}_p}$ ($g$ factores), donde $O_{\mathbb{Q}_p}$ es el anillo de enteros de $\mathbb{Q}_p$.

Ahora, veremos que $C \cap \overline{J(\mathbb{Q})}$ es finito. Supongamos por contradicción que es infinito. Como $J(\mathbb{Q}_p)$ es compacto, podemos considerar una sucesión de puntos $P_i$ distintos de $X \cap \overline{J(\mathbb{Q})}$, tal que $P_i \to P_0$ donde $P_0 \in X \cap \overline{J(\mathbb{Q})}$.

Podemos asumir que $P_0 = 0$, por traslación, y que los $P_i$'s están en el subgrupo abierto $U$ elegido antes, y que $J \cap U$ es libre de rango $g' < g$. Cambiando coordenadas, entonces todos los elementos $(x_1, \ldots, x_d) \in U \cap \overline{J(\mathbb{Q})}$ cumplen $x_i = 0$. Por tanto, la curva $X$ intersecta el hiperplano $x_1 = 0$ en infinitos puntos en el espacio $g$ dimensional. Es decir, $x_1$ es una función sobre la curva con infinitos ceros $x_1(P_i) = 0$, las cuales se acumulan en 0. El principio de los ceros aislados para funciones analíticas $p$-ádicas nos dice que $x_1 = 0$ en una vecindad de 0 en $X$.

Sea $\omega_1, \ldots \omega_d$ una base de formas diferenciales (holomorfas) correspontiendtes al sistema de coordenadas $x_1, \ldots x_g$, $dx_i = \omega_i$ en una vecindad de 0. La forma diferencial $\omega_1$ restringida en $X$ tiene a lo más $2g - 2$ ceros, por tanto, $\omega_1 \mid_C = 0$, el cual contradice el lema 2. □

## Referencias

1. Bourbaki, N. *Lie Groups and Lie Algebras. Chapters 1–3* (Springer Berlin, Heidelberg, 1998).
2. Coleman, R. F. Effective Chabauty. *Duke Mathematical Journal* **52,** 765-770. doi:10.1215/S0012-7094-85-05240-8 (1985).

3. Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones mathematicae* **73,** 349-366 (1983).
4. Milne, J. S. *Abelian Varieties (v2.00)* Available at www.jmilne.org/math/. 2008.
5. Mordell, L. J. *On the rational resolutions of the indeterminate equations of the third and fourth degree* en *Proc. Cambridge Phil. Soc.* **21** (1922), 179-192.
6. Skolem, T. Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen. *Fundamenta Mathematicae* **23,** 150-161 (1934).