El Principio Local-Global en Curvas Elípticas.

Adrián Camilo Cerda Morocho[1] and Luis Manuel Reyes de la Luz [2]

[1]Universidad San Francisco de Quito, Ecuador, acerdam@estud.usfq.edu.ec
[2]Instituto de Matemáticas, UNAM, México, luis.reyes@im.unam.mx

Julio 2026

Resumen

En Construcción

Índice

1. Introducción **2**

2. Herramientas sobre Geometría Algebraica y Geometría Arimética **2**
2.1. Preliminares de geometría algebraica . . . 2
2.1.1. El espectro de un anillo . . . 2
2.1.2. Esquemas . . . 3
2.1.3. Morfismos de esquemas . . . 4
2.1.4. Curvas algebraicas . . . 5
2.1.5. Divisores y divisores principales . . . 6
2.1.6. Funtores representables . . . 7
2.2. Preliminares de geometría aritmética . . . 9
2.2.1. Aritmética sobre los p-ádicos . . . 9
2.2.2. El Principio de Hasse. . . . 19

3. Fallo del Principio Local-Global **23**
3.1. La curva $3x^3 + 4y^3 + 5z^3 = 0$. . . . 23

4. Estudiando el fallo. **26**
4.1. Introducción a la cohomologia de Galois . . . 28
4.2. El Jacobiano de una curva. . . . 33

5. Grupos de Selmer y Tate-Shafarevich **35**
5.1. Obstrucciones locales-globales . . . 35
5.2. El caso de la curva de estudio . . . 36

6. Conclusión **38**

1. Introducción

Uno de los principios fundamentales que aparecen en el estudio de las ecuaciones diofánticas es el principio local-global, según el cual, bajo determinadas condiciones, la existencia de soluciones en todos los completamientos locales de un campo debería garantizar la existencia de una solución global. Esta idea establece una conexión particularmente profunda entre la aritmética local y la aritmética global, y constituye una herramienta poderosa para decidir la existencia de soluciones racionales.

Sin embargo, esta propiedad no es universal. Aunque el principio local-global funciona para importantes clases de ecuaciones, existen curvas para las cuales una ecuación admite puntos sobre todos los campos locales correspondientes y, sin embargo, no posee ningún punto racional. El ejemplo clásico de Selmer muestra precisamente este fenómeno y pone de manifiesto que la información local, por sí sola, no siempre es suficiente para recuperar la información global.

Esta situación motiva la búsqueda de herramientas que permitan estudiar y medir el fallo del principio local-global. En particular, para curvas elípticas y, más generalmente, para curvas mediante sus jacobianos, aparecen de manera natural los grupos de Selmer y el grupo de Tate–Shafarevich. Estos objetos permiten organizar la información proveniente de los puntos locales y compararla con la información global, proporcionando así un marco algebraico para entender por qué puede existir una obstrucción a la existencia de puntos racionales.

El objetivo de este trabajo es estudiar este fenómeno partiendo del principio local-global y de su fallo. Para ello, se introducen primero las herramientas necesarias de teoría de números y geometría algebraica, incluyendo los números p-ádicos, el lema de Hensel y los divisores sobre una curva. Posteriormente, se estudia el ejemplo de Selmer como un contraejemplo al principio local-global y, finalmente, se introducen los grupos de Selmer y de Tate–Shafarevich como herramientas destinadas a describir y estudiar sistemáticamente estas obstrucciones.

2. Herramientas sobre Geometría Algebraica y Geometría Arimética

2.1. Preliminares de geometría algebraica

2.1.1. El espectro de un anillo

Definición 2.1 — Espectro primo. Sea A un anillo conmutativo. El *espectro primo* de A se define como el conjunto

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p} \text{ es un ideal primo}\}.$$

Los elementos de $\mathrm{Spec}(A)$ se denominan los *puntos* del espectro de A.

El conjunto $\mathrm{Spec}(A)$ se dota de una estructura topológica mediante la topología de Zariski.

Definición 2.2 — Topología de Zariski. Sea A un anillo conmutativo. Para cada ideal $I \subseteq A$ definimos

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) : I \subseteq \mathfrak{p}\}.$$

Los conjuntos $V(I)$ forman los conjuntos cerrados de una topología sobre $\mathrm{Spec}(A)$, denominada la *topología de Zariski*.

Esta topología permite dotar al conjunto de ideales primos de una estructura geométrica.

Por ejemplo, para ideales $I, J \subseteq A$ se tiene

$$V(I) \cup V(J) = V(IJ) \quad \text{y} \quad V(I) \cap V(J) = V(I + J).$$

▪ **Ejemplo 2.1** Consideremos ahora el caso de un anillo de polinomios. Sea K un campo algebraicamente cerrado y tomemos

$$A = K[x].$$

Los ideales maximales de $K[x]$ son de la forma

$$(x - a), \qquad a \in K.$$

Por tanto, los puntos cerrados de $\mathrm{Spec}(K[x])$ pueden identificarse con los elementos de K. Sin embargo, también tenemos el ideal primo (0), que no es maximal. Así,

$$\mathrm{Spec}(K[x]) = \{(0)\} \cup \{(x - a) : a \in K\}.$$

De manera análoga, si

$$A = K[x_1, \ldots, x_n],$$

los ideales maximales

$$(x_1 - a_1, \ldots, x_n - a_n), \qquad (a_1, \ldots, a_n) \in K^n,$$

corresponden a los puntos de K^n. ▪

2.1.2. Esquemas

Para convertir $\mathrm{Spec}(A)$ en un objeto geométrico no basta considerar únicamente su estructura topológica. Es necesario dotarlo de un haz de anillos.

Definición 2.3 — Esquema afín. Sea A un anillo conmutativo. El *esquema afín* asociado a A es el espacio localmente anillado

$$\mathrm{Spec}(A) = \left(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)}\right),$$

donde $\mathcal{O}_{\mathrm{Spec}(A)}$ es el *haz estructural* de $\mathrm{Spec}(A)$.

Así, cuando escribimos $\mathrm{Spec}(A)$, entenderemos no solamente el conjunto de ideales primos, sino el esquema afín formado por dicho espacio junto con su haz estructural.

Los esquemas generales se obtienen pegando localmente esquemas afines.

Definición 2.4 — Esquema. Un *esquema* es un espacio localmente anillado $(X, \mathcal{O}_X)$ tal que para todo punto $x \in X$ existe un entorno abierto $U \subseteq X$ y un anillo conmutativo A para los cuales

$$(U, \mathcal{O}_X|_U) \cong \left(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)}\right)$$

como espacios localmente anillados.

En particular, todo esquema afín es un esquema. La importancia de esta definición radica en que permite estudiar objetos geométricos localmente mediante anillos.

▪ **Ejemplo 2.2** Si K es un campo y $f \in K[x,y]$, podemos considerar el anillo

$$A = K[x,y]/(f).$$

El esquema afín

$$\operatorname{Spec}\left(K[x,y]/(f)\right)$$

corresponde a la ecuación

$$f(x,y) = 0.$$

Si K es algebraicamente cerrado, los puntos cerrados de este esquema corresponden a los puntos de la curva afín definida por f. En particular, si

$$(a,b) \in K^2$$

satisface

$$f(a,b) = 0,$$

el punto correspondiente está dado por el ideal maximal

$$(x-a, y-b)/(f).$$

▪

2.1.3. Morfismos de esquemas

Para relacionar esquemas necesitamos una noción de morfismo que sea compatible tanto con su estructura topológica como con su estructura de anillos.

Definición 2.5 — Morfismo de esquemas. Sean $(X, \mathcal{O}_X)$ y $(Y, \mathcal{O}_Y)$ esquemas. Un *morfismo de esquemas*

$$f : X \longrightarrow Y$$

es un morfismo de espacios localmente anillados. Esto consiste en una aplicación continua

$$f : X \longrightarrow Y$$

junto con un morfismo de haces de anillos

$$f^\sharp : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X.$$

En el caso de esquemas afines, esta definición tiene una descripción algebraica particularmente sencilla.

Teorema 2.1 *Sean A y B anillos conmutativos. Existe una correspondencia biyectiva natural*

$$\operatorname{Hom}_{\mathrm{Sch}}\left(\operatorname{Spec}(A), \operatorname{Spec}(B)\right) \cong \operatorname{Hom}_{\mathrm{Ring}}(B, A).$$

Es decir, un homomorfismo de anillos

$$\varphi : B \longrightarrow A$$

induce un único morfismo de esquemas

$$\begin{array}{ccc} \operatorname{Spec}(A) & \longrightarrow & \operatorname{Spec}(B) \\ \mathfrak{p} & \longmapsto & \varphi^{-1}(\mathfrak{p}). \end{array}$$

La preimagen de un ideal primo mediante un homomorfismo de anillos es nuevamente un ideal primo, por lo que esta aplicación está bien definida.

Observamos que la dirección del morfismo de esquemas es opuesta a la dirección del homomorfismo de anillos:

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & A \\ \operatorname{Spec}(A) & \longrightarrow & \operatorname{Spec}(B). \end{array}$$

Esta inversión de la dirección se expresa diciendo que el funtor espectro es contravariante:

$$\operatorname{Spec} : \mathbf{Ring}^{\mathrm{op}} \longrightarrow \mathbf{Sch}.$$

Por ejemplo, consideremos el homomorfismo de K-álgebras

$$\varphi : K[x] \longrightarrow K[x, y], \qquad x \longmapsto x.$$

Este homomorfismo induce un morfismo de esquemas

$$\operatorname{Spec}(K[x, y]) \longrightarrow \operatorname{Spec}(K[x]).$$

Si K es algebraicamente cerrado, sobre los puntos cerrados podemos identificar este morfismo con la proyección

$$K^2 \longrightarrow K, \qquad (a, b) \longmapsto a.$$

2.1.4. Curvas algebraicas

Definición 2.6 — Curva algebraica. Sea K un campo. Una *curva algebraica* sobre K es un esquema C de tipo finito sobre K cuya dimensión es 1.

En el caso afín, si

$$C = \operatorname{Spec}(A),$$

decimos que C es una curva afín cuando A es una K-álgebra de tipo finito y

$$\dim(A) = 1.$$

Por ejemplo, si $f \in K[x, y]$ es un polinomio no constante e irreducible, podemos considerar

$$C = \operatorname{Spec}\left(K[x, y]/(f)\right).$$

Bajo las condiciones apropiadas, este esquema corresponde a la curva afín definida por

$$f(x, y) = 0.$$

Una curva puede ser también proyectiva. En este caso, la curva se obtiene como un esquema cerrado de un espacio proyectivo $\mathbb{P}^n_K$. Si está dada por ecuaciones homogéneas

$$f_1(X_0, \ldots, X_n) = \cdots = f_r(X_0, \ldots, X_n) = 0,$$

decimos que dichas ecuaciones definen una curva proyectiva.

Cuando K es un campo algebraicamente cerrado, los puntos cerrados de una curva afín pueden identificarse con las soluciones de sus ecuaciones en K. Sin embargo, trabajar con esquemas permite considerar también puntos definidos sobre extensiones de K y conservar información algebraica que no aparece únicamente al considerar los puntos clásicos.

En particular, si C es una curva sobre K y L/K es una extensión de campos, podemos considerar sus puntos definidos sobre L:

$$C(L) = \mathrm{Hom}_{K\text{-Sch}}\left(\mathrm{Spec}(L), C\right).$$

Cuando $L = K$, obtenemos el conjunto de puntos K-racionales

$$C(K).$$

2.1.5. Divisores y divisores principales

Sea C una curva algebraica suave sobre un campo K. Un divisor permite registrar formalmente los puntos de la curva junto con multiplicidades enteras.

Definición 2.7 — Divisor. Un *divisor* sobre C es una combinación formal finita

$$D = \sum_{P \in C} n_P P,$$

donde $n_P \in \mathbb{Z}$ y solamente un número finito de los coeficientes n_P son distintos de cero.

El conjunto de todos los divisores sobre C, con la suma término a término, forma un grupo abeliano que denotamos por

$$\mathrm{Div}(C).$$

El *grado* de un divisor se define como

$$\deg(D) = \sum_{P \in C} n_P.$$

En particular, los divisores de grado cero forman el subgrupo

$$\mathrm{Div}^0(C) \coloneqq \{D \in \mathrm{Div}(C) : \deg(D) = 0\}.$$

Para relacionar divisores con funciones racionales, consideremos el cuerpo de funciones racionales $K(C)$ de la curva C. Para cada punto $P \in C$ y cada función racional no nula $f \in K(C)^\times$, se define el *orden de f en P*, denotado por

$$\mathrm{ord}_P(f).$$

Este entero mide el orden de anulación o de polo de f en P. Si $\mathrm{ord}_P(f) > 0$, entonces P es un cero de f de orden $\mathrm{ord}_P(f)$, mientras que si $\mathrm{ord}_P(f) < 0$, se tiene que P es un polo de orden $-\mathrm{ord}_P(f)$.

Definición 2.8 — Divisor principal. Sea $f \in K(C)^\times$. El *divisor principal* asociado a f es el divisor

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f) P.$$

Los divisores que pueden escribirse de esta forma se denominan *divisores principales*.

Los divisores principales forman un subgrupo de $\operatorname{Div}(C)$, que denotamos por

$$\operatorname{Prin}(C).$$

Si C es una curva proyectiva y $f \in K(C)^\times$, se tiene la propiedad fundamental

$$\deg(\operatorname{div}(f)) = 0.$$

Es decir, en una curva proyectiva, una función racional tiene el mismo número total de ceros y polos, contando sus multiplicidades.

Definición 2.9 — Equivalencia lineal. Dos divisores $D_1, D_2 \in \operatorname{Div}(C)$ son *linealmente equivalentes*, y escribimos

$$D_1 \sim D_2,$$

si existe una función racional no nula $f \in K(C)^\times$ tal que

$$D_1 - D_2 = \operatorname{div}(f).$$

El cociente por los divisores principales conduce al grupo de Picard.

Definición 2.10 — Grupo de Picard. El *grupo de Picard* de C se define como

$$\operatorname{Pic}(C) = \frac{\operatorname{Div}(C)}{\operatorname{Prin}(C)}.$$

El subgrupo formado por las clases de divisores de grado cero se denota por

$$\operatorname{Pic}^0(C).$$

2.1.6. Funtores representables

Sea X un esquema. Para cada anillo conmutativo R, consideramos el conjunto de morfismos

$$X(R) = \operatorname{Hom}_{\mathrm{Sch}}\left(\operatorname{Spec}(R), X\right).$$

Este conjunto se denomina el conjunto de R-puntos de X. La construcción es functorial en R, pues todo homomorfismo de anillos

$$R \longrightarrow S$$

induce, por contravarianza del espectro, un morfismo

$$\operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R).$$

Por composición obtenemos una aplicación

$$X(R) \longrightarrow X(S).$$

De esta manera, cada esquema X determina un funtor

$$h_X : \mathbf{Ring} \longrightarrow \mathbf{Set},$$

dado por

$$h_X(R) = \mathrm{Hom}_{\mathrm{Sch}}\left(\mathrm{Spec}(R), X\right).$$

Definición 2.11 — Funtor representable. Sea

$$F : \mathbf{Ring} \longrightarrow \mathbf{Set}$$

un funtor. Decimos que F es *representable* si existe un esquema X y un isomorfismo natural de funtores

$$F \cong h_X.$$

En este caso, decimos que X *representa* al funtor F.

Un ejemplo sencillo se obtiene considerando el anillo

$$A = \mathbb{Z}/3\mathbb{Z}$$

y el esquema afín

$$X = \mathrm{Spec}(\mathbb{Z}/3\mathbb{Z}).$$

Para cualquier anillo conmutativo R, por la correspondencia entre morfismos de esquemas afines y homomorfismos de anillos tenemos

$$X(R) \cong \mathrm{Hom}_{\mathrm{Ring}}\left(\mathbb{Z}/3\mathbb{Z}, R\right).$$

Un homomorfismo de anillos

$$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow R$$

debe satisfacer $\varphi(\overline{1}) = 1_R$ y, por tanto,

$$0 = \varphi(\overline{3}) = 3 \cdot 1_R.$$

En consecuencia, existe un único homomorfismo de anillos

$$\mathbb{Z}/3\mathbb{Z} \longrightarrow R$$

si $3 \cdot 1_R = 0$, y no existe ninguno en caso contrario. Por tanto,

$$X(R) = \begin{cases} \{*\}, & \text{si } 3 \cdot 1_R = 0, \\ \varnothing, & \text{si } 3 \cdot 1_R \neq 0. \end{cases}$$

Así, el esquema

$$\mathrm{Spec}(\mathbb{Z}/3\mathbb{Z})$$

representa el funtor

$$R \longmapsto \mathrm{Hom}_{\mathrm{Ring}}\left(\mathbb{Z}/3\mathbb{Z}, R\right).$$

2.2. Preliminares de geometría aritmética

2.2.1. Aritmética sobre los p-ádicos

En esta sección fijemos p un número primo. Los números p-ádicos surgen de la misma necesidad de la existencia de los números reales, como la completación de $\mathbb{Q}$ bajo una valor absoluto.

Definición 2.12 — Valor absoluto. Sea K un campo, un valor absoluto es una función $|\cdot| : K \to \mathbb{R}^+$ tal que satisface las siguientes propiedades para toda $x, y \in K$:

1. $|x| = 0$ si y sólo si $x = 0$.
2. $|xy| = |x|\,|y|$.
3. $|x + y| \leq |x| + |y|$.

Además decimos que el valor absoluto es *no arquimediano* si se cumple para cada $x, y \in K$ que

$$|x + y| \leq \max\{|x|, |y|\}$$

Definición 2.13 — Norma n-ádica. Sea n un entero positivo, definimos la norma n-ádica como sigue, para cada $x \in \mathbb{Z}$:

$$|x|_n := \frac{1}{n^{\sup\{m \in \mathbb{Z}^+ |\ x = n^m h\}}}$$

Proposición 2.2 *Las siguientes afirmaciones son válidas para la norma n-ádica:*

1. $|x|_n = 0$ *si y sólo si* $x = 0$.
2. $|xy|_n \leq |x|_n\,|y|_n$.
3. $|x + y|_n \leq \max\{|x|_n, |y|_n\}$

Además la norma n-ádica es multiplicativa si y sólo si $n = p$ *es primo.*

Demostración.

1. Se tiene que $|x|_n = 0$ sí y solo sí $n^m | x$ para todo $m \geq 1$, y esto se cumple sí y solo sí $x = 0$.
2. Sean $a = v_n(x)$ y $b = v_n(y)$. Entonces $x = n^a u$ y $y^b v$, con u y v no divisibles para n. Luego, como $xy = n^{a+b}uv$, entonces $v_n(xy) \geq a + b$. Se sigue que

$$|xy|_n \leq \frac{1}{n^{a+b}} = |x|_n\,|y|_n$$

3. Con a y b como en el anterior literal, supongamos, sin pérdida de generalidad, que $a \leq b$. Entonces $n^a | x$ y $n^a | y$, por lo que $n^a | x + y$. Se cumple entonces que $v_n(x + y) \geq \min\{v_n(x), v_n(y)\}$, de lo que se sigue que $|x + y|_n \leq \max\{|x|_n, |y|_n\}$.
4. Tomando u y v como arriba. Se tiene que $|xy|_n = |x|_n\,|y|_n$ para todo x y y si y solo si n no divide a uv para todo u y v no divisibles para n, lo que se cumple si y solo si n es primo.

■

Definición 2.14 — Valor absoluto p-ádico. Sea p un primo, definimos el valor absoluto p-ádico

en $\mathbb{Q}$ como sigue:

$$\left|\frac{n}{m}\right|_p := \frac{|n|_p}{|m|_p}$$

Corolario 2.3 *La función $|\cdot|_p$ definida sobre $\mathbb{Q}$ es un valor absoluto no arquimediano.*

Demostración. Como p es primo, entonces

$$\begin{aligned}
\left|\frac{n}{m}+\frac{x}{y}\right|_p &= \left|\frac{ny+mx}{my}\right|_p \\
&= \frac{\left|ny+mx\right|_p}{\left|my\right|_p} \\
&\leq \frac{\max\{\left|ny\right|_p, |mx|_p\}}{\left|my\right|_p} \\
&= \frac{\max\{|n|_p\left|y\right|_p, |m|_p|x|_p\}}{|m|_p\left|y\right|_p} \\
&= \max\{\frac{|n|_p\left|y\right|_p}{|m|_p\left|y\right|_p}, \frac{|m|_p|x|_p}{|m|_p\left|y\right|_p}\} \\
&= \max\{\left|\frac{n}{m}\right|_p, \left|\frac{x}{y}\right|_p\}
\end{aligned}$$

■

■ **Ejemplo 2.3** Consideremos la sucesión $s_n := 1 + p + p^2 + \cdots + p^{n-1}$, notemos que se puede escribir como

$$s_n = \frac{1-p^n}{1-p}$$

sabemos que $\text{mcd}(p, p-1) = 1$ eso implica que $\left|p-1\right|_p = 1$. Luego notemos

$$\left|s_n - \frac{1}{1-p}\right|_p = \left|\frac{p^n}{1-p}\right|_p = \frac{\left|p^n\right|_p}{\left|1-p\right|_p} = \frac{1/p^n}{1} = 1/p^n$$

esto implica que

$$\lim_{n\to\infty}\sum_{k=0}^{n} p^k = \frac{1}{1-p}$$

en $(\mathbb{Q}, |\cdot|_p)$. Esto se puede generalizar si estudiamos la sucesión

$$p_n := \sum_{k=0}^{n} a^k p^k,\ a \in \mathbb{Z}$$

entonces

$$\lim_{n\to\infty}\sum_{k=0}^{n} a^k p^k = \frac{1}{1-ap}$$

en $(\mathbb{Q}, |\cdot|_p)$. ▪

▪ **Ejemplo 2.4** La interpretación de la valuación p-ádica, en contraste con la valuación euclidiana estándar, es del tipo aritmético. De hecho para todo $x, y \in \mathbb{Z} \subseteq \mathbb{Q}$ se cumple

$$\left|x-y\right|_p \leq \frac{1}{p^n} \iff x \cong y \mod p^n$$

obteniendo un puente entre técnicas del análisis y técnicas de la aritmética. Por ejemplo, consideremos $a \in \mathbb{Z} - \{0,1\}$ un entero coprimo con p y definamos la sucesión $s_n := a^{p^n}$, vamos a probar que esta sucesión es una *sucesión de Cauchy*. Observemos

$$\begin{aligned} |s_{n+1} - s_n|_p &= \left|a^{p^n}(a^{p^n(p-1)} - 1)\right|_p \\ &= \left|a^{p^n}\right|\left|a^{p^n(p-1)} - 1\right|_p \end{aligned}$$

Aquí entra en juego el teorema de Euler. Recordemos que la función indicatriz de Euler para p^{n+1} es $\phi(p^{n+1}) = p^n(p-1)$. Por el teorema de Euler (o elevando el Pequeño Teorema de Fermat):

$$a^{\phi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}$$

Sustituyendo el exponente, esto significa que $a^{p^n(p-1)} - 1$ es divisible por p^{n+1}. Por lo tanto, su norma p-ádica es:

$$|a^{p^n(p-1)} - 1|_p \leq p^{-(n+1)}$$

Como $|a^{p^n}|_p = 1$, la distancia entre términos consecutivos es:

$$|s_{n+1} - s_n|_p \leq p^{-(n+1)}$$

A medida que $n \to \infty$, la distancia tiende a 0. En valores absolutos no arquimedianos, que la diferencia entre términos consecutivos tienda a cero es condición necesaria y suficiente para que la sucesión entera sea de Cauchy. ▪

▪ **Ejemplo 2.5 — $(\mathbb{Q}, |\cdot|_p)$ no es completo.** Continuando con el ejemplo 2.4, tenemos que la sucesión $s_n = a^{p^n}$ es una sucesión de Cauchy. Vamos a probar que esta sucesión no converge. Supongamos por el contrario que si converge a un elemento $L \in \mathbb{Q}$, es decir

$$L = \lim_{n\to\infty} a^{p^n}$$

Si elevamos el límite a la potencia p:

$$L^p = \left(\lim_{n\to\infty} a^{p^n}\right)^p = \lim_{n\to\infty} a^{p^{n+1}} = L$$

Obtenemos la ecuación $L^p = L$, o equivalentemente:

$$L(L^{p-1} - 1) = 0$$

Como asumimos que $p \nmid a$, sabemos que $L \neq 0$. Por lo tanto, el límite debe satisfacer:

$$L^{p-1} = 1$$

Esto significa que el límite L debe ser una raíz $(p-1)$-ésima de la unidad. Pero, las únicas raíces de la unidad que existen dentro del campo de los números racionales $\mathbb{Q}$ son 1 y -1. Si eliges un primo $p > 3$ y un entero a tal que $a \not\equiv 1 \pmod{p}$ y $a \not\equiv -1 \pmod{p}$, la sucesión intentará converger a una raíz de la unidad que no existe en $\mathbb{Q}$. ∎

Del ejemplo anterior, necesitamos una noción de completación de campos.

Teorema 2.4 — Completación de campos. *Sea $(K, |\cdot|)$ un campo valuado. Entonces existe un campo valuado completo $(\widehat{K}, \widehat{|\cdot|})$ y un morfismo de campos contractivo*

$$j \colon (K, |\cdot|) \longrightarrow (\widehat{K}, \widehat{|\cdot|})$$

tal que, para cualquier campo valuado completo $(L, |\cdot|_L)$ y cualquier morfismo de campos contractivo $f \colon (K, |\cdot|) \longrightarrow (L, |\cdot|_L)$, existe un único morfismo de campos continuo $\widehat{f} \colon (\widehat{K}, \widehat{|\cdot|}) \longrightarrow (L, |\cdot|_L)$ que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} (K, |\cdot|) & \xrightarrow{\ j\ } & (\widehat{K}, \widehat{|\cdot|}) \\ & \searrow^{f} & \downarrow{\scriptstyle \exists! \widehat{f}} \\ & & (L, |\cdot|_L) \end{array}$$

es decir, $f = \widehat{f} \circ j$.

Además, j es una isometría (cumple que $\widehat{|j(x)|} = |x|$ para todo $x \in K$) y su imagen $j(K)$ es topológicamente densa en $\widehat{K}$.

Demostración. La norma induce una métrica $d \colon K^2 \longrightarrow \mathbb{R}$ dada por $d(x, y) = |x - y|$. Como todo espacio métrico posee una completación, entonces existe un espacio $(\widehat{K}, \widehat{d})$ y una isometría $j \colon K \longrightarrow \widehat{K}$ cuya imagen es densa en $\widehat{K}$. Una construcción concreta del espacio $(\widehat{K}, \widehat{d})$ consiste en tomar las series de Cauchy en K e identificarlas si su diferencia converge a 0. La isometría (y por tanto función contractiva) j es dada por $j(a) = [(a, a, a, \cdots)]$, con $a \in K$. La métrica $\widehat{d}$ es inducida por la valuación $\widehat{|\cdot|} \colon \widehat{K} \longrightarrow \mathbb{R}^+$, dada por $\widehat{|[(x_n)]|} = \lim_{n\to\infty} |x_n|$.

Hay que demostrar que $\widehat{K}$ es en efecto un campo y que $\widehat{|\cdot|}$ es un valor absoluto. Veamos primero que podemos extender las operaciones de K a $\widehat{K}$.

Sean $\alpha = [(a_n)]$, $\beta = [(b_n)]$ elementos de $\widehat{K}$, definimos su suma y su producto como

$$\alpha + \beta = [(a_n + b_n)] \quad \alpha\beta = [(a_n b_n)].$$

Hay que demostrar que estas operaciones no dependen de los representantes. Si $(a_n) \sim (a'_n)$ y

$(b_n) \sim (b'_n)$, por la desigualdad triangular tenemos que

$$\begin{aligned} |(a_n + b_n) - (a'_n + b'_n)| &= |(a_n - a'_n) + (b_n - b'_n)| \\ &\leq |a_n - a'_n| + |b_n - b'_n| \longrightarrow 0 \end{aligned}$$

Por lo que ambas sucesiones representan al mismo elemento. Nótese que para la suma, el elemento neutro 0 consiste en la clase de las sucesiones de Cauchy en K que convergen a 0. La existencia de inversos, la asociatividad y la conmutatividad de la suma se obtienen directo de las propiedades de la suma en K.

Para el producto, dado a la desigualdad triangular y a que las sucesiones de Cauchy son acotadas, se tiene que

$$\begin{aligned} |(a_n b_n) - (a'_n b'_n)| &= |a_n(b_n - b'_n) + b'_n(a_n - a'_n)| \\ &\leq |a_n||b_n - b'_n| + |b'_n||a_n - a'_n| \longrightarrow 0 \end{aligned}$$

Por lo que el producto está bien definido. La conmutatividad del producto se obtiene directamente de la conmutatividad en K. Hace falta demostrar la existencia de inversos multiplicativos. Si $\alpha = [(a_n)] \neq 0$, entonces

$$\lim_{n\to\infty} |a_n| > 0.$$

Existe entonces $c > 0$ y N entero positivo tal que $|a_n| \geq c$ para $n \geq N$ (lo cual asegura la existencia de a_n^{-1} para $n \geq N$). Definimos la secuencia (a'_n) como $a'_n = 0$ si $n < N$ y $a'_n = a_n^{-1}$ si $n \geq N$. Nótese que para $n, m \geq N$

$$\begin{aligned} \left|a_n^{-1} - a_m^{-1}\right| &= \left|(a_m - a_n)(a_n a_m)^{-1}\right| \\ &= |a_m - a_n|\left|(a_n a_m)^{-1}\right| \\ &= |a_m - a_n|\,|(a_n a_m)|^{-1} \\ &\leq |a_m - a_n|\, c^{-2}. \end{aligned}$$

Por lo tanto (a'_n) es una secuencia de Cauchy. Es fácil ver que $\gamma = [(a'_n)]$ corresponde al inverso de α.

Ahora comprobemos que $\widehat{|\cdot|}$ cumple con las propiedades del valor absoluto. Sean $x = [(x_n)]$ y $y = [(y_n)]$ elementos de $\widehat{K}$, entonces

$$\widehat{|x|} = 0 \iff \lim_{n\to\infty} |x_n| = 0 \iff (x_n) \sim (0, 0, 0, \cdots) \iff x = 0.$$

También

$$\begin{aligned} \widehat{|xy|} &= \lim_{n\to\infty} |x_n y_n| \\ &= \lim_{n\to\infty} |x_n|\,|y_n| = \lim_{n\to\infty} |x_n| \cdot \lim_{n\to\infty} |y_n| \\ &= \widehat{|x|} \cdot \widehat{|y|} \end{aligned}$$

y

$$\begin{aligned} \widehat{|x + y|} &= \lim_{n\to\infty} |x_n + y_n| \\ &\leq \lim_{n\to\infty} |x_n| + \lim_{n\to\infty} |y_n| \\ &= \widehat{|x|} + \widehat{|y|}. \end{aligned}$$

Se obtiene así que $\widehat{|\cdot|}$ es un valor absoluto.

Por último, sea $(L, |\cdot|_L)$ un campo valuado completo y sea $f : (K, |\cdot|) \longrightarrow (L, |\cdot|_L)$ un homomorfismo de campos contractivo. Si $x = [(x_n)] \in \widehat{K}$, entonces

$$\left|f(x_n) - f(x_m)\right|_L = \left|f(x_n - x_m)\right|_L \leq |x_n - x_m|,$$

por lo que $(f(x_n))$ es una secuencia de Cauchy en L, y como L es completo, entonces la secuencia converge. Definimos

$$\begin{array}{rcl} \widehat{f} : (\widehat{K}, \widehat{|\cdot|}) & \longrightarrow & (L, |\cdot|_L) \\ x & \longrightarrow & \widehat{f}(x) \coloneqq \lim\limits_{n\to\infty} f(x_n) \end{array}$$

Veamos que está bien definido. Si $(a_n) \sim (b_n)$ entonces

$$\left|f(a_n) - f(b_n)\right|_L = \left|f(a_n - b_n)\right|_L \leq |a_n - b_n| \longrightarrow 0.$$

De lo que resulta que $\lim_{n\to\infty} f(a_n) = \lim_{n\to\infty} f(b_n)$, es decir $\widehat{f}([(a_n)]) = \widehat{f}([(b_n)])$.

Demostramos que $\widehat{f}$ es un homomorfismo de campos: dados $x = [(x_n)], y = [(y_n)] \in \widehat{K}$, se tiene

$$\begin{array}{rcl} \widehat{f}(x+y) & = & \lim\limits_{n\to\infty} f(x_n + y_n) = \lim\limits_{n\to\infty} f(x_n) + \lim\limits_{n\to\infty} f(y_n) \\ & = & \widehat{f}(x) + \widehat{f}(y), \end{array}$$

$$\begin{array}{rcl} \widehat{f}(xy) & = & \lim\limits_{n\to\infty} f(x_n y_n) = \lim\limits_{n\to\infty} f(x_n) \cdot \lim\limits_{n\to\infty} f(y_n) \\ & = & \widehat{f}(x)\widehat{f}(y). \end{array}$$

y

$$\widehat{f}(1_{\widehat{K}}) = \widehat{f}(j(1_K)) = f(1_K) = 1_L.$$

Nótese que si $a \in K$,

$$\widehat{f}(j(a)) = \widehat{f}([(a, a, a, \cdots)]) = \lim_{n\to\infty} f(a) = f(a),$$

es decir $f = \widehat{f} \circ j$. Si $x = [(x_n)], y = [(y_n)] \in \widehat{K}$, entonces

$$\begin{array}{rcl} \left|\widehat{f}(x) - \widehat{f}(y)\right|_L & = & \left|\lim\limits_{n\to\infty} f(x_n) - \lim\limits_{n\to\infty} f(y_n)\right|_L \\ & = & \lim\limits_{n\to\infty} \left|f(x_n) - f(y_n)\right|_L \\ & \leq & \lim\limits_{n\to\infty} \left|x_n - y_n\right| \\ & = & \widehat{|x-y|}. \end{array}$$

Obteniéndose así que $\widehat{f}$ es contractiva, y como toda aplicación contractiva es Lipschitz, en particular es continua. Por la continuidad y como $j(K)$ es denso en $\widehat{K}$, se concluye que $\widehat{f}$ es único. ■

Proposición 2.5 *Sea $(K, |\cdot|)$ un campo valuado no arquimediano entonces su completación (2.4)*

$(\widehat{K}, \widehat{|\cdot|})$ *es no arquimediano.*

Demostración. Sean $x = [(x_n)]$ y $y = [(y_n)]$ elementos de $\widehat{K}$,

$$\widehat{|x+y|} = \widehat{d(x+y,0)} = \lim_{n\to\infty} |x_n + y_n|.$$

Dado que $|\cdot|$ es no arquimediano, se tiene

$$\widehat{|x+y|} \leq \lim_{n\to\infty} \max\{|x_n|, |y_n|\},$$

luego, como la función max es continua en $\mathbb{R}^2$, se obtiene

$$\begin{aligned} \widehat{|x+y|} &\leq \max\{\lim_{n\to\infty} |x_n|, \lim_{n\to\infty} |y_n|\} \\ &= \max\{\widehat{d}(x,0), \widehat{d}(y,0)\} \\ &= \max\{\widehat{|x|}, \widehat{|y|}\}. \end{aligned}$$

Se tiene así que $\widehat{|\cdot|}$ es no arquimediano. ∎

Definición 2.15 — Los números p-ádicos. Sea p un primo, definimos el campo de los números p-ádicos $(\mathbb{Q}_p, |\cdot|_p)$ como la completación (2.4) de $(\mathbb{Q}, |\cdot|_p)$.

Representacion de los números p-ádicos en potencias de p y su valuación.

Proposición 2.6 — Anillo de valoración de una valoración no arquimediana. *Sea K un campo y sea $|\cdot|$ una valoración no arquimediana sobre K. Definimos*

$$\mathcal{O} = \{x \in K : |x| \leq 1\}$$

y

$$\mathcal{P} = \{x \in K : |x| < 1\}.$$

Entonces $\mathcal{O}$ es un subanillo de K, mientras que $\mathcal{P}$ es un ideal de $\mathcal{O}$. Además, $\mathcal{P}$ es un ideal maximal de $\mathcal{O}$ y todo elemento de $\mathcal{O} \setminus \mathcal{P}$ es invertible en $\mathcal{O}$.

Demostración. Para $\mathcal{O}$ subanillo de K, es claro que 0 y 1 pertenecen a $\mathcal{O}$, por lo que basta demostrar que $\mathcal{O}$ es cerrado bajo la suma y la multiplicación.

Sean $a, b \in \mathcal{O}$, entonces $|a|, |b| \leq 1$ y luego

$$|a-b| \leq \max\{|a|, |-b|\} = \max\{|a|, |b|\} \leq 1,$$

por lo que $a - b \in \mathcal{O}$. Además

$$|ab| = |a||b| \leq 1,$$

de modo que $ab \in \mathcal{O}$. Por tanto $\mathcal{O}$ es un subanillo de K.

Para ver que $\mathcal{P}$ es ideal de $\mathcal{O}$, sean $a \in K$ y $x \in \mathcal{O}$, entonces $|a| < 1$ y $|x| \leq 1$, de lo que se obtiene que

$$|ax| = |a||x| < 1.$$

Por lo tanto $\mathcal{P}$ es un ideal de $\mathcal{O}$.

Ahora, si que $x \in \mathcal{O} \setminus \mathcal{P}$, entonces $|x| = 1$. Como K es campo, el inverso de x está en K, es decir que $x^{-1} \in K$. Nótese que

$$|x|\left|x^{-1}\right| = \left|xx^{-1}\right| = |1| = 1,$$

por lo que $\left|x^{-1}\right| = \frac{1}{|x|} = 1$. Entonces se tiene que $x^{-1} \in \mathcal{O}$, es decir que todo elemento de $\mathcal{O} \setminus \mathcal{P}$ es una unidad de $\mathcal{O}$.

Por último, supongamos que I es un ideal de $\mathcal{O}$ que contiene propiamente a $\mathcal{P}$, es decir

$$\mathcal{P} \subsetneq I \subseteq \mathcal{O}.$$

Si $x \in I \setminus \mathcal{P}$, se tiene también que $x \in \mathcal{O} \setminus \mathcal{P}$, por lo tanto $x^{-1} \in \mathcal{O}$. Luego $xx^{-1} = 1 \in I$, de lo que se sigue que $I = \mathcal{O}$. Por tanto, $\mathcal{P}$ es un ideal maximal de $\mathcal{O}$. ■

Definición 2.16 — Anillo de valoración. Sea K un campo y sea $|\cdot|$ un valor absoluto no arquimediano sobre k. El subanillo

$$\mathcal{O} = B(0,1) = \{x \in K \colon |x| \leq 1\} \subseteq k$$

se denomina el *anillo de valoración* asociado a $|\cdot|$.

El ideal

$$\mathcal{P} = B(0,1) = \{x \in k \colon |x| < 1\} \subseteq \mathcal{O}$$

se denomina el *ideal maximal* del anillo de valoración.

Definición 2.17 — Anillo local. Un anillo R se dice **local** si tiene un único ideal maximal.

Lema 2.7 *Todo anillo de valuación es un anillo local.*

Demostración. Dados $\mathcal{O}$ y $\mathcal{P}$ como arriba, vamos a demostrar que $\mathcal{P}$ es el único ideal maximal de $\mathcal{O}$.

Ya vimos que los elementos de $\mathcal{O} \setminus \mathcal{P}$ son invertibles. Si $x \in \mathcal{P}$, entonces $|x| < 1$, luego su inverso (que vive en el campo K), debe satisfacer $\left|x^{-1}\right| > 1$. Por lo tanto $x^{-1} \notin \mathcal{O}$ y x no es una unidad. Entonces se tiene que

$$\mathcal{O}^\times = \{x \in k : |x| = 1\},$$

y consecuentemente

$$\mathcal{O} \setminus \mathcal{O}^\times = \mathcal{P}.$$

Ahora, si $\mathfrak{m}$ es cualquier ideal maximal de $\mathcal{O}$, como $\mathfrak{m}$ no contiene unidades, entonces

$$\mathfrak{m} \subseteq \mathcal{O} \setminus \mathcal{O}^\times = \mathcal{P},$$

pero como $\mathfrak{m}$ es maximal, se debe cumplir que $\mathfrak{m} = \mathcal{P}$. ■

Definición 2.18 — Los enteros p-ádicos. Sea $(\mathbb{Q}_p, |\cdot|_p)$ el campo de los números p-ádicos. Definimos el anillo de los enteros p-ádicos como

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Nótese que $\mathbb{Z}_p$ es el anillo de valoración asociado a $|\cdot|_p$ con respecto a $\mathbb{Q}_p$.

Proposición 2.8 *El anillo $\mathbb{Z}_p$ de los enteros p-ádicos es un anillo local cuyo único ideal maximal es el ideal principal*

$$p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}.$$

Además:

1. $$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \colon p \nmid b\}.$$

2. *La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene imagen densa. Específicamente, dado $x \in \mathbb{Z}_p$ y $n \geq 1$, existe un único $\alpha \in \mathbb{Z}$ tal que*
$$0 \leq \alpha \leq p^n - 1$$
y
$$|x - \alpha|_p \leq p^{-n}.$$

3. *Para todo $x \in \mathbb{Z}_p$, existe una única secuencia de Cauchy (α_n) que converge a x y que satisface:*
   - $\alpha_n \in \mathbb{Z}$ *y* $0 \leq \alpha_n \leq p^n - 1$;
   - *para todo* $n \geq 2$,
$$\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}.$$

Demostración. Como $\mathbb{Z}_p$ es un anillo de valoración, entonces es un anillo local. Para determinar el ideal maximal, observemos que si $x \in \mathbb{Z}_p$ satisface $|x|_p < 1$, entonces, como la valuación p-ádica solo toma valores de la forma p^{-n}, se tiene

$$|x|_p \leq \frac{1}{p}.$$

Como $\left|p\right|_p = \frac{1}{p}$, obtenemos

$$\left|\frac{x}{p}\right|_p = \frac{|x|_p}{\left|p\right|_p} \leq 1.$$

Por lo tanto,

$$\frac{x}{p} \in \mathbb{Z}_p,$$

y así

$$x \in p\mathbb{Z}_p.$$

Esto muestra que el ideal de valoración está contenido en $p\mathbb{Z}_p$. Como $p\mathbb{Z}_p \neq \mathbb{Z}_p$ y el ideal de valoración es un ideal maximal, se concluye que

$$p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \colon |x|_p < 1\}.$$

Para demostrar (i), veamos que $\mathbb{Z}_{(p)}$ es el anillo de valoración de $\mathbb{Q}$ asociado a la valuación p-ádica. Se tiene que

$$\left|\frac{a}{b}\right| = p^{-n} \iff \frac{a}{b} = p^n \frac{a'}{b'} \quad \text{con } p \nmid a'b'.$$

Entonces $\left|\frac{a}{b}\right| \leq 1$ si y solo si $n \geq 0$. Si a y b son reducidos, solo se requiere $p \nmid b$.

Por tanto,

$$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \colon p \nmid b\}.$$

Para (ii), sean $x \in \mathbb{Z}_p$ y $n \geq 1$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, podemos escoger $\frac{a}{b} \in \mathbb{Q}$ tal que

$$\left| x - \frac{a}{b} \right|_p \leq p^{-n} < 1.$$

Por la desigualdad triangular ultramétrica,

$$\left| \frac{a}{b} \right|_p \leq \max\{ |x|_p , \left| x - \frac{a}{b} \right|_p \} \leq 1.$$

Por tanto, $\frac{a}{b} \in \mathbb{Z}_{(p)}$, y en particular $p \nmid b$. Luego, se tiene que $p^n \nmid b$, por lo que b es invertible módulo p^n. Existe entonces $b' \in \mathbb{Z}$ tal que

$$bb' \equiv 1 \pmod{p^n}.$$

Por consiguiente,

$$\frac{a}{b} - ab' = a \cdot \frac{1 - bb'}{b},$$

y como $p^n \mid (1 - bb')$ y $p \nmid b$, obtenemos

$$\left| \frac{a}{b} - ab' \right|_p \leq p^{-n}.$$

Es claro que $ab' \in \mathbb{Z}$. Por la desigualdad ultramétrica,

$$|x - ab'|_p \leq \max\{ \left| x - \frac{a}{b} \right|_p , \left| \frac{a}{b} - ab' \right|_p \} \leq p^{-n}.$$

Se tiene que ab' es congruente módulo p^n con un único entero α que satisface $0 \leq \alpha \leq p^n - 1$. Luego

$$|ab' - \alpha|_p \leq p^{-n}.$$

y por la desigualdad ultramétrica,

$$|x - \alpha|_p \leq \max\{ |x - ab'|_p , |ab' - \alpha|_p \} \leq p^{-n}.$$

Finalmente, (iii) se obtiene directamente de (ii). Para cada $n \geq 1$, aplicamos (ii) con el mismo elemento x y obtenemos un único entero α_n tal que

$$0 \leq \alpha_n \leq p^n - 1 \quad \text{y} \quad |x - \alpha_n|_p \leq p^{-n}.$$

Entonces

$$|x - \alpha_n|_p \longrightarrow 0,$$

por lo que $\alpha_n \longrightarrow x$.

Además, para $n \geq 2$,

$$|\alpha_n - \alpha_{n-1}|_p \leq \max\{ |\alpha_n - x|_p , |x - \alpha_{n-1}|_p \} \leq p^{-(n-1)},$$

y por tanto

$$\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}.$$

La unicidad se sigue de la unicidad de cada α_n en (ii). ■

Corolario 2.9 *Sea $a \in \mathbb{Z}_p$. Entonces*

$$a \in \mathbb{Z}_p^\times \iff |a|_p = 1 \iff a \notin p\mathbb{Z}_p.$$

Demostración. El resultado de obtiene directamente dado que $\mathbb{Z}_p$ es un anillo local y que $p\mathbb{Z}_p$ es su único ideal maximal. ■

Lema de Hensel y factorizaciones.

2.2.2. El Principio de Hasse.

Una de las herramientas fundamentales de la teoría de los números p-ádicos es el Lema de Hensel. Este resultado permite levantar soluciones de congruencias módulo p a soluciones exactas en el anillo de enteros p-ádicos, desempeñando un papel análogo al método de Newton en el análisis real. Además, constituye la principal herramienta para factorizar polinomios sobre $\mathbb{Z}_p$ y construir soluciones locales de ecuaciones diofánticas.

Lema 2.10 — Lema de Hensel. *Sea $F(X) \in \mathbb{Z}_p[X]$. Supongamos que existe $\alpha_1 \in \mathbb{Z}_p$ tal que*

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$

y

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

donde $F'(X)$ es la derivada formal de $F(X)$. Entonces existe un único $\alpha \in \mathbb{Z}_p$ tal que

$$\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p} \quad y \quad F(\alpha) = 0.$$

Demostración. Construiremos una sucesión de enteros p-ádicos

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$$

tal que, para todo $n \geq 1$ se cumpla

1. $F(\alpha_n) \equiv 0 \pmod{p^n\mathbb{Z}_p}$,
2. $\alpha_{n+1} \equiv \alpha_n \pmod{p^n\mathbb{Z}_p}$.

La segunda condición implica que (α_n) es una sucesión de Cauchy en $\mathbb{Z}_p$ y como $\mathbb{Z}_p$ es completo, existe su límite α, el cual satisface $F(\alpha) = 0$ por continuidad de los polinomios sobre $\mathbb{Z}_p$, además que $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ por construcción. Solo hace falta construir la sucesión. La existencia de α_1 es una de las hipótesis del lema. Supongamos ahora construido α_n. Buscamos

$$\alpha_{n+1} = \alpha_n + b_n p^n$$

para algún $b_1 \in \mathbb{Z}_p$. Desarrollando F mediante la expansión de Taylor formal se obtiene

$$F(\alpha_n + b_n p^n) \equiv F(\alpha_n) + F'(\alpha_n) b_n p^n \pmod{p^{n+1}\mathbb{Z}_p}.$$

Buscamos b_n tal que

$$F(\alpha_n) + F'(\alpha_n) b_n p^n \equiv 0 \pmod{p^{n+1}\mathbb{Z}_p}$$

Como $F(\alpha_n) \equiv 0 \pmod{p^n\mathbb{Z}_p}$, entonces $F(\alpha_n) = x p^n$ para algún x. Se obtiene la ecuación

$$x p^n + F'(\alpha_n) b_n p^n \equiv 0 \pmod{p^{n+1}\mathbb{Z}_p},$$

y luego de dividir para p^n

$$x + F'(\alpha_n)b_n \equiv 0 \pmod{p\mathbb{Z}_p}.$$

Nótese que por la construcción se tiene que $\alpha_n \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$, por lo tanto

$$F'(\alpha_n) \equiv F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

es decir que $F'(\alpha_n)$ es una unidad de $\mathbb{Z}_p$, es decir es invertible. Podemos tomar entonces

$$b_n \equiv -x\big(F'(\alpha_n)\big)^{-1} \pmod{p\mathbb{Z}_p},$$

y esta elección se puede hacer de manera única, considerando $0 \leq b_n \leq p-1$. Con esta elección de b_n se tiene

$$F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}},$$

por lo que $\alpha_{n+1} = \alpha_n + b_n p^n$ tiene las propiedades deseadas. La unicidad de cada b_n implica la unicidad de la sucesión (α_n) y, en consecuencia, de su límite α. ■

Teorema 2.11 — Principio Local-Global de Hasse-Minkowski. *Sea $Q(X_1, \ldots, X_n)$ una forma cuadrática homogénea con coeficientes en $\mathbb{Q}$. La ecuación diofántica $Q(X_1, \ldots, X_n) = 0$ admite una solución no trivial en $\mathbb{Q}^n$ (y consecuentemente en $\mathbb{Z}^n$) si y solo si admite una solución no trivial sobre $\mathbb{R}^n$ y sobre $\mathbb{Q}_p^n$ para todo número primo p.*

En geometría aritmética suele ser más elegante unificar $\mathbb{R}$ y $\mathbb{Q}_p$ utilizando el conjunto de lugares (o valuaciones) de $\mathbb{Q}$, denotado por $M_{\mathbb{Q}}$. Si denotamos $\mathbb{R}$ como $\mathbb{Q}_\infty$ (el lugar arquimediano), el teorema se reduce a decir que existe solución en $\mathbb{Q}$ si y solo si existe solución no trivial en $\mathbb{Q}_v$ para todo lugar $v \in M_{\mathbb{Q}}$. Aquí tienes un ejemplo clásico y riguroso de cómo el principio local-global y el Lema de Hensel operan en conjunto. He elegido una forma cuadrática que requiere analizar tanto un primo impar donde el Lema de Hensel clásico funciona de forma directa, como el primo $p = 2$, que exige la versión generalizada del lema debido a la ramificación de la derivada.

▪ **Ejemplo 2.6** Consideremos la forma cuadrática homogénea sobre $\mathbb{Q}$:

$$Q(X, Y, Z) = X^2 - 2Y^2 - 7Z^2$$

Queremos demostrar que la ecuación diofántica $Q(X, Y, Z) = 0$ admite una solución no trivial en $\mathbb{Q}^3$ utilizando el Principio de Hasse-Minkowski 2.11.

1. Solución sobre $\mathbb{R}$ (el lugar arquimediano): Como los coeficientes no tienen el mismo signo, la forma es indefinida. Tomando, por ejemplo, $Y = 1$ y $Z = 1$, obtenemos $X^2 = 9$, lo cual tiene solución real $X = 3$. Por tanto, $Q = 0$ tiene la solución no trivial $(3, 1, 1) \in \mathbb{R}^3$.

2. Solución sobre $\mathbb{Q}_7$ (Reducción y Lema de Hensel clásico): Debemos encontrar una solución en los enteros 7-ádicos $\mathbb{Z}_7$. Para aplicar el Lema de Hensel, fijamos algunas variables y buscamos levantar una solución módulo 7. Fijemos $Y = 1$ y $Z = 0$, de modo que definimos el polinomio en una variable:

$$f(X) = Q(X, 1, 0) = X^2 - 2$$

Reducimos el polinomio módulo la congruencia de $\mathbb{F}_7$:

$$\overline{f}(X) \equiv X^2 - 2 \pmod 7$$

Buscamos una raíz $X_0 \in \mathbb{F}_7$. Probando valores, vemos que $X_0 = 3$ funciona, ya que $3^2 - 2 = 7 \equiv 0 \pmod 7$.

Ahora, verificamos la condición de la derivada formal para aplicar el Lema de Hensel. La derivada es $f'(X) = 2X$. Evaluamos en nuestra aproximación inicial:

$$f'(3) = 6 \not\equiv 0 \pmod 7$$

En términos de norma ultramétrica, tenemos $|f(3)|_7 \leq 7^{-1} < 1 = |f'(3)|_7^2$. Como la derivada no se anula módulo 7, el Lema de Hensel garantiza que existe un único $\alpha \in \mathbb{Z}_7$ tal que:

$$\alpha \equiv 3 \pmod 7 \quad \text{y} \quad f(\alpha) = \alpha^2 - 2 = 0$$

Por lo tanto, el vector $(\alpha, 1, 0)$ es una solución no trivial en $\mathbb{Q}_7^3$.

3. Solución sobre $\mathbb{Q}_2$ (Lema de Hensel generalizado): Para $p = 2$, la reducción directa suele fallar porque la derivada formal de X^2 es $2X$, la cual siempre se anula módulo 2. Requerimos el Lema de Hensel generalizado, que exige una "mejor aproximación" inicial. Fijemos esta vez $Y = 1$ y $Z = 1$. Definimos el polinomio:

$$g(X) = Q(X, 1, 1) = X^2 - 9$$

Proponemos como aproximación inicial $X_0 = 1$. Evaluamos el polinomio y su derivada $g'(X) = 2X$ en este punto y medimos sus valuaciones 2-ádicas:

$$g(1) = -8 \implies v_2(g(1)) = 3$$
$$g'(1) = 2 \implies v_2(g'(1)) = 1$$

La condición fuerte de Hensel exige que $v_2(g(X_0)) > 2v_2(g'(X_0))$. Sustituyendo nuestros valores:

$$3 > 2(1) \implies 3 > 2$$

La desigualdad se cumple estrictamente. El Lema de Hensel nos asegura que existe un elemento $\beta \in \mathbb{Z}_2$ tal que $g(\beta) = 0$ (y además $\beta \equiv 1 \pmod{2^2}$). Esto nos provee la solución no trivial $(\beta, 1, 1)$ en $\mathbb{Q}_2^3$.

4. Solución sobre los demás primos: Para cualquier primo $p \notin \{2, 7\}$, el determinante de la forma cuadrática (det = 14) es una unidad en $\mathbb{Z}_p$. Todo espacio cuadrático no degenerado de dimensión $n \geq 3$ sobre $\mathbb{Q}_p$ es automáticamente isótropo (tiene vectores nulos no triviales) si la forma tiene buena reducción.

Conclusión Global: Dado que $Q(X, Y, Z) = 0$ posee soluciones no triviales en $\mathbb{R}$ y en todo $\mathbb{Q}_p$ (comprobado explícitamente en los lugares "malos" 2 y 7, y garantizado en el resto), el Principio de Hasse-Minkowski establece de forma definitiva que existe una solución no trivial en $\mathbb{Q}^3$ y, consecuentemente, en $\mathbb{Z}^3$. ∎

∎ **Ejemplo 2.7** Consideremos la forma cuadrática homogénea:

$$Q(X, Y, Z) = 5X^2 + 7Y^2 - 13Z^2$$

Queremos demostrar que la ecuación $Q(X, Y, Z) = 0$ admite una solución no trivial en $\mathbb{Z}^3$. Para ello, buscaremos soluciones locales que claramente no residen en los racionales.

1. Solución sobre $\mathbb{R}$ (El lugar arquimediano): Fijemos las variables $Y = 1$ y $Z = 1$. Obtenemos la ecuación:

$$5X^2 + 7(1)^2 - 13(1)^2 = 0 \implies 5X^2 - 6 = 0$$

Despejando, obtenemos $X = \sqrt{\frac{6}{5}}$. Por lo tanto, el vector $\left(\sqrt{\frac{6}{5}}, 1, 1\right)$ es una solución en $\mathbb{R}^3$. Es evidente que esta solución es puramente local (irracional) y no nos sirve como solución en $\mathbb{Q}$.

2. Solución sobre $\mathbb{Q}_{13}$ (Reducción y Lema de Hensel): Veamos qué ocurre en el primo $p = 13$, que divide a uno de los coeficientes. Para aplicar Hensel, buscaremos una raíz módulo 13. Fijemos $X = 2$ y $Z = 1$, definiendo el polinomio en la variable Y:

$$f(Y) = Q(2, Y, 1) = 5(4) + 7Y^2 - 13 = 7Y^2 + 7$$

Reducimos módulo 13:

$$\overline{f}(Y) \equiv 7Y^2 + 7 \equiv 7(Y^2 + 1) \pmod{13}$$

Buscamos una raíz $Y_0 \in \mathbb{F}_{13}$. Necesitamos que $Y^2 \equiv -1 \pmod{13}$. Dado que $13 \equiv 1 \pmod{4}$, sabemos que -1 es un residuo cuadrático. De hecho, $5^2 = 25 \equiv -1 \pmod{13}$. Tomamos entonces $Y_0 = 5$.

Verificamos la derivada formal $f'(Y) = 14Y$ evaluada en nuestra aproximación:

$$f'(5) = 14(5) = 70 \equiv 5 \not\equiv 0 \pmod{13}$$

Como la derivada no se anula módulo 13, el Lema de Hensel clásico garantiza la existencia de un elemento $\beta \in \mathbb{Z}_{13}$ tal que $\beta = 5 + 13k_1 + 13^2k_2 + \cdots$ y $f(\beta) = 0$. Hemos encontrado la solución local $(2, \beta, 1) \in \mathbb{Q}_{13}^3$. Al igual que en el caso real, β es un número 13-ádico con una expansión infinita, por lo que esta solución local no es racional.

3. El salto Global (Principio de Hasse-Minkowski): Mediante cálculos similares (reduciendo y aplicando Hensel), se puede verificar que la ecuación posee soluciones en $\mathbb{Q}_5$ y $\mathbb{Q}_7$ (donde también se levantan raíces p-ádicas infinitas), y para el resto de los primos el determinante det $= -455$ es una unidad, garantizando isotropía local.

Hemos construido soluciones locales que consisten en números con raíces cuadradas irracionales y series de potencias infinitas. Ninguna de estas construcciones nos da un vector de números enteros. Sin embargo, el Teorema de Hasse-Minkowski 2.11 toma esta colección de existencias locales y dicta un veredicto global: *debe existir* una solución racional.

Sabiendo que la solución global existe con total certeza, podemos realizar una búsqueda en $\mathbb{Z}$. Si inspeccionamos valores, eventualmente descubrimos que:

$$X = 3, \quad Y = 1, \quad Z = 2$$

Evaluando la forma:

$$5(3)^2 + 7(1)^2 - 13(2)^2 = 5(9) + 7(1) - 13(4) = 45 + 7 - 52 = 0$$

El vector $(3, 1, 2)$ es la solución global garantizada por la existencia de nuestras abstractas

raíces locales $\sqrt{6/5}$ y β. ∎

3. Fallo del Principio Local-Global

El principio de Hasse–Minkowski establece que una forma cuadrática posee una solución racional si y solo si posee soluciones en todos los lugares de $\mathbb{Q}$. Es natural preguntarse si este principio continua siendo válido para ecuaciones diofantinas más generales. La respuesta es no: existen curvas con soluciones en todos los lugares de $\mathbb{Q}$, pero sin soluciones racionales.

3.1. La curva $3x^3 + 4y^3 + 5z^3 = 0$.

El primer contraejemplo fue encontrado por Ernst Selmer en 1951. Selmer define la curva

$$C : 3X^3 + 4Y^3 + 5Z^3 = 0$$

y demuestra que tiene solución en todos los lugares de $\mathbb{Q}$, pero no en $\mathbb{Q}$.

Lema 3.1 *Sea $p \neq 3$ un primo. Entonces:*
1. *Si $p \not\equiv 1 \pmod 3$, todo elemento de $(\mathbb{Z}/p\mathbb{Z})^\times$ es un cubo.*
2. *Si $p \equiv 1 \pmod 3$, los cubos forman un subgrupo de índice 3 de $(\mathbb{Z}/p\mathbb{Z})^\times$.*

Demostración. Consideremos el homomorfismo

$$\begin{aligned} \varphi : (\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\ x &\longrightarrow x^3 \end{aligned}$$

Sabemos que $x \in \ker(\varphi)$ si y solo si $x^3 = 1$. Dado que $(\mathbb{Z}/p\mathbb{Z})^\times$ es un grupo cíclico de orden $p-1$, entonces la ecuación $x^3 = 1$ tiene $\gcd(3, p-1)$ soluciones, es decir

$$\left|\ker(\varphi)\right| = \gcd(3, p-1).$$

Por el Primer Teorema de Isomorfismo,

$$\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = \left|\ker(\varphi)\right| \left|\mathrm{Img}(\varphi)\right|,$$

y entonces

$$\left|\mathrm{Img}(\varphi)\right| = \frac{p-1}{\gcd(3, p-1)}.$$

Tenemos dos casos

1. Si $p \not\equiv 1 \pmod 3$, entonces $\gcd(3, p-1) = 1$, y por tanto

   $$\left|\mathrm{Img}(\varphi)\right| = p - 1.$$

   Esto indica que $\mathrm{Img}(\varphi) = (\mathbb{Z}/p\mathbb{Z})^\times$, es decir que todos los elementos de $(\mathbb{Z}/p\mathbb{Z})^\times$ son cubos.
2. Si $p \equiv 1 \pmod 3$, se tiene que $\gcd(3, p-1) = 3$, y luego

   $$\left|\mathrm{Img}(\varphi)\right| = \frac{p-1}{3}.$$

Como $\mathrm{Img}(\varphi)$ es un subgrupo de $(\mathbb{Z}/p\mathbb{Z})^\times$, se obtiene que los cubos forman un subgrupo de índice 3.

■

Teorema 3.2 — Selmer. *La curva*

$$C : 3X^3 + 4Y^3 + 5Z^3 = 0$$

posee un punto no trivial sobre $\mathbb{R}$ y sobre $\mathbb{Q}_p$ para todo primo p, pero no posee ningún punto racional no trivial.

Demostración. **1. Solución sobre $\mathbb{R}$:** Es fácil ver que $(\sqrt[3]{\frac{5}{3}}, 0, -1)$ es una solución.

2. Solución sobre $\mathbb{Q}_2$: Fijamos $Y = 0$ y $Z = 1$ y definimos el polinomio en una variable:

$$f(X) = 3X^3 + 5.$$

Con $X = 1$ y reduciendo el polinomio módulo la congruencia en $\mathbb{F}_2$:

$$f(1) \equiv 0 \pmod 2.$$

Dado que $f'(X) = 9X^2$, se tiene que:

$$f'(1) \not\equiv 0 \pmod 2.$$

Por el lema de Hensel, existe un único $\alpha \in \mathbb{Z}_2$ tal que:

$$\alpha \equiv 1 \pmod 2 \quad \text{y} \quad f(\alpha) = 3\alpha^3 + 5 = 0.$$

Por lo tanto, $(\alpha, 0, 1)$ es una solución no trivial en $\mathbb{Q}_2^3$.

3. Solución sobre $\mathbb{Q}_3$: Fijamos $X = 0$ y $Z = -1$, obteniendo el polinomio

$$f(Y) = 4Y^3 - 5.$$

Como

$$2^3 = 8 \equiv -1 \equiv \frac{5}{4} \pmod{27},$$

el lema de Hensel garantiza la existencia de un único $\beta \in \mathbb{Z}_3$ tal que

$$\beta^3 = \frac{5}{4}.$$

Por lo tanto, $(0, \beta, -1)$ es una solución no trivial en $\mathbb{Q}_3^3$.

4. Solución sobre $\mathbb{Q}_5$: Fijamos $Y = -1$ y $Z = -1$, obteniendo el polinomio

$$f(X) = 3X^3 - 9.$$

Como

$$2^3 = 8 \equiv 3 \pmod 5,$$

el lema de Hensel garantiza la existencia de un único $\gamma \in \mathbb{Z}_5$ tal que

$$\gamma^3 = 3.$$

Por lo tanto, $(\gamma, -1, -1)$ es una solución no trivial en $\mathbb{Q}_5^3$.

5. Solución sobre $\mathbb{Q}_p$ para el resto de primos: Sea $p \neq 2, 3, 5$. Como el grupo multiplicativo

$$(\mathbb{Z}/p\mathbb{Z})^\times$$

es cíclico de orden $p-1$, se distinguen dos casos:

- Supongamos que 3 es un cubo módulo p, es decir que existe solución para $x^3 - 3 = 0$ en $\mathbb{F}_3$, entonces por el lema de Hensel existe un $\gamma \in \mathbb{Z}_p$ tal que $\gamma^3 = 3$. En consecuencia, $(x, -1, -1)$ es una solución no trivial de la curva sobre $\mathbb{Q}_p$.
- Suponiendo ahora que 3 no es un cubo módulo p. En este caso, no todos los elementos de $(\mathbb{Z}/p\mathbb{Z})^\times$ son cubos, por lo que del lema anterior se obtiene que $p \equiv 1 \pmod 3$ y los cubos forman un subgrupo de índice 3. Por lo tanto, existen tres clases laterales representadas por $\{1, 3, 9\}$, de modo que todo elemento no nulo de $\mathbb{F}_p$ es congruente a uno de los números

  $$b^3, \qquad 3b^3, \qquad 9b^3,$$

  para algún $b \not\equiv 0 \pmod p$.
  Aplicando esto a 5, se presentan tres posibilidades:

  1. Si
  $$5 \equiv b^3 \pmod p,$$
  entonces, por el lema de Hensel, existe $y \in \mathbb{Z}_p$ tal que
  $$y^3 = 5.$$
  En consecuencia,
  $$(-y, y, -1)$$
  es una solución de la curva.
  2. Si
  $$5 \equiv 3b^3 \pmod p,$$
  entonces
  $$\frac{5}{3}$$
  es un cubo en $\mathbb{Z}_p$. Luego, existe un $x \in \mathbb{Z}_p$ tal que
  $$x^3 = \frac{5}{3},$$
  y se obtiene la solución
  $$(x, 0, -1).$$
  3. Si
  $$5 \equiv 9b^3 \pmod p,$$
  entonces
  $$15$$
  es un cubo en $\mathbb{Z}_p$. Existe $t \in \mathbb{Z}_p$ tal que
  $$t^3 = 15.$$

De aquí se obtiene la solución

$$(3t, 5, -7),$$

y, por homogeneidad de la ecuación,

$$\left(\frac{3t}{7}, \frac{5}{7}, -1\right)$$

también es una solución.

En todos los casos la ecuación admite una solución no trivial sobre $\mathbb{Q}_p$, concluyendo así la demostración.

■

4. Estudiando el fallo.

Definición 4.1 — Curva elíptica. Sea K un campo. Una *curva elíptica* sobre K es una curva algebraica suave, proyectiva y de género 1, junto con un punto distinguido $O \in E(K)$, llamado *punto en el infinito*.

Si $\text{char}(K) \neq 2, 3$, toda curva elíptica puede escribirse mediante una ecuación de Weierstrass de la forma

$$E: \quad y^2 = x^3 + Ax + B,$$

donde $A, B \in K$ y

$$4A^3 + 27B^2 \neq 0.$$

La condición anterior garantiza que la curva sea suave, es decir, que no posea puntos singulares.

En coordenadas proyectivas, la ecuación se escribe como

$$E: \quad Y^2Z = X^3 + AXZ^2 + BZ^3,$$

y el punto distinguido es

$$O = [0 : 1 : 0].$$

La importancia de las curvas elípticas para nuestro propósito radica en que sus puntos racionales forman un grupo abeliano. La operación de grupo puede describirse geométricamente mediante la conocida construcción de la recta secante y tangente.

Teorema 4.1 *Sea E una curva elíptica sobre K. Entonces $E(K)$ posee una estructura natural de grupo abeliano, cuyo elemento identidad es el punto O.*

Para la ecuación

$$E: \quad y^2 = x^3 + Ax + B,$$

si $P, Q \in E(K)$, la suma $P + Q$ se obtiene geométricamente trazando la recta que pasa por P y Q (o la recta tangente si $P = Q$). Esta recta corta a E en un tercer punto R, y se define

$$P + Q = -R,$$

donde el inverso de un punto se obtiene mediante la reflexión respecto del eje x:

$$-(x, y) = (x, -y).$$

Además,

$$-P = O$$

cuando $P = O$.

Esta estructura de grupo permite estudiar las curvas elípticas mediante herramientas de teoría de grupos y, posteriormente, mediante isogenias y cohomología de Galois.

Definición 4.2 — Isogenia. Sean E y E' curvas elípticas definidas sobre un campo K. Una *isogenia* es un morfismo no constante

$$\phi : E \longrightarrow E'$$

definido sobre K que preserva el punto identidad, es decir,

$$\phi(O_E) = O_{E'}.$$

ϕ también es un homomorfismo de grupos:

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

para todos $P, Q \in E(\overline{K})$.

Una isogenia es, por tanto, una aplicación que permite relacionar dos curvas elípticas conservando su estructura de grupo. Si

$$\phi : E \longrightarrow E'$$

es una isogenia, definimos su *núcleo* como

$$\ker(\phi) := \{P \in E(\overline{K}) : \phi(P) = O_{E'}\}.$$

De esta manera, tenemos la sucesión

$$0 \longrightarrow \ker(\phi) \longrightarrow E(\overline{K}) \xrightarrow{\phi} E'(\overline{K}),$$

donde la primera flecha es la inclusión natural y la segunda es la aplicación inducida por ϕ. La sucesión es exacta en $E(\overline{K})$, pues

$$\ker\left(E(\overline{K}) \xrightarrow{\phi} E'(\overline{K})\right) = \ker(\phi).$$

Más generalmente, denotamos

$$E[\phi] := \ker(\phi)$$

y llamamos a $E[\phi]$ el *grupo de ϕ-torsión*.

Un caso particularmente importante se obtiene al considerar la isogenia de multiplicación por n,

$$[n] : E \longrightarrow E, \qquad P \longmapsto nP.$$

La aplicaciónes un morfismo de esquemas. En efecto, en coordenadas afines una curva elíptica está dada por

$$E : \quad y^2 = x^3 + Ax + B,$$

y la ley de grupo de E está dada por funciones racionales en las coordenadas de los puntos. Por

tanto, la multiplicación por n se obtiene componiendo sucesivamente la ley de suma y es, en particular, un morfismo algebraico.

Más generalmente, si

$$\phi\colon E \longrightarrow E'$$

es una isogenia, entonces ϕ es, por definición, un morfismo de curvas algebraicas definido sobre K que preserva el punto identidad. Al considerar los puntos sobre $\overline{K}$, obtenemos un homomorfismo de grupos

$$\phi\colon E(\overline{K}) \longrightarrow E'(\overline{K}).$$

Como ϕ está definida sobre K, esta aplicación es compatible con la acción del grupo absoluto de Galois. Es decir, para todo $\sigma \in G_K$ y todo $P \in E(\overline{K})$ se tiene

$$\phi(\sigma P) = \sigma(\phi(P)).$$

Por tanto, el núcleo

$$E[\phi] = \ker(\phi)$$

es estable bajo la acción de G_K y, en consecuencia, es un G_K-módulo.

4.1. Introducción a la cohomologia de Galois

Sea K un campo y sea $\overline{K}$ una clausura algebraica de K. Para estudiar los puntos de una curva elíptica definidos sobre K a partir de sus puntos sobre $\overline{K}$, consideramos la acción de los automorfismos de $\overline{K}$ que fijan K.

Definición 4.3 — Grupo absoluto de Galois. El *grupo absoluto de Galois* de K se define como

$$G_K := \mathrm{Gal}(\overline{K}/K).$$

Es decir, G_K es el grupo formado por todos los automorfismos

$$\sigma\colon \overline{K} \longrightarrow \overline{K}$$

que fijan cada elemento de K.

El grupo G_K es, en general, un grupo infinito. Sin embargo, puede entenderse a partir de los grupos de Galois de las extensiones finitas de K contenidas en $\overline{K}$. Si $K \subseteq L \subseteq M \subseteq \overline{K}$ son extensiones finitas, la restricción de automorfismos induce un homomorfismo

$$\mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(L/K), \qquad \sigma \longmapsto \sigma|L.$$

Estos homomorfismos forman un sistema inverso y, de manera natural, se tiene

$$G_K \cong \varprojlim_{L/K \text{ finita}} \mathrm{Gal}(L/K).$$

Por esta razón, G_K se denomina un *grupo profinito*.

Definición 4.4 — Acción continua de Galois. Sea M un grupo abeliano dotado de una estructura

topológica. Una *acción continua de Galois* de G_K sobre M es una acción de grupos

$$G_K \times M \longrightarrow M, \qquad (\sigma, m) \longmapsto \sigma(m),$$

que es continua.

En este caso, decimos que M es un G_K-módulo topológico. Cuando M está dotado de la topología discreta, la continuidad de la acción significa que para cada $m \in M$ el estabilizador

$$\mathrm{Stab}_{G_K}(m) = \{\sigma \in G_K : \sigma(m) = m\}$$

es un subgrupo abierto de G_K.

Para un G_K-módulo M, consideramos el conjunto de elementos que permanecen fijos bajo la acción de todos los elementos de G_K.

Definición 4.5 — Elementos invariantes. Sea M un G_K-módulo. El subgrupo de *elementos invariantes* de M se define como

$$M^{G_K} \coloneqq \{m \in M \colon \sigma(m) = m \text{ para todo } \sigma \in G_K\}.$$

En particular, para una curva elíptica E definida sobre K, los puntos de $E(\overline{K})$ que son invariantes bajo la acción de G_K son precisamente los puntos definidos sobre K. Es decir,

$$E(\overline{K})^{G_K} = E(K).$$

En efecto, si $P = (x, y) \in E(\overline{K})$ es fijo por todo $\sigma \in G_K$, entonces

$$\sigma(x) = x \qquad \text{y} \qquad \sigma(y) = y$$

para todo $\sigma \in G_K$. Por la caracterización de K como el subcampo de $\overline{K}$ fijado por G_K, se tiene $x, y \in K$, y por tanto $P \in E(K)$. El recíproco es inmediato, pues todo elemento de G_K fija los elementos de K.

La operación que asocia a un G_K-módulo M su subgrupo de invariantes M^{G_K} constituye el grado cero de la cohomología de Galois.

Definición 4.6 — Cohomología de grado cero. Sea M un G_K-módulo. Definimos

$$H^0(G_K, M) \coloneqq M^{G_K}.$$

La construcción de los elementos invariantes es functorial. Si $f : M \longrightarrow N$ es un homomorfismo de G_K-módulos, entonces f lleva elementos invariantes de M en elementos invariantes de N. En efecto, si $m \in M^{G_K}$, para todo $\sigma \in G_K$ se tiene

$$\sigma(m) = m,$$

y, como f es G_K-equivariante,

$$\sigma(f(m)) = f(\sigma(m)) = f(m).$$

Por tanto,

$$f(m) \in N^{G_K}.$$

Así, los invariantes definen un funtor

$$(-)^{G_K} : G_K\text{-}\mathbf{Mod} \longrightarrow \mathbf{Ab},$$

que a cada G_K-módulo M le asocia M^{G_K}.

Este funtor es exacto por la izquierda, pero no necesariamente exacto por la derecha. Para verlo, consideremos una sucesión exacta de G_K-módulos

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0.$$

Al tomar invariantes obtenemos una sucesión

$$0 \longrightarrow M_1^{G_K} \longrightarrow M_2^{G_K} \longrightarrow M_3^{G_K},$$

que sigue siendo exacta. Sin embargo, la última aplicación no tiene por qué ser sobreyectiva.

La cohomología de Galois surge precisamente al estudiar la obstrucción a que el funtor de invariantes sea exacto.

Para definir el primer grupo de cohomología, consideremos un M G_K-módulo. Un 1-*cociclo* es una aplicación

$$c : G_K \longrightarrow M$$

que satisface

$$c(\sigma\tau) = c(\sigma) + \sigma(c(\tau))$$

para todos $\sigma, \tau \in G_K$.

El conjunto de todos los 1-cociclos se denota por

$$Z^1(G_K, M).$$

La condición anterior se denomina *condición de cociclo*.

Para cada elemento $m \in M$, podemos definir una aplicación

$$c_m : G_K \longrightarrow M$$

mediante

$$c_m(\sigma) = \sigma(m) - m.$$

Esta aplicación satisface la condición de cociclo, pues

$$\begin{aligned} c_m(\sigma\tau) &= \sigma\tau(m) - m \\ &= \sigma(\tau(m) - m) + \sigma(m) - m \\ &= \sigma(c_m(\tau)) + c_m(\sigma). \end{aligned}$$

Los cociclos de esta forma se denominan 1-*cociclos principales*. El conjunto de todos ellos se denota por

$$B^1(G_K, M).$$

Se tiene entonces

$$B^1(G_K, M) \subseteq Z^1(G_K, M).$$

Definición 4.7 — Cohomología de primer grado. Sea M un G_K-módulo. El *primer grupo de*

cohomología de Galois se define como

$$H^1(G_K, M) \coloneqq \frac{Z^1(G_K, M)}{B^1(G_K, M)}.$$

Sean M_1, M_2 y M_3 G_K-módulos y supongamos que tenemos una sucesión exacta de G_K-módulos

$$0 \longrightarrow M_1 \xrightarrow{\iota} M_2 \xrightarrow{\pi} M_3 \longrightarrow 0.$$

Al aplicar el funtor de invariantes obtenemos

$$0 \longrightarrow M_1^{G_K} \xrightarrow{\iota} M_2^{G_K} \xrightarrow{\pi} M_3^{G_K}.$$

Como vimos anteriormente, esta sucesión no tiene por qué ser exacta a la derecha. La cohomología de Galois permite completar esta sucesión introduciendo los grupos H^1.

En particular, existe un homomorfismo

$$\delta : M_3^{G_K} \longrightarrow H^1(G_K, M_1),$$

llamado *homomorfismo de conexión*, que permite extender la sucesión anterior a una sucesión exacta

$$0 \longrightarrow H^0(G_K, M_1) \longrightarrow H^0(G_K, M_2) \longrightarrow H^0(G_K, M_3) \xrightarrow{\delta} H^1(G_K, M_1) \longrightarrow H^1(G_K, M_2) \longrightarrow H^1(G_K, M_3).$$

Recordemos que

$$H^0(G_K, M_i) = M_i^{G_K}.$$

Por tanto, la sucesión puede escribirse también como

$$0 \longrightarrow M_1^{G_K} \longrightarrow M_2^{G_K} \longrightarrow M_3^{G_K} \xrightarrow{\delta} H^1(G_K, M_1) \longrightarrow H^1(G_K, M_2) \longrightarrow H^1(G_K, M_3).$$

El homomorfismo de conexión puede describirse explícitamente. Sea $m_3 \in M_3^{G_K}$. Como $\pi : M_2 \to M_3$ es sobreyectiva, existe $m_2 \in M_2$ tal que

$$\pi(m_2) = m_3.$$

Para cada $\sigma \in G_K$, definimos

$$c_{m_2}(\sigma) = \sigma(m_2) - m_2.$$

Como m_3 es G_K-invariante, se tiene

$$\pi\big(\sigma(m_2) - m_2\big) = \sigma(\pi(m_2)) - \pi(m_2) = \sigma(m_3) - m_3 = 0.$$

Por la exactitud de la sucesión, existe un único elemento $c_{m_2}(\sigma) \in M_1$ tal que

$$\iota(c_{m_2}(\sigma)) = \sigma(m_2) - m_2.$$

La aplicación

$$c_{m_2} : G_K \longrightarrow M_1$$

es un 1-cociclo. Definimos entonces

$$\delta(m_3) = [c_{m_2}] \in H^1(G_K, M_1).$$

La clase de c_{m_2} no depende de la elección de m_2, por lo que δ está bien definida.

La exactitud en $M_3^{G_K}$ significa que

$$\ker(\delta) = \operatorname{im}\left(M_2^{G_K} \longrightarrow M_3^{G_K}\right).$$

En otras palabras, un elemento $m_3 \in M_3^{G_K}$ proviene de un elemento G_K-invariante de M_2 si y solamente si su imagen mediante el homomorfismo de conexión es trivial en $H^1(G_K, M_1)$.

Supongamos ahora que L/K es una extensión finita de Galois contenida en $\overline{K}$. Consideremos los grupos absolutos de Galois

$$G_L = \operatorname{Gal}(\overline{K}/L) \qquad \text{y} \qquad G_K = \operatorname{Gal}(\overline{K}/K).$$

Como todo automorfismo que fija L fija también K, tenemos una inclusión

$$G_L \subseteq G_K.$$

Además, como L/K es una extensión de Galois, G_L es un subgrupo normal de G_K y existe un isomorfismo

$$G_K/G_L \cong \operatorname{Gal}(L/K).$$

Sea M un G_K-módulo. Por restricción de la acción de G_K, podemos considerar M también como un G_L-módulo. Esta inclusión de grupos induce un homomorfismo

$$\operatorname{res}_{L/K} : H^1(G_K, M) \longrightarrow H^1(G_L, M),$$

llamado *homomorfismo de restricción*.

Si $c : G_K \to M$ es un 1-cociclo, su restricción a G_L está dada simplemente por

$$\operatorname{res}_{L/K}([c]) = [c|_{G_L}].$$

Por otro lado, como

$$G_K/G_L \cong \operatorname{Gal}(L/K),$$

podemos considerar el grupo finito $\operatorname{Gal}(L/K)$ actuando sobre los elementos de M que son invariantes bajo G_L.

Sea

$$M^{G_L} = \{m \in M : \sigma(m) = m \text{ para todo } \sigma \in G_L\}.$$

Como G_L es normal en G_K, el grupo $\operatorname{Gal}(L/K)$ actúa naturalmente sobre M^{G_L}.

Un 1-cociclo

$$c : \operatorname{Gal}(L/K) \longrightarrow M^{G_L}$$

puede entonces componerse con la proyección

$$G_K \longrightarrow G_K/G_L \cong \operatorname{Gal}(L/K)$$

para obtener un 1-cociclo sobre G_K. Esto induce un homomorfismo

$$\inf_{L/K} : H^1(\operatorname{Gal}(L/K), M^{G_L}) \longrightarrow H^1(G_K, M),$$

llamado *homomorfismo de inflación*.

Los homomorfismos de inflación y restricción aparecen en la sucesión exacta

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), M^{G_L}) \xrightarrow{\inf_{L/K}} H^1(G_K, M) \xrightarrow{\mathrm{res}_{L/K}} H^1(G_L, M).$$

En particular,

$$\mathrm{im}(\inf_{L/K}) = \ker(\mathrm{res}_{L/K}).$$

Esta sucesión permite relacionar la cohomología del grupo absoluto de Galois G_K con la cohomología del grupo G_L y, a través de este, con el grupo finito $\mathrm{Gal}(L/K)$.

4.2. El Jacobiano de una curva.

Sea k un campo base y C una curva algebraica sobre k, entendida como un k-esquema proyectivo, suave, geométricamente conexo (o geométricamente irreducible) de dimensión 1. Sea $g \geq 0$ el género de la curva.

Denotamos $\mathbf{Sch}/k$ como la categoría de esquemas sobre k, $S \to \mathrm{Spec}(k)$. Definimos el funtor de Picard:

$$\mathcal{P}ic_{C/k} : (\mathbf{Sch}/k)^{\mathrm{op}} \to \mathbf{Ab}, (T \to \mathrm{Spec}(k)) \mapsto \mathcal{P}ic_{C/k}(T) = \frac{\mathrm{Pic}(C \times_k T)}{p_T^* \mathrm{Pic}(T)}$$

donde $p_T : C \times_k T \to T$ es la proyección natural. Sabemos que el grupo de Picard esta en correspondencia biyectiva con respecto a las clases de equivalencia de haces invertibles. Definimos el subfuntor caracterizado para cada A una k-álgebra arbitraria y $C_A = C \times_k \mathrm{Spec}(A)$, entonces se define:

$$P^0_{C/k}(A) = \frac{\mathrm{Pic}^0(C_A)}{p_A^* \mathrm{Pic}(A)}$$

Proposición 4.2 *Si C admite un punto racional sobre k, el funtor $\mathcal{P}ic^0_{C/k}$ es un haz sobre el sitio $\mathbf{Sch}/k$ con la topología fppf.*

Definición 4.8 — El Jacobiano de una curva. El Jacobiano $\mathrm{Jac}(C)$ es el k-esquema en grupos que representa al subfuntor $\mathcal{P}ic^0_{C/k}$.

Proposición 4.3 *Sea k un campo de cartacteristica distinta a 2 y 3. Consideremos la curva proyectiva*

$$C : ax^3 + by^3 + cz^3 = 0$$

entonces la curva elíptica definida por

$$E : x^3 + y^3 + abcz^3 = 0$$

es el Jacobiano de C.

Sobre la clausura algebraica $\overline{K}$, la curva C y la jacobiana E son isomorfas. Fijamos el isomorfismo

$\phi : C_{\overline{K}} \to E_{\overline{K}}$ dado por el cambio de coordenadas algebraico:

$$\phi([x : y : z]) = \left[\sqrt[3]{a}x : \sqrt[3]{b}y : \frac{1}{\sqrt[3]{ab}}z\right]$$

Dados los puntos $P \in C(\overline{K})$ y $Q \in E(\overline{K})$, definimos la acción

$$\mu : C \times_K E \to C,\ (P, Q) \mapsto \mu(P, Q) = \phi^{-1}\big(\phi(P) +_E Q\big)$$

El morfismo μ es $G_{\overline{K}}$-equivariante y está definido sobre el campo base K.

Demostración. Para un K-esquema T y un T-punto $q \in E(T)$, denotamos el automorfismo de traslación inducido como:

$$\tau_q : C_T \to C_T$$

Por definición, el jacobiano $\mathrm{Jac}(C)$ es el esquema en grupos que representa al funtor. Para demostrar que $E \cong \mathrm{Jac}(C)$, debemos construir un isomorfismo functorial natural:

$$\eta : h_E \xrightarrow{\sim} \mathcal{P}ic^0_{C/K}$$

donde $h_E = \mathrm{Hom}_K(-, E)$. Para definir $\eta_T : E(T) \to \mathcal{P}ic^0_{C/K}(T)$, necesitamos asignar a cada morfismo $q : T \to E$ un haz invertible de grado 0 sobre C_T, siguiendo los siguientes paso:

- Consideramos el producto $C \times_K C$ y su subesquema diagonal cerrado $\Delta \subset C \times_K C$.
- Sea $\mathcal{I}_\Delta$ el haz de ideales que define a la diagonal. Como C es suave, Δ es un divisor de Cartier. Definimos el haz invertible universal $\mathcal{O}_{C\times C}(\Delta) = \mathcal{I}_\Delta^{-1}$. Este haz tiene grado relativo 1 respecto a ambas proyecciones.
- Dado $q \in E(T)$, formamos el morfismo de grafos asociado a su traslación:

$$\Gamma_q = (1_{C_T}, \tau_q) : C_T \to C_T \times_T C_T \cong (C \times_K C) \times_K T$$

- Hacemos el pullback:

$$\mathcal{L}_q = \Gamma_q^* \left(\mathcal{O}_{C\times C}(\Delta)\right)$$

  El haz $\mathcal{L}_q$ es un haz invertible sobre C_T de grado relativo 1 sobre T.
- Para ajustar el grado a 0, tomamos el elemento neutro $e \in E(T)$ (obtenido por cambio de base de $\mathcal{O} \in E(K)$) y construimos su respectivo haz $\mathcal{L}_e$.
- Definimos el haz torcido:

$$\mathcal{M}_q = \mathcal{L}_q \otimes \mathcal{L}_e^{-1}$$

  Como la diferencia de dos divisores relativos de grado 1 tiene grado 0, $\mathcal{M}_q$ es un haz invertible sobre C_T de grado relativo 0.

Mapeamos $q \mapsto [\mathcal{M}_q]$. Como las construcciones de haces diagonales y pullbacks conmutan con el cambio de base de T-esquemas, esta asignación define una transformación natural estricta $\eta : h_E \to \mathcal{P}ic^0_{C/K}$ en el sitio fppf.

Para probar que la transformación natural η induce un isomorfismo de esquemas, basta verificar que es un isomorfismo de haces fppf. Puesto que E y el funtor $\mathcal{P}ic^0_{C/K}$ (que sabemos a priori que está representado por una variedad abeliana lisa) son localmente de presentación finita y lisos sobre K, es suficiente y necesario demostrar que η induce un isomorfismo sobre la clausura geométrica $\overline{K}$.

Sobre $\overline{K}$, la curva $C_{\overline{K}}$ tiene puntos racionales. Fijemos un punto $P \in C(\overline{K})$. Evaluando nuestra construcción geométrica fibra a fibra, el haz $\mathcal{O}_{C\times C}(\Delta)$ se especializa a $\mathcal{O}_C(x)$ para puntos concretos. El haz relativo $\mathcal{M}_q$ evaluado en el punto $q \in E(\overline{K})$ corresponde exactamente a la clase

del divisor:

$$[\mathcal{M}_q] = [\tau_q(P)] - [P] = [P + q] - [P] \in \mathrm{Pic}^0(C_{\overline{K}})$$

Esto significa que $\eta_{\overline{K}} : E(\overline{K}) \to \mathrm{Pic}^0(C_{\overline{K}})$ es precisamente el mapeo clásico de Abel-Jacobi asociado al torsor.

Por la teoría fundamental de curvas de género 1 sobre campos algebraicamente cerrados, el mapeo $q \mapsto [P + q] - [P]$ es un isomorfismo de grupos abelianos biyectivo y un isomorfismo de variedades algebraicas. ■

El discriminante de una curva de la forma $X^3 + Y^3 + cZ^3 = 0$ es $\triangle = -27c^2$. Para $c = 60$, tenemos $\triangle = -27(60)^2$, por lo que los primos de mala reducción son 2, 3 y 5.

Tomemos el primo de buena reducción $p = 7$. Por el teorema de inyectividad, la restricción del morfismo de reducción $E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_7)$ es inyectiva (ya que $7 \nmid 2\triangle$).

Analicemos la curva reducida $\tilde{E}/\mathbb{F}_7$:

$$X^3 + Y^3 + 4Z^3 \equiv 0 \pmod 7$$

En $\mathbb{F}_7$, los cubos perfectos son $\{0, 1, -1\}$. Por lo tanto, la suma de dos cubos $X^3 + Y^3 \pmod 7$ solo puede tomar los valores $\{0, 1, 6, 2, 5\}$. Si $Z \not\equiv 0 \pmod 7$, entonces $4Z^3 \in \{4, -4\} \equiv \{4, 3\} \pmod 7$. Para que la suma sea cero, necesitaríamos que $X^3 + Y^3 \in \{3, 4\} \pmod 7$, lo cual es imposible. Por lo tanto, cualquier punto en $\tilde{E}(\mathbb{F}_7)$ debe tener $Z \equiv 0 \pmod 7$.

Si $Z = 0$, la ecuación se reduce a $X^3 + Y^3 = 0$. En el plano proyectivo $\mathbb{P}^2(\mathbb{F}_7)$, podemos asumir $X = 1$, lo que implica $Y^3 = -1$. En $\mathbb{F}_7$, las raíces cúbicas de -1 son $3, 5$ y 6.Esto nos da exactamente tres puntos en el infinito:

$$(1 : 3 : 0), \quad (1 : 5 : 0), \quad (1 : 6 : 0)$$

Concluimos que $\#\tilde{E}(\mathbb{F}_7) = 3$. Como $E(\mathbb{Q})_{\text{tors}}$ se inyecta en $\tilde{E}(\mathbb{F}_7)$, el grupo de torsión racional debe ser trivial o isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

Para descartar la 3-torsión racional, recordamos que los puntos de orden 3 en una curva cúbica coinciden con sus puntos de inflexión. Estos son los ceros del Hessiano, que para nuestra curva es proporcional a XYZ. El único punto de inflexión definido sobre $\mathbb{Q}$ es $O = (1 : -1 : 0)$. Como no hay puntos racionales afines en el Hessiano, no hay elementos racionales de orden 3. Por lo tanto, $E(\mathbb{Q})_{\text{tors}} = \{O\}$.

5. Grupos de Selmer y Tate-Shafarevich

5.1. Obstrucciones locales-globales

Definición 5.1 — Puntos de Torsión. Sea $A \in \mathbf{Ab}$ un grupo abeliano, y m un entero positivo, definimos el grupo de puntos de m-torsión como el kernel del morfismo

$$0 \to A[m] \xrightarrow{i} A \xrightarrow{m\cdot -} A$$

Sea K un cuerpo de números y $G_K = \mathrm{Gal}(\bar{K}/K)$ su grupo de Galois absoluto. Para un entero $m \geq 2$, el morfismo de multiplicación por m, denotado $[m] : E \to E$, induce una sucesión exacta corta de G_K-módulos:

$$0 \to E[m] \to E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 0$$

Al aplicar el funtor de cohomología de Galois $H^i(G_K, -)$, el cual denotamos simplemente como $H^i(K, -)$, obtenemos la sucesión exacta larga en cohomología:

$$0 \to E(K)[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} H^1(K, E[m]) \to H^1(K, E) \xrightarrow{[m]} H^1(K, E)$$

obteniendo la sucesión exacta

$$0 \to E(K)/mE(K) \xrightarrow{\delta} H^1(K, E[m]) \xrightarrow{\varphi} H^1(K, E)[m] \to 0$$

Para estudiar las obstrucciones locales-globales, consideramos las compleciones K_v para cada lugar v de K (primos finitos y el infinito). La inclusión $G_{K_v} \hookrightarrow G_K$ induce morfismos de restricción $\mathrm{res}_v : H^1(K, -) \to H^1(K_v, -)$. Definimos el **grupo de Selmer** $\mathrm{Sel}_m(E/K)$ como el subgrupo de elementos en $H^1(K, E[m])$ cuyas imágenes en $H^1(K, E)$ se anulan localmente en todas partes:

$$\mathrm{Sel}_m(E/K) = \{\xi \in H^1(K, E[m]) \colon \mathrm{res}_v(\varphi(\xi)) = 0 \in H^1(K_v, E) \text{ para todo } v\}$$

Y definimos el grupo de Tate-Shafarevich $Ш(E/K)$ como el núcleo del mapa de localización global:

$$Ш(E/K) = \ker\left(H^1(K, E) \xrightarrow{\prod \mathrm{res}_v} \prod_v H^1(K_v, E)\right)$$

Por el lema de la serpiente y la conmutatividad de los diagramas de restricción, esto induce la sucesión exacta canónica:

$$0 \to E(K)/mE(K) \to \mathrm{Sel}_m(E/K) \to Ш(E/K)[m] \to 0$$

5.2. El caso de la curva de estudio

Teorema 5.1 *Para la curva eliptica E se tiene*

- $$Sel_3(E/\mathbb{Q}) \cong Ш(E/\mathbb{Q})[3] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$
- *Cuando $p \neq 3$, se tiene $Ш(E/\mathbb{Q})[p] = 0$*

Tenemos

$$Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Demostración. Comenzamos demostrando que $E(\mathbb{Q}) = O$. Por el cálculo realizado anteriormente sabemos que

$$E(\mathbb{Q}) * \mathrm{tors} = O.$$

Por otra parte, un 2-descenso de la curva elíptica E muestra que

$$\mathrm{rank}\, E(\mathbb{Q}) = 0.$$

Por el teorema de Mordell–Weil,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q}) * \mathrm{tors},$$

donde $r = \mathrm{rank}\, E(\mathbb{Q})$. Como $r = 0$ y $E(\mathbb{Q})_{\mathrm{tors}} = O$, concluimos que

$$E(\mathbb{Q}) = O.$$

En particular,

$$E(\mathbb{Q})/3E(\mathbb{Q}) = 0.$$

"' Consideremos ahora la sucesión exacta

$$0 \to E(\mathbb{Q})/3E(\mathbb{Q}) \to \mathrm{Sel}_3(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[3] \to 0.$$

Como $E(\mathbb{Q})/3E(\mathbb{Q}) = 0$, obtenemos

$$0 \to \mathrm{Sel}_3(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[3] \to 0.$$

Por lo tanto,

$$\mathrm{Sel}_3(E/\mathbb{Q}) \cong Ш(E/\mathbb{Q})[3].$$

Para calcular este grupo se realiza un segundo descenso mediante una isogenia de grado 3. La curva E admite una isogenia racional

$$\phi : E \longrightarrow E'$$

de grado 3, junto con su isogenia dual

$$\widehat{\phi} : E' \longrightarrow E,$$

tales que

$$\widehat{\phi} \circ \phi = [3].$$

El descenso asociado a estas isogenias permite describir los elementos del grupo de Selmer mediante cociclos de Galois y condiciones locales.

En particular, el cálculo del 3-descenso para la curva E muestra que existen exactamente nueve clases que satisfacen las condiciones locales. Por tanto,

$$\#\,\mathrm{Sel}_3(E/\mathbb{Q}) = 9.$$

Como $\mathrm{Sel}_3(E/\mathbb{Q})$ es un grupo abeliano de exponente 3, es naturalmente un espacio vectorial sobre $\mathbb{F}_3$. Puesto que tiene $9 = 3^2$ elementos, su dimensión sobre $\mathbb{F}_3$ es 2. Así,

$$\mathrm{Sel}_3(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

De la identificación anterior concluimos que

$$Ш(E/\mathbb{Q})[3] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Veamos ahora que no existen componentes de 2-torsión. El mismo 2-descenso utilizado para determinar el rango de $E(\mathbb{Q})$ muestra que

$$Ш(E/\mathbb{Q})[2] = 0.$$

Para los primos $p > 3$, la curva E posee multiplicación compleja por el anillo de enteros de

$$\mathbb{Q}(\sqrt{-3}).$$

El resultado de Rubin sobre la conjetura principal para curvas elípticas con multiplicación compleja permite determinar los componentes p-primarios del grupo de Tate–Shafarevich para

los primos que no dividen el número de unidades de $\mathbb{Q}(\sqrt{-3})$. En nuestro caso, esto se aplica para todo primo $p > 3$ y da

$$Ш(E/\mathbb{Q})[p] = 0.$$

Por lo tanto, el único componente primario no trivial del grupo de Tate–Shafarevich es el correspondiente al primo 3. En consecuencia,

$$Ш(E/\mathbb{Q}) = Ш(E/\mathbb{Q})[3]$$

y obtenemos finalmente

$$\boxed{Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.}$$

■

6. Conclusión

El principio local-global proporciona una herramienta muy poderosa para estudiar la existencia de soluciones racionales a ecuaciones diofánticas. Sin embargo, el ejemplo de Selmer muestra que esta propiedad no es universal: una curva puede poseer puntos sobre todos los campos locales y, aun así, no tener ningún punto racional. Esto evidencia que la información local no siempre es suficiente para determinar la existencia de soluciones globales.

A lo largo de este trabajo se estudió este fenómeno desde una perspectiva geométrica y aritmética. La introducción de los números p-ádicos y del lema de Hensel permitió comprender la naturaleza de las condiciones locales, mientras que el estudio del jacobiano proporcionó un modo de trasladar el problema de los puntos de una curva a un objeto que posee una estructura de grupo. Esta estructura hace posible aplicar herramientas de teoría de Galois y de descenso.

En particular, el último resultado muestra cómo el estudio de los puntos racionales de una curva puede reducirse al estudio de determinados puntos racionales de su jacobiano mediante el mapa de Abel–Jacobi. En el caso de una curva que posee un punto racional, la inyección

$$C(k) \hookrightarrow J(k)$$

permite interpretar los puntos racionales de la curva dentro del grupo de puntos racionales de su jacobiano. El descenso permite entonces obtener información sobre estos últimos a partir de condiciones locales. De esta manera, el problema geométrico inicial se transforma en un problema aritmético sobre un grupo.

Este procedimiento conduce naturalmente a los grupos de Selmer y de Tate–Shafarevich. El grupo de Selmer permite reunir las clases que satisfacen las condiciones locales necesarias para provenir de un punto global, mientras que el grupo de Tate–Shafarevich mide, en cierto sentido, la obstrucción que permanece entre la información local y la global. Por tanto, estos grupos no aparecen simplemente como herramientas adicionales, sino como una respuesta natural al fallo del principio local-global.

Así, el ejemplo de Selmer deja de ser únicamente un contraejemplo al principio local-global y se convierte en la motivación para desarrollar una teoría capaz de estudiar sistemáticamente este tipo de fallos. El paso desde las curvas hacia sus jacobianos, y posteriormente hacia los grupos de Selmer y de Tate–Shafarevich, muestra cómo un problema aparentemente concreto sobre soluciones racionales puede revelar una estructura mucho más profunda en la interacción entre geometría algebraica, teoría de números y cohomología de Galois.

Referencias

[1] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction*, 2nd ed., Springer, 1997.

[2] Joe Harris, *Algebraic Geometry: A First Course*, Springer, 1992.

[3] David Mumford, *The Red Book of Varieties and Schemes: Includes the Michigan Lectures (1974) on Curves and their Jacobians*, 2nd ed., Springer, 1999.

[4] Joseph H. Silverman y John T. Tate, *Rational Points on Elliptic Curves*, 2nd ed., Springer, 2015.

[5] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, 2009.