HACIA EL TEOREMA DE CHABAUTY

El propósito de estas notas es presentar algunos preliminares para estudiar el teorema de Chabauty [Cha41]. Partiremos presentando una idea que es la base del teorema, para luego dar pie al estudio de manifolds analitícos y grupos de Lie p-ádicos. En la siguiente sesión demostraremos el teorema siguiendo la exposisición en [SBW89]

A lo largo de estas notas X denotará una curva algebraica proyectiva suave de género g definida sobre $\mathbb{Q}$, y J_X denota su variedad jacobiana.

1. Una idea para abordar la conjetura de Mordell

Supongamos que $X(\mathbb{Q})$ es no vacío. Entonces tomando un punto racional podemos fijar una incrustación $X \hookrightarrow J_X$. El conjunto de puntos $\mathbb{R}$-racionales $J_X(\mathbb{R})$ tiene estructura de manifold real. Mas aún de grupo de Lie real. Sea $\overline{J_X(\mathbb{Q})}$ la clausura de $J_X(\mathbb{Q})$ en $J_X(\mathbb{R})$. Observamos que $X(\mathbb{Q}) \subset X(\mathbb{R}) \cap \overline{J_X(\mathbb{Q})}$. Si $X(\mathbb{R}) \cap \overline{J_X(\mathbb{Q})}$ fuese finito, entonces concluiríamos la finitud de $X(\mathbb{Q})$. El problema es que $\overline{J(\mathbb{Q})}$ podría ser abierto en $J_X(\mathbb{R})$. De hecho se conjetura que si J_X es simple y $J_X(\mathbb{Q})$ es Zariski denso en J_X, entonces $\overline{J_X(\mathbb{Q})}$ es abierto en $J_X(\mathbb{R})$. Ver por ejemplo Conjecture 5 en [Maz92].

Como esto parece no funcionar, lo volvemos a intentar, pero ahora dentro de los punto p-ádicos de la variedad jacobiana.

2. Números p-ádicos

Recordemos que los números reales se construyen como la completación de $\mathbb{Q}$ con respecto al valor absoluto usual. Del mismo modo, si completamos $\mathbb{Q}$ respecto a otros valores absolutos, obtenemos otros campos de mucho interés aritmético.

Para cada número primo p, definimos la valuación p-ádica v_p, que a cada número racional $x = p^n \dfrac{a}{b}$ (con $p \nmid a, b$) le asigna $v_p(x) = n$. La función v_p se denomina *valuación p-ádica*, y ella es una valuación en el sentido de álgebra conmutativa.

La norma p-ádica se define como

$$\begin{aligned} |\cdot|_p \colon \mathbb{Q} &\longrightarrow \mathbb{R} \\ x &\longmapsto p^{-v_p(x)}. \end{aligned}$$

$|\cdot|_p$ es una norma que cumple la desigualdad triangular fuerte, es decir $|a+b|_p \leq \max\{|a|_p, |b|_p\}$. Una norma que satisfaga esta propiedad se conoce como una ultramétrica.

Definition 1. *Definimos los números p-ádicos como la completación de $\mathbb{Q}$ respecto de la norma p-ádica $|\cdot|_p$. Esta completación es de hecho un campo y es una extensión infinita no algebraica de $\mathbb{Q}$.*

Si $x \in \mathbb{Q}_p$, entonces x puede escribirse como

$$x = \sum_{n \geq n_0} a_n p^n,$$

donde n_0 es un número entero y los coeficientes a_n pertenecen a $\{0, ..., p-1\}$.

Date: November 10, 2024.

La bola unitaria en $\mathbb{Q}_p$ se puede caracterizar como los elementos que se escriben como $\sum_{n\geq 0} a_n p^n$. A esta bola se le denomina como $\mathbb{Z}_p$, la cual (gracias a la propiedad ultramétrica) es de hecho un anillo.

Lo que haremos ahora es estudiar la estructura *analítica* de los puntos $\mathbb{Q}_p$-racionales de J_X para usar la estrategia de la sección 1 con $J_X(\mathbb{Q}_p)$.

3. Manifolds analíticos p-ádicos y grupos de Lie

Usaremos la nomeclatura inglesa "manifold" para referirnos a las variedades analíticas y así evitar confusiones con las variedad algebraicas. Consideremos el espacio vectorial $\mathbb{Q}_p^n$ dotado de la norma del supremo $||(x_1, ..., x_n)|| = \max\{|x_1|_p, ..., |x_n|_p\}$.

Primero definiremos la funciones que nos darán la estructura en los manifold

Definition 2. *Sea $U \subset \mathbb{Q}_p^n$, una función $f\colon U \to \mathbb{Q}_p^m$ es analítica si es dada localmente por series de potencias convergentes al rededor de cada punto $x \in U$*

$$f(y) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha y^\alpha, \text{ para todo } y \in B_{\mathbb{Q}_p^n}(x, r)$$

donde $a_\alpha \in \mathbb{Q}_p^n$, $r > 0$ tal que $B_{\mathbb{Q}_p^n}(x, r) \subset U$ y

$$\sum_{\alpha\in\mathbb{N}^n} ||a_\alpha|| r^{|\alpha|} < \infty$$

Antes de dar la definicion de manifolds analíticos debemos hablar de cartas y atlas. Dado un espacio topológico Hausdorff M, definimos una carta de M como una tripleta ordenada $(U, \phi, \mathbb{Q}_p^n)$, que consiste de un subconjunto abierto $U \subset M$ y una función $U \to \mathbb{Q}_p^n$ tal que

(a) $\phi(U)$ es un abierto en $\mathbb{Q}_p^n$
(b) $\phi\colon U \to \phi(U)$ es un homeomorfismo.

Además diremos que dos cartas $(U_1, \phi_1, \mathbb{Q}_p^{n_1})$ y $(U_2, \phi_2, \mathbb{Q}_p^{n_2})$ de M son compatibles si las funciones

$$\phi_1(U_1 \cap U_2) \xrightarrow{\phi_2\circ\phi_1^{-1}} \phi_2(U_1 \cap U_2) \text{ y } \phi_2(U_1 \cap U_2) \xrightarrow{\phi_1\circ\phi_2^{-1}} \phi_1(U_1 \cap U_2)$$

son analíticas.

Un atlas para M es un conjunto de $\mathcal{A} = \{(U_i, \phi_i, K^{n_i})\}_{i\in I}$ de cartas para M tal que son 2 a 2 compatibles. Además $\{U_i\}$ es un cubrimiento de M. Si todas las cartas de dimensión n, diremos que el atlas es de dimensión n.

Definition 3 (Manifolds analíticos)**.** *Un manifold analítico $(M, \mathcal{A})$ definido sobre $\mathbb{Q}_p$ es un espacio topologico Hausdorff M junto a un atlas maximal $\mathcal{A}$. Por simplificación diremos que todas las cartas tienen la misma dimensión.*

Definition 4 (Funciones entre manifolds)**.** *Sean M, N manifolds analíticos p-ádicos. Una función $f\colon M \to N$ es analítica si para punto $x \in M$ existen cartas $(U, \phi, \mathbb{Q}_p^n)$ que contiene a x y $(V, \psi, \mathbb{Q}_p^m)$ que contiene a $f(x)$, con $f(U) \subset V$ y tal que la composición $\psi \circ f \circ \phi^{-1}$ es analítica de $\phi(U)$ en $\psi(V)$.*

Al conjunto de funciones analíticas de M en $\mathbb{Q}_p$ lo denotamos por $A(M)$.

Una exposición detalla sobre manifold analíticos p-ádicos puede encontrarse en el capitulo II de [Sch11].

3.1. **Grupos y Álgebras de Lie.** Partiremos dando las definiciones de un Grupo de Lie analítico p-ádico y la definición general de un álgebra de Lie. Luego veremos brevemente cual es la relación entre estas dos estructuras.

Definition 5. *Un grupo de Lie p-ádico es un grupo $(G, \cdot)$ dotado de una estructura de manifold analítico p-ádico tal que la función multiplicación del grupo $\cdot\colon G \times G \to G$ y la función tomar inverso en el grupo $()^{-1}\colon G \to G$ son analíticas*

Ahora veremos la definición de un álgebra de Lie, que a priori nada tiene que ver con grupos de Lie.

Definition 6. *Un álgebra de Lie sobre un campo F, es un espacio vectorial $\mathfrak{g}$ sobre F junto con una operación binaria $[\cdot,\cdot]\colon \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ que satisface:*

- *Bilinealidad*
- $[x, x] = 0$ *para todo* $x \in \mathfrak{g}$.
- $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ *para todo* $x, y, z \in \mathfrak{g}$.

Remark 3.1.

- La función $[\cdot,\cdot]$ se conoce como el corchete de Lie.
- La tercera propiedad de $[\cdot,\cdot]$ se conoce como la propiedad de Jacobi.
- Las álgebras de Lie se suelen denotar usando la fuente matemática *mathfrak.* $\mathfrak{g}, \mathfrak{h}, \mathfrak{k}$, *etc.*

A cada Grupo de Lie se le puede asignar un álgebra de Lie. Eso es lo que exploraremos ahora. Como la construcción del álgebra de Lie a partir de un grupo de Lie puede ser un poco confusa, explicaremos con palabras sencillas que es, antes de ver la construcción. En pocas palabras el álgebra de Lie de un grupo G es el espacio tangente de G en el neutro, dotado de un corchete de Lie $[\cdot,\cdot]$, que viene de los campos vectoriales. A continuación precisaremos esto, pero a grandes rasgos uno podría pensarlo así.

Sea G un grupo de Lie p-ádico. Recordemos que una derivación de $A(G)$ en un punto $p \in G$ es una función lineal v_p de $A(G)$ en $\mathbb{Q}_p$, tal que para $f, g \in A(G)$, $v_p(fg) = v_p(f)g(p) + v_p(g)f(p)$ (esta es la regla de Leibnitz). El espacio tangente de G en p (que denotaremos por T_pG) puede ser definido como el espacio de todas las derivaciones de $A(G)$ en p.

Por otro lado un campo vectorial de G es una función lineal $x\colon A(G) \to A(G)$ tal que $x(fg) = fx(g) + x(f)g$, para todo $f, g \in A(G)$ (regla de Leibnitz nuevamente). Al espacio de campos vectoriales lo denotamos por $\mathfrak{X}(G)$.

Dado dos campos vectoriales v, w, entonces podemos tomar la composición $v \circ w\colon A(M) \to A(M)$, la cual sigue siendo una función lineal, pero no es un campo vectorial. Falla la propiedad del producto (Leibnitz). para obtener nuevamente un campo vectorial lo que hacemos es tomar el *conmutador*, es decir, $[v, w] = v \circ w - w \circ v$. El conmutador sí es un campo vectorial. El espacio vectorial $\mathfrak{X}(G)$ dotado con el conmutador forman un álgebra de Lie. Pero esta no es el álgebra de Lie del grupo G, pues $\mathfrak{X}(G)$ es de dimensión infinita y nosotros queremos un álgebra cuya dimensión coincida con la dimensión analítica del grupo G. Lo que uno hace es tomar un subespacio de $\mathfrak{X}(G)$ que sí sea finito dimensional. Este subespacio es el de los campos vectoriales invariantes por izquierda y lo denotaremos por $\mathfrak{X}(G)^{inv}$.

Vamos a definir entonces este subespacio. Primero vemos que dado un isomofismo analítico $f\colon G \to G$, existe una función inducida a nivel de campos vectoriales (el push-forward) $f_*\colon \mathfrak{X}(G) \to \mathfrak{X}(G)$. Como f_*v es un campo vectorial, esta es una función de $A(G)$ en $A(G)$ y está definida de forma tal que $(f_*v)(g)(p) = v_{f^{-1}(p)}(g \circ f)$.

En particular podemos tomar el isomorfismo f como traslación por izquierda por un elemento x del grupo. A esta traslación la llamaremos L_x. Un campo vectorial invariante por izquierda (es decir un elemento en $\mathfrak{X}(G)^{inv}$) es aquel que satisface $(L_x)_*v = v$ para todo $x \in G$.

$\mathfrak{X}(G)^{inv}$ es un subespacio vectorial de $\mathfrak{X}(G)$, y además $[\mathfrak{X}(G)^{inv}, \mathfrak{X}(G)^{inv}] \subset \mathfrak{X}(G)^{inv}$.

Ahora queremos llegar a la conclusión que mencionamos al principio, es decir, que el álgebra de Lie se puede entender con el espacio tangente en la identidad. Primero observamos que dado la función $L_x : G \to G$, tenemos asociado la función a nivel de espacios tangentes $(dL_x)\colon T_e(G) \to T_x(G)$, dado por $v \mapsto (dL_x)_e(v)$. Así podemos construir el isomorfismo de grupos $T_e(G) \to \mathfrak{X}(G)^{inv}$ tal que $v \mapsto v^L$, donde $v^L_x = (dL_x)_e(v)$.

De este modo $T_e(G)$ hereda el corchete de Lie del conmutador de $\mathfrak{X}(G)^{inv}$, y este se denomina el algebra de Lie G. En adelante, en estas notas denotaremos a esta álgebra por Lie(G).

Ahora que ya hemos definido grupos de Lie, veamos la estructura de la variedad Jacobiana. Al ser una variedad algebraica, esta está definida localmente como cero de polinomios (los cuales son analíticos). Para obtener las cartas lo que hacemos es usar la versión no arquimediana del teorema de la función implicita (ver capitulo 2 de [Igu00]). El cual nos dirá que cierta cantidad de variables se pueden escribir en función de las otras. Al ser J_X una variedad algebraica suave, esta satisface el criterio de suavidad del jacobiano (el de la matriz con las derivadas parciales formales), el cual es precisamente la hipótesis del teorema de la función implicita. Este argumento es el mismo que se usa para ver que los conjuntos de nivel de funciones suaves definen manifolds reales. Además las funciones suma en la jacobiana y tomar inverso son algebraicas, es decir que vienen dada por expresiones polinomiales, las cuales también son analíticas.

4. Función exponencial y logaritmo

En esta sección definiremos dos funciones importantes en la teoría de grupos de Lie p-ádicos, la función exponencial y la función logaritmo. La referencia que se siguió para esta sección es el libro de Bourbaki [Bou89]

Primero haremos las construcciones teóricas y luego veremos algunos ejemplos. revisaremos el *logarítmo p-ádico* el cual se estudia en análisis p-ádico, y luego veremos el logaritmo en variedades Jacobianas.

Theorem 4.1 (exponencial)**.** *Sea G un grupo de Lie. Existe una* función exponencial exp *con las siguientes propiedades.*

(i) *Existe abierto U del grupo aditivo T_eG, tal que* $\exp\colon U \to G$ *está bien definida*
(ii) $\exp(U)$ *es abierto en G y* exp *es un isomorfismo de manifolds analíticos entre U y* $\exp(U)$.
(iii) $\exp(nx) = \exp(x)^n$ *para todo $x \in U$ y todo $n \in \mathbb{Z}$.*

Esbozo de demostración: Se dota a Lie(G) con una norma $||\cdot||$ y denotamos por G_1 el grupo de Lie definido por Lie(G). La función $\psi = id_{G_1}$ es una función exponencial de G_1. Sea $\mu \in \mathbb{R}$. Definimos $L_\mu = \{x \in Lie(G) : ||x|| < \mu\}$. Para μ suficientemente pequeño L_μ es un subgrupo del grupo aditivo Lie(G), entonces $\psi(L_\mu)$ es un subgrupo abierto de Lie(G). $\psi|_{L_\mu}$ es un isomorfismo de manifolds analitícos de L_μ en $\psi(L_\mu)$. además $\psi(nx) = \psi(x)^n$, para todo $x \in L_\mu$ y para todo $n \in \mathbb{Z}$.

L_μ forma un sistema de vecindades del 0 de Lie(G), por lo tanto existen subgrupos un subgrupo G' de G tal que $\psi(L_\mu)$ y G' son isomorfos. □

Remark 4.2. Lo que está detrás del último argumento es que grupos de Lie con álgebra de Lie isomorfas son localmente isomorfos.

Example 1 (Funcion exponencial p-adica)**.** *Consideremos la función definida por la serie de potencias*

$$\sum_{n\geq 0} \frac{x^n}{n!}$$

Esta función está definida en su disco de convegencia $B^{\mathbb{Q}_p}_{p^{-1/(p-1)}}(0)$. *Entonces la función exponencial es una función definida del abierto* $B^{\mathbb{Q}_p}_{p^{-1/(p-1)}}(0)$ *en* $\mathbb{Q}_p^\times$. *En el lenguaje de grupos de Lie, la exponencial p-adica es la exponencial del grupo multiplicativo* $\mathbb{Q}_p^\times$.

Antes de verificar la existencia de una función logaritmo, necesitamos la definición de un conjunto..

Sea G_f el conjunto de elementos $x \in G$ para los cuales existe una sucesión estrictamente creciente (n_i) de enteros tal que x^{n_i} tiende a e cuando $n_i \to \infty$. Este conjunto es un abierto no vacío de G, por Lemma 1 en sección 6 (Logarithmic mapping) en [Bou89].

Theorem 4.3 (Logaritmo)**.** *Existe una función* $\psi\colon G_f \to \mathrm{Lie}(G)$ *con las siguientes propiedades*

(a) $\psi(x^n) = n\psi(x)$ *para todo* $x \in G_f$ *y todo* $n \in \mathbb{Z}$.
(b) *Existe una vecindad* V *de* e *en* G *tal que* $\psi|_V$ *es la inversa de la función exponencial.*
(c) *La función* ψ *es analitica.*

Esbozo de demostración. Sea U un abierto de $\mathrm{Lie}(G)$ y $\phi\colon U \to \phi(U)$ la funcion exponencial. Podemos tomar U suficientemente pequeño tal que $\phi(U) \subset G_f$. Para $x \in G_f$, existe m tal que $x^m \in \phi(U)$. Verifiquemos que el elemento $\frac{1}{m}\phi^{-1}(x^m)$ no depende de la eleccion de m.

Supongamos que $x^{mn} \in \phi(U)$, entonces

$$n\phi^{-1}(x^m) = \phi^{-1}(x^{mn}) = m\phi^{-1}(n),$$

Entonces definimos $\psi(x) = \frac{1}{m}\phi^{-1}(x^m)$. Ademas $\psi|_{\phi(U)} = \phi^{-1}$.

Corroboramos además,

$$\psi(x^n) = \frac{1}{m}\phi^{-1}(x^{nm}) = \frac{n}{m}\phi^{-1}(x^m) = n\psi(x).$$

El hecho que la función sea analítica es por ser composición de $x \mapsto x^m$, $y \mapsto \phi^{-1}(y)$,$z \mapsto \frac{1}{m}z$. □

Proposition 4.4. *Si* G *es compacto, entonces* $G_f = G$

Proof. Sea $x \in G$, V vecindad de e en G. Entonces $x^n \to y$. Existen n_1, n_2 tal que $n_1 \geq 2n_2 \geq n$, con $x^{n_1} \in yV$ y $x^{n_2} \in yV$. Entonces $x^{n_1-n_2} \in V^{-1}\cdot V$ y además $n_1 - n_2 \geq n$. Por lo que concluimos que $x \in G_f$. □

4.1. **Diferenciales en la variedad jacobiana y logaritmo.** Empezamos recordando un teorema sobre la geometría de las variedades abelianas

Theorem 4.5. *Si* $\iota\colon X \to J_X$ *es la incrustación de* X *en su Jacobiana. entonces* $\iota^*\colon H^0(J_X, \Omega^1_{J_X}) \to H^0(X, \Omega^1_X)$ *es un isomorfismo.*

Proof. Ver por ejemplo Proposition 2.2 en [Mil86] □

Del teorema podemos concluir que la dimension de J_X es igual al género de la curva X.

Tomemos $\omega \in H^0(J_X, \Omega^1_{J_x})$, entonces podemos definir la función

$$\begin{aligned} \eta_w\colon J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ q &\mapsto \int_0^q w, \end{aligned}$$

Donde el valor $\int_0^q w$ significa tomar una antiderivada formal del diferencial w y luego evaluar en los extremos de intgración.

De esta forma podemos construir una aplicación bilineal

$$J_X(\mathbb{Q}_p) \times H^0(J_X, \Omega^1) \to \mathbb{Q}_p$$
$$(q, w) \mapsto \int_0^q w,$$

Esta aplacación induce un homomorfismo $J_X(\mathbb{Q}_p) \to H^0(J_X, \Omega^1_{J_X})^\vee$. Esta es una forma de construir el logaritmo usando integrales. Una descripción mas detallada puede encontrarse en la sección 4 de [MP12]

References

[Bou89] Nicolas Bourbaki, *Lie groups and lie algebras: Chapters 1-3*, vol. 1, Springer Science & Business Media, 1989.

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algebriques de genre superieura l'unite*, CR Acad. Sci. Paris **212** (1941), no. 882-885, 1.

[Igu00] Jun-ichi Igusa, *An introduction to the theory of local zeta functions*, vol. 14, American Mathematical Soc., 2000.

[Maz92] Barry Mazur, *The topology of rational points*, Experimental Mathematics **1** (1992), no. 1, 35–45.

[Mil86] James S Milne, *Jacobian varieties*, Arithmetic geometry, Springer, 1986, pp. 167–212.

[MP12] William McCallum and Bjorn Poonen, *The method of chabauty and coleman*, Explicit methods in number theory **36** (2012), 99–117.

[SBW89] Jean-Pierre Serre, Martin Brown, and Michel Waldschmidt, *Lectures on the mordell-weil theorem*, Springer, 1989.

[Sch11] Peter Schneider, *p-adic lie groups*, vol. 344, Springer Science & Business Media, 2011.

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

Email address, M. Alvarado: mnalvarado1@uc.cl