Trabajo monográfico

El Teorema de Mazur

Camilo Gallardo

Orientador:

Gonzalo Tornaría

Maestría en Matemática
Universidad de la República
Montevideo, Uruguay

Resumen

En este trabajo de maestría se presenta una exposición del Teorema de Mazur sobre torsión racional de curvas elípticas, así como los resultados previos necesarios para comprender la prueba. Se recurre a herramientas y resultados profundos de geometría algebraica, entre ellos el modelo de Néron. Se presentan elementos de esquemas de grupos, curvas modulares y la teoría de reducción de curvas elípticas en cuerpos locales.

La extensión del cuerpo generado por los puntos $\mathbb{Q}$-racionales de N-torsión sobre $\mathbb{Q}(\zeta_N)$ va a tener una importancia particular en la prueba del teorema, siendo esencial la demostración de que, para N primo mayor a 13, ésta no tiene ramificación.

El capítulo 1 presenta el Teorema de Mazur desde tres ángulos distintos: primero en su forma original y luego en el lenguaje de las curvas modulares, y finalmente esbozando su relacion con las representaciones de Galois. En el capítulo 2 daremos una prueba del Teorema asumiendo un Lema Principal y otras hipótesis adicionales. El capítulo 3 es el más extenso y abarca tres áreas distintas: la reducción de curvas elípticas y su relación con la torsión; los esquemas de grupos, y finalmente el modelo de Néron. El capítulo 4 usa todo lo anterior para presentar las ideas de la prueba del Lema Principal. Por último, el capítulo 5 muestra algunos resultados que se han obtenido en busca de una generalización del Teorema de Mazur a cuerpos de números.

Agradecimientos:

A mis amigos y compis de casa(jistán), Martín, Iván y Paula por acompañar y brindar un espacio precioso donde existir.

A Gonzalo por la paciencia y el tiempo invertido en escuchar mis dudas y explicarme sobre curvas elípticas.

También a Alvarito por colgarse a responder en detalle cualquier pregunta sobre esquemas.

A los gurises que andan siempre en el piso 14 dándole vida. Cuando precisaba un respiro me ponía a pensar con ellos algún ejercicio de anillos o de algo que estuvieran estudiando.

Índice general

Capítulo 1

Introducción

Arrest this man, he talks in maths

Thom Yorke

1. Torsión y el Teorema de Mazur

Este trabajo va a discurrir en el contexto de curvas elípticas racionales, o bien curvas elípticas definidas sobre una extensión finita de los racionales. Se asume cierta familiaridad de parte del lector con los dos libros de Silverman (principalmente [Sil86], y para algunos temas [Sil94]). Muchas demostraciones se encuentran en dichos libros y habrá referencias frecuentes a ellos.

A modo de repaso veamos algunas definiciones básicas:

Definición 1. *Por curva de Weierstrass entendemos una curva proyectiva dada por una ecuación cúbica de la forma*

$$0 = f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

Si escribimos la ecuación en forma proyectiva,

$$\begin{aligned} 0 &= Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \\ &= F(X, Y, Z), \end{aligned}$$

encontramos una solución extra: el *punto en el infinito* $\mathcal{O} = (0 : 1 : 0)$. Esta es la única solución *no afín*, es decir con $Z = 0$.

Definición 2. *Sea $P = (X : Y : Z)$ solución de la ecuación de Weierstrass de arriba, es decir, $f(P) = 0$. Decimos que P es un punto singular de la curva si*

$$\frac{\partial}{\partial X}f(P) = \frac{\partial}{\partial Y}f(P) = \frac{\partial}{\partial Z}f(P) = 0$$

Observación 1. *El punto en el infinito es no singular:*

$$\frac{\partial}{\partial Z}f(0 : 1 : 0) = 1 \neq 0.$$

Definición 3. *Una curva elíptica es una curva de Weierstrass sin puntos singulares. Sea E una tal curva y sea K un cuerpo. Decimos que E está definida sobre K si el polinomio que la define tiene coeficientes en K. Esto se abrevia escribiendo E/K.*

Definición 4. *Sean K un cuerpo y E/K una curva elíptica. Los puntos de E con coordenadas en K se llaman puntos K-racionales. El conjunto de puntos K-racionales de E se nota $E(K)$. Cuando hablemos de los puntos de E sin referirnos a ningun cuerpo en particular, estaremos implícitamente hablando de los puntos de $E(\overline{K})$, donde $\overline{K}$ es una clausura algebraica de K previamente establecida.*

Definición 5. *Se llama cuerpo de números a toda extensión finita de $\mathbb{Q}$.*

Recordamos que una curva elíptica tiene estructura de grupo. Con esta estructura, si E y K son como antes, entonces $E(K)$ es un subgrupo de $E = E(\mathbb{C})$.

Asumamos además que K es un cuerpo de números. Entonces $E(K)$ es finitamente generado:

Teorema 1 (Mordell-Weil). *Sean K un cuerpo de números, E una curva elíptica definida sobre K. Los puntos K-racionales de E forman un subgrupo finitamente generado. Es decir,*

$$E(K) \cong \mathbb{Z}^r \oplus \left(\bigoplus_{i \in I} (\mathbb{Z}/n_i\mathbb{Z}) \right)$$

con $|I| < \infty$.

Observación 2. *Cuando $K = \mathbb{Q}$, el número r en la ecuación anterior es lo que se conoce como el rango de E.*

Distinguimos dos partes del grupo $E(K)$. Una parte *libre*, isomorfa a un producto finito de copias de $\mathbb{Z}$, y una parte *de torsión*.

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}}$$

Definición 6. *Sean E y K como antes. El subgrupo de torsión K-racional $E(K)_{tors}$ está dado por todos los puntos $P \in E(K)$ de orden finito. La torsión E_{tors}, omitiendo K, quiere decir la torsión en $E(\overline{K})$, donde $\overline{K}$ es una clausura algebraica de K previamente establecida. Dado $N \in \mathbb{N}$, se define la N-torsión $E[N]$ como el subgrupo de los puntos $P \in E_{tors}$ tales que $N \cdot P = \mathcal{O}$. La restricción de $E[N]$ a $E(K)$ se llama la N-torsión K-racional.*

Ejemplo 1. *La curva $y^2 = x^3 + 1$ tiene 6 puntos racionales:*

$$x = -1,\ y = 0 \qquad x = 0,\ y = \pm 1 \qquad x = 2,\ y = \pm 3$$

*y el **punto en el infinito** $\mathcal{O}$.*

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

En este caso $E(\mathbb{Q}) = E(\mathbb{Q})_{tors}$.

La torsión total E_{tors} es un grupo mucho más grande que su restricción a $E(K)$, siendo K un cuerpo de números. De hecho, E_{tors} no es finitamente generado. Esto es consecuencia del siguiente Teorema, cuya prueba diferimos para la siguiente sección:

TEOREMA 2. *Sea E una curva elíptica definida sobre $\mathbb{C}$. Hay un isomorfismo de grupos*

$$E(\mathbb{C}) \cong S^1 \times S^1$$

En particular, la torsión sobre $\mathbb{C}$ no es finitamente generada, pero

$$E[N] = (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$$

para todo entero $N > 0$.

Un problema interesante y difícil es determinar cuál es el grupo de torsión de una curva elíptica sobre $\mathbb{Q}$ y qué tanto cambia el grupo $E(K)_{\text{tors}}$ cuando variamos el cuerpo K. El teorema de Mazur clasifica los posibles grupos de torsión sobre $\mathbb{Q}$.

TEOREMA 3. *Sea E una curva elíptica sobre $\mathbb{Q}$ y sea Φ el subgrupo de torsión de $E(\mathbb{Q})$. Entonces Φ es isomorfo a uno de los siguientes 15 grupos:*

$\mathbb{Z}/m\mathbb{Z}$	*para* $m \leq 10$ *o* $m = 12$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$	*para* $m \leq 4$

2. Curvas modulares

2.1. El grupo modular. Recordamos brevemente la definición del grupo modular y su acción en el semiplano superior $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$.

DEFINICIÓN 7. *Dado R un anillo se define $\mathcal{M}_{2\times 2}(R)$ el anillo de matrices 2×2 con coordenadas en R y $\mathrm{GL}_2(R)$ el grupo de elementos invertibles de $\mathcal{M}_{2\times 2}(R)$. En particular nos interesa el caso $R = \mathbb{Z}$. Notar que $\mathrm{GL}_2(\mathbb{Z})$ son las matrices de $\mathcal{M}_{2\times 2}(\mathbb{Z})$ con determinante igual a ± 1. Se define el grupo modular:*

$$\mathrm{SL}_2(\mathbb{Z}) = \{M \in \mathrm{GL}_2(\mathbb{Z}) : \det(M) = 1\}$$

PROPOSICIÓN 1. *Sean $\tau \in \mathbb{H}$ y $M \in \mathrm{SL}_2(\mathbb{Z})$ dada por*

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

La aplicación

$$M \cdot \tau = \frac{a\tau + b}{c\tau + d} \tag{1}$$

define una acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{H}$.

DEMOSTRACIÓN. Consideremos el grupo más grande de las matrices invertibles con coeficientes en $\mathbb{C}$. Llamamos a este grupo $\mathrm{GL}_2(\mathbb{C})$. Notar que $\mathrm{GL}_2(\mathbb{C})$ actúa en el espacio vectorial $\mathbb{C}^2$ como el conjunto de transformaciones lineales invertibles.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} az_1 + bz_2 \\ cz_1 + dz_2 \end{bmatrix}$$

Siendo transformaciones lineales, los elementos de $\mathrm{GL}_2(\mathbb{C})$ llevan vectores colineales en vectores colineales. Además son transformaciones invertibles, por lo que ninguna lleva un vector no nulo en el origen. De esto se deduce que la acción de $\mathrm{GL}_2(\mathbb{C})$ en $\mathbb{C}^2$ se restringe a una acción en $\mathbb{C}^2 - \{(0,0)\}$, y que además induce una acción en el cociente que viene de identificar vectores colineales:

$$(\mathbb{C}^2 - \{(0,0)\})/\sim \qquad\qquad v \sim w \iff \exists \lambda \in \mathbb{C} : v = \lambda w$$

A este cociente se le llama la *recta proyectiva compleja* $\mathbb{P}^2(\mathbb{C})$.

Para calcular la acción de $\mathrm{GL}_2(\mathbb{C})$ sobre $\mathbb{P}^2(\mathbb{C})$ vamos a usar el siguiente sistema de representantes de clases de equivalencia:

$$(z_1, z_2) \sim \begin{cases} (z_1/z_2, 1) & z_2 \neq 0 \\ (1,0) & z_2 = 0 \end{cases}$$

A la clase de $(1,0)$ la notamos ∞ por convención y a la clase de $(z_1/z_2, 1)$ la identificamos con el número complejo $z_1/z_2 \in \mathbb{C}$. Considerar el mapa

$$\varphi : \mathbb{C}^2 - \{(0,0)\} \to \mathbb{C} \cup \{\infty\} \qquad\qquad (z_1, z_2) \mapsto \begin{cases} z_1/z_2 & z_2 \neq 0 \\ \infty & z_2 = 0 \end{cases}$$

Ya que φ es constante en las clases de equivalencia, induce un único mapa $\widetilde{\varphi}$ con dominio en $\mathbb{P}^2(\mathbb{C})$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathbb{C}^2 - \{(0,0)\} & & \\ \downarrow & \searrow^{\varphi} & \\ \mathbb{P}^2(\mathbb{C}) & \xrightarrow{\widetilde{\varphi}} & \mathbb{C} \cup \{\infty\} \end{array}$$

A su vez, la acción de $\mathrm{GL}_2(\mathbb{C})$ en $\mathbb{P}^2(\mathbb{C})$ induce una única acción en $\mathbb{C} \cup \{\infty\}$ de manera que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{C}) \times \mathbb{P}^2(\mathbb{C}) & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ \downarrow \widetilde{\varphi} & & \downarrow \widetilde{\varphi} \\ \mathrm{GL}_2(\mathbb{C}) \times (\mathbb{C} \cup \{\infty\}) & \longrightarrow & \mathbb{C} \cup \{\infty\} \end{array}$$

Queda como ejercicio al lector demostrar la siguiente fórmula explícita:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot (\tau) = \begin{cases} \frac{a\tau + b}{c\tau + d} & \tau \in \mathbb{C},\ c\tau + d \neq 0 \\ \infty & \tau \in \mathbb{C},\ c\tau + d = 0 \\ a/c & \tau = \infty \end{cases} \tag{2}$$

Notar que si M tiene coeficientes reales y $\tau \notin \mathbb{R}$, entonces $(c\tau + d) \neq 0$ y luego $M \cdot \tau \neq \infty$. Por lo tanto la expresión (1) representa una acción de $\mathrm{GL}_2(\mathbb{R})$ en $\mathbb{C} - \mathbb{R}$.

Veamos cómo se transforma por M la parte imaginaria de τ:

$$\begin{aligned}\Im(M\cdot\tau) &= \Im\left(\frac{a\tau+b}{c\tau+d}\right)\\ &= \Im\left((a\tau+b)\frac{c\overline{\tau}+d}{|c\tau+d|^2}\right)\\ &= \Im\left(\frac{ac|\tau|^2+ad\tau+bc\overline{\tau}+bd}{|c\tau+d|^2}\right)\\ &= \Im(\tau)\frac{ad-bc}{|c\tau+d|^2}\\ &= \Im(\tau)\frac{\det(M)}{|c\tau+d|^2}\end{aligned}$$

En particular, cuando $\det(M)>0$ esta fórmula dice que la acción por M preserva el signo de $\Im(\tau)$, es decir, lleva $\mathbb{H}$ en sí mismo. Esto prueba que (1) realmente define una acción de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$.

□

Definición 8. *Un retículo de $\mathbb{C}$ es un subgrupo aditivo generado por dos elementos linealmente independientes sobre $\mathbb{R}$. El par de generadores es entonces una base del retículo. Decimos que dos retículos Λ,Λ' son equivalentes si $\Lambda=\alpha\Lambda'$ para un $\alpha\in\mathbb{C}$. En particular todo retículo es equivalente a uno de la forma $\langle 1,\tau\rangle$ con $\Im(\tau)>0$.*

Lema 1. *Sean $\Lambda=\{\alpha,\beta\},\Lambda'=\langle\alpha',\beta'\rangle$ dos retículos.*

1. *$\Lambda'\subseteq\Lambda$ si y solo si existen $a,b,c,d\in\mathbb{Z}$ tales que*

$$\begin{aligned}\alpha' &= a\alpha+b\beta\\ \beta' &= c\alpha+d\beta\end{aligned}$$

2. *$\Lambda'=\Lambda \iff ad-bc=\pm 1$*

Demostración. La primera parte es trivial usando que α y β generan Λ como $\mathbb{Z}$-módulo. Si además vale la inclusión inversa $\Lambda\subseteq\Lambda'$, aplicamos la parte (1) en sentido contrario obteniendo una matriz con coeficientes $a',b',c',d'\in\mathbb{Z}$ de α y β como combinaciones lineales de α' y β'. Éstos deben satisfacer

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}a' & b'\\ c' & d'\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

es decir, $\begin{bmatrix}a & b\\ c & d\end{bmatrix}$ tiene una inversa con coeficientes en $\mathbb{Z}$, y esto vale si y solo si $ad-bc=\pm 1$. □

Proposición 2. *Sean $\Lambda=\langle 1,\tau\rangle,\Lambda'=\langle 1,\tau'\rangle$ dos retículos con $\tau,\tau'\in\mathbb{H}$. Entonces Λ,Λ' son equivalentes si y solo si $\tau'=M\cdot\tau$ para un $M\in\mathrm{SL}_2(\mathbb{Z})$.*

Demostración.

$$\begin{aligned}
\langle 1,\tau\rangle = \alpha\langle 1,\tau'\rangle &\iff \langle 1,\tau\rangle = \langle \alpha, \alpha\tau'\rangle \\
&\iff \begin{cases} \alpha\tau' = a\tau + b \\ \alpha = c\tau + d \end{cases}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \\
&\iff \tau' = \frac{a\tau+b}{c\tau+d}, \ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \\
&\iff \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})
\end{aligned}$$

donde la segunda equivalencia es una aplicación del Lema anterior y la última se debe a que τ y $\tau' \in \mathbb{H}$ fuerza a la matriz a tener determinante positivo.

□

Consideramos ahora el cociente de $\mathbb{C}$ por un retículo Λ. Como subgrupo, Λ actúa de manera obvia sobre $\mathbb{C}$ por la traslación $(z,\lambda) \mapsto z+\lambda$. Más precisamente consideramos el cociente de $\mathbb{C}$ por la acción de este subgrupo, identificando cada punto $z \in \mathbb{C}$ con su órbita $\{c+\lambda : \lambda \in \Lambda\}$. El espacio resultante es una superficie de Riemann compacta, y en este caso es topológicamente un toro, por lo que recibe el nombre de *toro complejo*. Resulta que los mapas holomorfos entre dos toros complejos $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ son de la forma $z+\Lambda \mapsto \alpha z + \Lambda'$ donde α es tal que $\alpha\Lambda \subseteq \Lambda'$ (ver [Mil17], capítulo 3, o bien el trabajo de grado [Gal22], Prop 2.4). En particular se tiene:

Proposición 3. *Sea $\Lambda \subseteq \mathbb{C}$ un retículo. El cociente $\mathbb{C}/\Lambda$ es una superficie de Riemann, y*

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda' \iff \Lambda \text{ y } \Lambda' \text{ son equivalentes},$$

donde el isomorfismo de la izquierda es como superficies de Riemann.

Teorema 4. *Todo toro complejo $\mathbb{C}/\Lambda$ es isomorfo a una curva elíptica compleja $E/\mathbb{C}$ mediante un isomorfismo que preserva la estructura de grupo. Recíprocamente, toda curva elíptica compleja se obtiene de esta manera para un retículo Λ.*

Demostración. Ver el trabajo de grado [Gal22], Teoremas 2.1 y 2.2. □

Ahora es inmediata una demostración del Teorema (2):

Prueba del Teorema (2): La estructura de grupo en $\mathbb{C}/\Lambda$ es la inducida por la suma en $\mathbb{C}$. Los puntos de N-torsión son por definición aquellos que sumados N veces dan la identidad. Es fácil ver que, en el toro descrito anteriormente, los puntos de N-torsión son de la forma $\frac{a}{N} + \frac{b}{N}\tau + \Lambda$, con $a, b \in \mathbb{Z}$. Obtenemos así que la N-torsión de una curva elíptica sobre $\mathbb{C}$ es isomorfa a $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Para la primera parte, notar que el mapa $\mathbb{C}/\Lambda \to S^1 \times S^1$ dado por $(x+y\tau) \mapsto (e^{2\pi i x}, e^{2\pi i y})$ es un isomorfismo de grupos ($x, y \in \mathbb{R}$). □

Definición 9. *Dado un retículo Λ denotamos $E(\Lambda)$ a una curva elíptica que es isomorfa a $\mathbb{C}/\Lambda$ mediante el teorema anterior. También usamos la notación $\Lambda_\tau = \langle 1, \tau\rangle$.*

Combinando los resultados anteriores con el Lema 2, se obtiene:

COROLARIO 1. *Las curvas elípticas $E(\Lambda_\tau)$ y $E(\Lambda_{\tau'})$ son isomorfas si y solo si existe $M \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\tau' = M \cdot \tau$.*

COROLARIO 2. *Sea $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. El mapa*

$$\Gamma \cdot \tau \mapsto E(\Lambda_\tau)$$

induce una biyección entre las Γ-órbitas de $\mathbb{H}$ y las clases de isomorfismo de curvas elípticas complejas.

DEMOSTRACIÓN. El corolario anterior implica que el mapa está bien definido, ya que dos puntos en una misma Γ-orbita dan lugar a curvas isomorfas, y también implica que el mapa es inyectivo, ya que dos curvas $E(\Lambda_\tau)$ y $E(\Lambda_{\tau'})$ están en la misma clase de isomorfismo solo si $\Gamma \cdot \tau = \Gamma \cdot \tau'$.

Sea E una curva elíptica compleja. Por el Teorema 4 existe un retículo Λ tal que $E \cong E(\Lambda)$. A su vez sabemos Λ es equivalente a $\langle 1, \tau \rangle$ para cierto $\tau \in \mathbb{H}$, y retículos equivalentes dan lugar a curvas isomorfas. Por lo tanto

$$E(\Lambda_\tau) \cong E(\Lambda) \cong E$$

y esto muestra que el mapa es sobreyectivo sobre las clases de isomorfismo de curvas elípticas. □

TEOREMA 5. *Sea $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. El espacio de Γ-órbitas de $\mathbb{H}$ tiene estructura de superficie de Riemann. Si se agrega la órbita del infinito $\Gamma \cdot \infty$ (recordar la acción en infinito (2)), la curva se vuelve compacta y es isomorfa a la esfera de Riemann.*

DEMOSTRACIÓN. Ver [Gal22] capítulo 1, sección 5. □

2.2. Conexión con la torsión. De hecho la biyección del Corolario (2) va mucho más lejos, como veremos a continuación.

DEFINICIÓN 10. *Se definen los siguientes subgrupos de $\mathrm{SL}_2(\mathbb{Z})$:*

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ mod\ N \right\},$$

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \exists\, b \in \mathbb{Z}, \gamma \equiv \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \ mod\ N \right\},$$

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \exists\, a, b, d \in \mathbb{Z}, \gamma \equiv \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \ mod\ N \right\}.$$

En particular, usamos la notación $\Gamma(1)$ para el grupo modular $\mathrm{SL}_2(\mathbb{Z})$.

*Los cocientes de $\mathbb{H}$ por estos grupos se llaman **curvas modulares** y se escriben $Y(N), Y_1(N), Y_0(N)$ respectivamente. También llamamos curvas modulares a sus compactificaciones $X(N), X_1(N), X_0(N)$, las cuales obtenemos agregando las correspondientes Γ-órbitas en el conjunto $\mathrm{SL}_2(\mathbb{Z}) \cdot \infty$.*

La razón de la palabra *curva* en el nombre hace referencia al hecho de que solo vamos a considerar la estructura de *curva algebraica*, entendiendo como tal la solución a una ecuación $F(X, Y) = 0$ con F un polinomio en $\mathbb{C}[X, Y]$.

El Teorema (2) establecía una correspondencia entre los puntos de $Y(1)$ y las clases de isomorfismo de curvas elípticas complejas. Se suele decir que los puntos de $Y(1)$ *parametrizan* dichas clases de isomorfismo. A su vez, la curva $Y(N)$ parametriza los pares $[E, \{P, Q\}]$, donde $\{P, Q\}$ es una base de la N-torsión. Los puntos de $Y_1(N)$ corresponden a curvas elípticas con un punto marcado de orden N, mientras que $Y_0(N)$ parametriza curvas elípticas con un subgrupo marcado de orden N. La demostración de estos resultados es elemental y está hecha explícita en [Gal22], Teorema 4.1.

Las curvas modulares también nos permiten simplificar el problema de existencia de una curva elíptica con un punto *racional* de N-torsión a la existencia de un punto racional específico en una curva modular correspondiente.

Por ejemplo, en el caso de la curva $X_0(N)$ el polinomio F mencionado antes puede tomarse siempre con coeficientes en $\mathbb{Q}$[1], de manera tal que los puntos racionales de $F(X, Y) = 0$ se corresponden a clases de isomorfismo de curvas elípticas sobre $\mathbb{Q}$ con un subgrupo de orden N, y la misma correspondencia se mantiene cambiando la palabra *racionales* por *K-racionales*, siendo K una extensión finita de $\mathbb{Q}$.

La existencia de un punto racional $P \in E$ de N-torsión para N primo es equivalente a la existencia de un punto racional en $X_0(N)$ asociado al par $[E, \langle P \rangle]$. Mazur usa el contrarecíproco: prueba la no existencia de puntos racionales (no cuspidales) en $X_0(N)$ para mostrar la no existencia de puntos racionales de orden N en una curva elíptica.

Volvamos al enunciado del teorema de Mazur. De acuerdo al Teorema (3) los grupos de torsión racional posibles son:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z} && \text{para } m \leq 10 \text{ o } m = 12, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} && \text{para } m \leq 4. \end{aligned}$$

Todos estos grupos son realizados como grupos de torsión de curvas elípticas racionales. Es esperable que sea así porque las curvas modulares $X_1(m)$ tienen género cero exactamente para los valores $m \leq 10$ y $m = 12$, y para estos valores de m también se puede tomar $X_1(m)$ racional. La razón es que cuando una curva racional tiene género cero, entonces la curva tiene un punto racional si y solo si tiene infinitos puntos racionales, es decir si y solo si admite una parametrización por $\mathbb{P}^1(\mathbb{Q})$. Sin embargo, una curva racional de género igual a 1 puede tener o bien infinitos o bien finitos puntos racionales, y para género 2 o más el Teorema de Faltings asegura que puede haber a lo sumo finitos puntos racionales.

La parte difícil, entonces, es mostrar que los 15 grupos son lo únicos posibles. En [Maz77a] Mazur demuestra que $X_1(13)$ no tiene puntos racionales excepto las cúspides. En el artículo [Maz77b] Mazur prueba la siguiente versión del Teorema:

TEOREMA 6. *La curva modular $X_0(N)$ no tiene puntos racionales no cuspidales para N primo mayor a* 13.

[1]Ver [Mil17] Capítulo 7: *The canonical model of $X_0(N)$ over $\mathbb{Q}$*

3. Representaciones de Galois

Una herramienta central para este trabajo y para el estudio de la torsión de curvas elípticas es la acción del grupo de Galois de una extensión de $\mathbb{Q}$ sobre dicho grupo de torsión, en particular sobre la N-torsión $E[N]$. Como describimos a continuación, la existencia de un punto racional de N-torsión se puede leer claramente en la representación de Galois.

DEFINICIÓN 11. *Notamos por E/K a una curva elíptica definida sobre el cuerpo K (dada por una ecuación de Weierestrass con coeficientes en K). La clausura algebraica de K se escribe $\overline{K}$ y está contenida en $\mathbb{C}$. Los puntos de E con coordenadas en K se llaman puntos K-racionales y el conjunto de dichos puntos se escribe $E(K)$. Por último $K(E[N])$ denota el cuerpo obtenido agregando a K las coordenadas de los puntos de N-torsión.*

DEFINICIÓN 12. *Si σ es un automorfismo de un cuerpo L y $P \in E(L)$ para una curva elíptica E, entonces $\sigma(P) = P^\sigma$ denota la acción de σ en P, definida como la acción aplicada a cada coordenada del punto.*

Sea E una curva elíptica definida sobre $\mathbb{Q}$. El grupo de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ actúa sobre la N-torsión $E[N]$ (la acción conmuta con la operación de suma de puntos, esencialmente porque ésta está definida por ecuaciones con coeficientes en $\mathbb{Q}$).

Recordemos el isomorfismo (definido sobre $\mathbb{C}$) $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Restringida a $E[N]$ la acción de cada $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ se puede representar con una matriz 2×2 con coeficientes en $\mathbb{Z}/N\mathbb{Z}$, indicando de qué manera transforma una base de N-torsión específica. Si $\{P, Q\}$ es una tal base, existen $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$ tal que

$$P^\sigma = a \cdot P + c \cdot Q$$
$$Q^\sigma = b \cdot P + d \cdot Q$$

y la representación de σ (respecto a $\{P, Q\}$) es:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Supongamos que $P \in E(\mathbb{Q})$. Esto ocurre si y solo si $P^\sigma = P$ para todo σ en el grupo de Galois, y las matrices en la representación del grupo son todas de la siguiente forma:

$$\begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix}$$

Es posible que no haya puntos racionales de N-torsión, pero que sí exista un subgrupo de orden N invariante por la acción de Galois: esto es, un subgrupo definido sobre cierta extensión intermedia de Galois $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(E[N])$. En ese caso para cierta base K-racional de N-torsión las matrices de la representación son triangulares superiores:

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

Capítulo 2

Prueba del Teorema

En este capítulo vamos a probar el Teorema de Mazur bajo ciertas hipótesis que describiremos como tres *axiomas*, y asumiendo un Lema Principal. En el capítulo 4 daremos una prueba del Lema Principal de nuevo asumiendo los tres axiomas. Siguiendo al artículo original de Mazur ([Maz77b]) vamos a intentar probar los resultados para la torsión K-racional siempre que sea posible, y en su defecto trabajaremos sobre $\mathbb{Q}$.

Alguna notación y convenciones que usaremos de aquí en adelante:

- N es un número primo.
- E es una curva elíptica definida sobre un cuerpo K. En principio $K = \mathbb{Q}$, pero muchos argumentos en la prueba de hecho valen para cuerpos más grandes y por eso los planteamos en el contexto de un cuerpo K explicitándolo cuando necesitemos usar $K = \mathbb{Q}$.
- La curva E tiene un punto K-racional P de orden N. El punto neutro es O.
- $\mu_N \subseteq \overline{K}$ es el grupo de las raíces N-ésimas de la unidad.
- Fijamos un generador ζ_N de μ_N.

1. Pairing de Weil

Recordamos que para toda curva elíptica E y todo entero positivo m el *pairing de Weil* es una función $e_m : E[m] \times E[m] \to \mu_m$, donde μ_m es el grupo multiplicativo formado por las raíces m-ésimas de la unidad. El pairing de Weil cumple varias propiedades que listamos en la siguiente proposición ([Sil86], III.8.1)

Proposición 4. *El pairing de Weil es:*

1. *Bilineal:*
$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$$
2. *Alternado:*
$$e_m(S, T) = e_m(T, S)^{-1}$$
3. *No degenerado: si $e_m(S, T) = 1$ para todo $S \in E[m]$ entonces $T = O$.*
4. *Invariante por Galois:*
$$e_m(S^\sigma, T^\sigma) = e_m(S, T)^\sigma$$
para todo $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Corolario 3. *Existen $P, Q \in E[m]$ tales que $e_m(P, Q) = \zeta_m$.*

DEMOSTRACIÓN. La imagen de e_m es un subgrupo del grupo de las raíces m-ésimas, μ_m. Todo tal subgrupo es μ_d para algún divisor d de m. Por bilinealidad,

$$e_m(S,T)^d = e_m([d]S,T).$$

El lado izquierdo es 1 porque $e_m(S,T) \in \mu_m$, y como la igualdad vale para todo $S,T \in E[m]$ y el pairing es no degenerado se tiene $[d]S = O$. Pero existe S de m-torsión que no es de d-torsión, contradiciendo lo anterior. □

OBSERVACIÓN 3. *Del corolario anterior se tiene que el pairing de Weil es sobreyectivo. En particular, si P es un punto racional de m-torsión entonces hay una sucesión exacta de módulos de Galois:*

$$0 \to \mathbb{Z}/m\mathbb{Z} \to E[m] \to \mu_m \to 0$$

La primera flecha es la inclusión $\langle P \rangle \subseteq E[m]$. La segunda flecha es el mapa $Q \mapsto e_m(P,Q)$. Esta observación será importante en el capítulo 4.

COROLARIO 4. *Sean P,Q dos puntos de m-torsión cualesquiera, y sean $a,b,c,d \in \mathbb{Z}/m\mathbb{Z}$.*

$$e_m(aP + cQ, bP + dQ) = e_m(P,Q)^{ad-bc}$$

DEMOSTRACIÓN. Directo de expandir por linealidad y del hecho de que e_m es alternada. □

COROLARIO 5. *$\{P,Q\}$ es una base de la m-torsión si y solo si $e_m(P,Q)$ es una raíz primitiva m-ésima de la unidad.*

DEMOSTRACIÓN. Sea $\{P,Q\}$ una base de $E[m]$. El corolario (4) implica que la imagen de e_m es generada por $e_m(P,Q)$, y el corolario (3) muestra que dicha imagen es todo μ_m, lo cual no sería posible a menos que el generador $e_m(P,Q)$ fuera una raíz m-ésima primitiva.

Para todo par de puntos $\{P',Q'\}$ en $E[m]$ considero la matriz que lleva $\{P,Q\}$ en $\{P',Q'\}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$P' = aP + bQ$$
$$Q' = cP + dQ$$

El par $\{P',Q'\}$ es una base si y solo si la matriz es invertible módulo m, y de nuevo aplicando el corolario (4) esto es si y solo si $e_m(P',Q')$ es $e_m(P,Q)^k$ para un k coprimo com m, si y solo si $e_m(P,Q)$ y $e_m(P',Q')$ tienen el mismo orden en μ_m, pero $e_m(P,Q)$ es raiz primitiva, i.e., tiene orden maximal en μ_m.

□

2. χ^j-extensiones

Vamos a asumir que E tiene un punto K-racional P de orden N. Podemos extender $\{P\}$ a una base de N-torsión agregando un punto Q.

PROPOSICIÓN 5. *En la base $\{P, Q\}$ el grupo $\mathrm{Gal}(\overline{K}/K)$ tiene la siguiente representación como automorfismo de $E[N]$:*

$$\tau \mapsto \begin{bmatrix} 1 & * \\ 0 & \chi(\tau) \end{bmatrix}$$

donde $\chi : \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/N\mathbb{Z})^\times$ es el carácter estándar, tal que

$$\tau(\zeta_N) = \zeta^{\chi(\tau)}$$

para todo $\tau \in \mathrm{Gal}(\overline{K}/K)$, y $*$ simboliza un coeficiente que también depende de τ (de aquí en más escribiremos solo χ en vez de $\chi(\tau)$ ya que la dependencia en τ es clara).

DEMOSTRACIÓN. Se deduce del corolario (4) y de la siguiente cuenta:

$$\zeta_N^{\chi(\tau)} = \zeta_N^\tau = e_N(P, Q)^\tau = e_N(P^\tau, Q^\tau) = \zeta_N^{\det(\tau)}$$

donde $\det(\tau) = \chi(\tau)$ es el determinante de la matriz asociada a τ. □

Por último llamaremos L la extensión generada por los puntos de N-torsión de E. Es fácil ver que la extensión L/K es Galois.

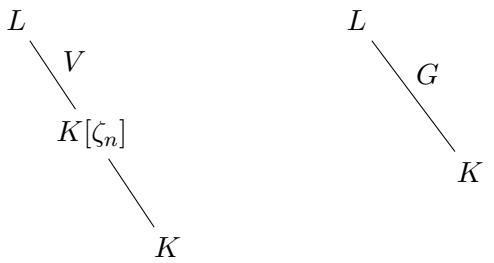
PROPOSICIÓN 6. *L contiene a $K[\zeta_n]$*

DEMOSTRACIÓN. Es equivalente a la inclusión de grupos $\mathrm{Gal}(\overline{K}/L) \subseteq \mathrm{Gal}(\overline{K}/K[\zeta_N])$. Sea $\sigma \in \mathrm{Gal}(\overline{K}/L)$, de modo que σ fija toda la N-torsión. Sean $Q_1, Q_2 \in E[N]$ tales que el pairing de Weil $e_N(Q_1, Q_2)$ es la raíz N-ésima de la unidad ζ_N, como en (3). Recordamos que el pairing de Weil conmuta con la acción de Galois, por lo tanto:

$$\zeta_N = e_N(Q_1, Q_2) = e_N(Q_1^\sigma, Q_2^\sigma) = e_N(Q_1, Q_2)^\sigma = \zeta_N^\sigma$$

Entonces σ fija ζ_N, es decir $\sigma \in \mathrm{Gal}(K[\zeta_N]/K)$. □

Tenemos las siguientes extensiones, donde $V = \mathrm{Gal}(L/K[\zeta_N])$ y $G = \mathrm{Gal}(L/K)$:



Notar que G actúa por conjugación en V. Esto es evidente porque la extensión correspondiente $K[\zeta_N]/K$ es de Galois, entonces V es subgrupo normal de G (G lleva $K[\zeta_N]$ en sí mismo y V fija este cuerpo por definición, luego $\tau\sigma\tau^{-1}$ también lo fija).

Sea $\{P, Q\}$ una base de N-torsión como antes, con P un punto K-racional de orden N. El grupo V fija el punto K-racional y también fija el pairing de Weil:

$$e_N(P,Q) = e_N(P,Q)^\sigma = e_N(P^\sigma, Q^\sigma) = e_N(P, Q^\sigma)$$

$$e_N(P, Q^\sigma - Q) = 1 \implies Q^\sigma - Q \in \langle P \rangle$$

Por lo tanto tenemos

$$Q^\sigma - Q = \alpha P$$

para un α que depende de σ.

Proposición 7. *Sea $\sigma \in V$.*

1. *La función*

$$E[N] \to E[N]$$
$$R \mapsto R^\sigma - R$$

   es un homomorfismo de grupos y se restringe a un homomorfismo entre los subgrupos cíclicos $\langle Q \rangle \to \langle P \rangle$.
2. *Sea ψ_σ el homomorfismo $\langle Q \rangle \to \langle P \rangle$ de la parte anterior. Entonces la asociación*

$$V \to \mathrm{Hom}(\langle Q \rangle, \langle P \rangle)$$

$$\sigma \mapsto \psi_\sigma$$

   es un homomorfismo inyectivo.

Demostración.

1. La acción de Galois conmuta con la operación de grupo, por lo tanto:
$$(R_1 + R_2)^\sigma - (R_1 + R_2) = (R_1^\sigma - R_1) + (R_2^\sigma - R_2)$$
   Además vimos que $Q^\sigma - Q = \alpha P \in \langle P \rangle$ para cierto α. Luego para todo múltiplo mQ se tiene
$$(mQ)^\sigma - (mQ) = m(Q^\sigma - Q) = m\alpha P \in \langle P \rangle$$
2. Sea τ otro elemento de V, y sea $\beta \in \mathbb{Z}/N\mathbb{Z}$ tal que
$$Q^\tau - Q = \beta P$$
   Recordar que P es K-racional, por lo tanto $P^\tau = P = P^\sigma$. En particular para todo $Q' \in \langle Q \rangle$ se tiene que $\psi_\tau(Q') = Q^\tau - Q$ es fijo por τ.

$$\begin{aligned}\psi_{\sigma\tau}(Q) &= Q^{\sigma\tau} - Q \\ &= (Q^\tau)^\sigma - Q \\ &= (Q^\tau)^\sigma - Q^\sigma + Q^\sigma - Q \\ &= (Q^\tau - Q)^\sigma + Q^\sigma - Q \\ &= (Q^\tau - Q) + (Q^\sigma - Q) \\ &= \psi_\tau(Q) + \psi_\sigma(Q)\end{aligned}$$

Como ψ_σ, ψ_τ son homomorfismos, la igualdad vale para todo múltiplo de Q. Esto muestra que $\tau \mapsto \psi_\tau$ es un homomorfismo. Que dicho mapa es inyectivo se deduce de las siguientes equivalencias:

$$\begin{aligned}\psi_\tau = 0 &\iff \psi_\tau(Q) - Q = 0 \\ &\iff Q^\tau = Q \\ &\iff (mQ)^\tau = mQ \ \ \forall m \in \mathbb{Z}/N\mathbb{Z} \\ &\iff \tau \text{ fija la } N\text{-torsión} \\ &\iff \tau = 1\end{aligned}$$

□

Corolario 6. *V es abeliano y es un $\mathbb{Z}/N\mathbb{Z}$-módulo.*

Demostración. El grupo de homomorfismos $\mathrm{Hom}(\langle Q\rangle, \langle P\rangle)$ es abeliano y para cada $g \in \mathrm{Hom}(\langle Q\rangle, \langle P\rangle)$ se tiene $N \cdot g = 0$, ya que su codominio es un grupo de orden N. Por la parte (2) de la proposición anterior V es isomorfo a un subgrupo de $\mathrm{Hom}(\langle Q\rangle, \langle P\rangle)$. □

Observación 4. *Como V es abeliano, actúa trivialmente sobre sí mismo, es decir que la acción de G en V induce una acción de $G/V \cong \mathrm{Gal}(K[\zeta_N]/K)$ en V.*

2.1. Acción de G en la N-torsión. Para todo $\sigma \in V$ vimos que $Q^\sigma = \alpha P + Q$ (α depende de σ) y la acción de σ en la N-torsión se representa en la base $\{P, Q\}$ con la siguiente matriz:

$$\sigma = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$$

Más en general, vimos que la acción de $\tau \in G$ en la N-torsión está dada por:

$$\tau = \begin{bmatrix} 1 & * \\ 0 & \chi \end{bmatrix}$$

Calculamos ahora la matriz asociada al conjugado $\tau\sigma\tau^{-1}$:

$$\begin{aligned}
&\tau\cdot\sigma\cdot\tau^{-1}(Q)\\
&\qquad=\begin{bmatrix}1 & *\\ 0 & \chi\end{bmatrix}\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}\begin{bmatrix}\chi & -*\\ 0 & 1\end{bmatrix}\frac{1}{\chi}\\
&\qquad=\begin{bmatrix}1 & *\\ 0 & \chi\end{bmatrix}\begin{bmatrix}\chi & \alpha-*\\ 0 & 1\end{bmatrix}\frac{1}{\chi}\\
&\qquad=\begin{bmatrix}\chi & \alpha\\ 0 & \chi\end{bmatrix}\frac{1}{\chi}\\
&\qquad=\begin{bmatrix}1 & \alpha\chi^{-1}\\ 0 & 1\end{bmatrix}\\
&\qquad=\sigma^{\chi(\tau)^{-1}}
\end{aligned}$$

Todo σ tiene $\chi = 1$ en su representación, y se deduce nuevamente del cálculo anterior que V actúa trivialmente sobre sí mismo, como ya habíamos visto del hecho de que es abeliano.

Si usamos notación aditiva para V, la cuenta anterior se reescribe así:

$$\tau\cdot\sigma\cdot\tau^{-1} = \chi(\tau)^{-1}\cdot\sigma$$

Observación 5. *El caracter χ toma valores en $(\mathbb{Z}/N\mathbb{Z})^\times$, por lo que el producto $\chi(\tau)\cdot\sigma$ no tendría sentido si no supiéramos que de hecho V es un $\mathbb{Z}/N\mathbb{Z}$-módulo.*

Definición 13. *Sea L/K una extensión tal que $\zeta_N \in L$ y tal que $V = \mathrm{Gal}(L/K[\zeta_N])$ es abeliano aniquilado por N. Supongamos que la acción de $\mathrm{Gal}(K[\zeta_N]/K)$ por conjugación es dada por multiplicar por el caracter χ elevado a la j.*

$$\tau\cdot\sigma\cdot\tau^{-1} = \chi(\tau)^j\cdot\sigma$$

Entonces decimos que L/K es una χ^j-extensión.

3. El Lema Principal

Sea E/K una curva elíptica. Recordemos semi-formalmente que un endomorfismo de E es una función $E \to E$ con imagen densa, dada por cocientes de polinomios, la cual respeta la estructura de grupo (las definiciones precisas se encuentran en [Sut13], Lecture 4). Cuando los polinomios mencionados tiene coeficientes en K se dice que el endomorfismo está *definido sobre K*.

Definición 14. *Sea E/K una curva elíptica. Se dice que E tiene multiplicación compleja sobre K si existe un endomorfismo de E definido sobre K que no es la multiplicación por un entero $R \mapsto n\cdot R$ para $n \in \mathbb{Z}$.*

Veremos que el Teorema de Mazur es una consecuencia relativamente inmediata del siguiente Lema Principal:

Lema 2 (Lema Principal).

1. *$L/K[\zeta_N]$ es totalmente no ramificada.*
2. *E no es una curva con multiplicación compleja definida sobre K.*

3.1. Tres Axiomas. Más adelante vamos a probar el Lema Principal asumiendo tres Axiomas:

1. Sea $d = [K : \mathbb{Q}]$. Entonces $N > 1 + 3^d + 2 \cdot 3^{d/2}$.
2. Existe un morfismo no constante definido sobre $\mathbb{Q}$:

$$f : X_0(N) \to A$$

donde A es una variedad abeliana, tal que
   a) Si 0, ∞ son las cúspides de $X_0(N)$, entonces $f(0) \neq f(\infty)$.
   b) El grupo de Mordell-Weil $A(K)$ es finito.
3. No existen χ^{-1}-extensiones totalmente no ramificadas de $K[\zeta_N]$.

Observación 6. *En el caso $K = \mathbb{Q}$, la variedad A del axioma 2 se puede construir como un cociente del jacobiano de $X_0(N)$. Esto lo prueba Mazur en el artículo Modular Curves and the Eisenstein Ideal [Maz77a].*

Observación 7. *El axioma 3 se cumple cuando $K = \mathbb{Q}$ debido a un teorema que relaciona los números pares de Bernoulli ($B_2 = 1/6, B_4 = 1/30$, ...) con las χ^j-extensiones. Explícitamente, se deduce de aplicar el siguiente teorema con $k = 1$ y $j = -1 = 1 - 2k$.*

Teorema 7 (Herbrand-Kummer). *Si B_{2k} es una unidad N-ádica, con $2 \leq 2k < N - 1$. Sea $j = 1 - 2k$ módulo $N - 1$. Entonces no existen χ^j-extensiones no triviales de $\mathbb{Q}(\zeta_N)$.*

4. Más lemas

Lema 3. *Supongamos que el cuerpo generado por la N-torsión, $K(E[N])$, es igual a $K[\zeta_N]$, y sea P un punto K-racional de orden N. Entonces hay un isomorfismo de módulos de Galois:*

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mu_N$$

Demostración. Sea $Q \in E[N]$ tal que $\{P, Q\}$ es base de N-torsión. Podemos asumir $e_N(P, Q) = \zeta_N$ (de lo contrario, tomar un múltiplo adecuado de Q).

Por hipótesis, $\mathrm{Gal}(K(E[N])/K) = \mathrm{Gal}(K(\zeta_N)/K)$ es cíclico con un generador σ.
Según la Proposición (5), la representación matricial de σ es:

$$\begin{bmatrix} 1 & r \\ 0 & \chi \end{bmatrix}$$

para algún r entero definido módulo N.

Distinguimos dos casos:

Caso 1: $\chi(\sigma) = 1$

En este caso σ es la identidad y la extensión $K(\zeta_N)/K$ es trivial. La N-torsión es K racional y es el módulo constante $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, el cual es igual a $\mathbb{Z}/N\mathbb{Z} \times \mu_N$ como $\mathrm{Gal}(\overline{K}/K)$-módulo porque $\zeta_N \in K$.

Caso 2: $\chi(\sigma) \neq 1$

En este caso la matriz anterior tiene dos valores propios distintos, $\{1, \chi(\sigma)\}$. El punto $Q' = \frac{r}{\chi(\sigma)-1}P + Q$ (la división es módulo N) es un vector propio asociado a $\chi(\sigma)$. Es decir,

$$(Q')^\sigma = \chi(\sigma) \cdot Q'.$$

La matriz de σ respecto a la base $\{P, Q'\}$ es ahora

$$\begin{bmatrix} 1 & 0 \\ 0 & \chi \end{bmatrix}$$

y como σ genera el grupo $\mathrm{Gal}(K(E[N])/K) = \mathrm{Gal}(K(\zeta_N)/K)$, la acción de este grupo en la N-torsión queda determinada por la matriz diagonal anterior. Esto implica $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mu_N$.

□

Observación 8. *En la demostración anterior distinguimos dos casos de acuerdo a si la extension $K[\zeta_N]/K$ era trivial o no, pero de hecho sabemos que no puede serlo. El axioma 1 implica que $N - 1 = [\mathbb{Q}(\zeta_N) : \mathbb{Q}]$ es mayor a $d = [K : \mathbb{Q}]$, por lo que K no puede contener una raíz N-ésima de la unidad.*

A continuación citamos un teorema básico cuya demostración se encuentra en [Ser68], en la sección IV.1.4. En el capítulo siguiente vamos a dar una definición rigurosa de *reducción*, pero por ahora alcanza con tener en mente que una curva elíptica se puede considerar *módulo p* para todo primo p, y la reducción es *mala* o *buena* dependiendo de si la curva obtenida es singular o no respectivamente.

Proposición 8 (Teorema de Shafarevich). *Sea S un subconjunto finito de (ideales) primos en el anillo de enteros $\mathcal{O}_K$ de un cuerpo K. Existen finitas clases de isomorfismo de curvas elípticas sobre K con buena reducción en los primos fuera de S.*

Lema 4. *Si E es una curva elíptica con buena buena reducción en p y E' es isógena a E, entonces E' tiene buena reducción en p.*

Demostración. Es un resultado elemental de la teoría de isogenias. Una buena referencia es [Ser68], IV.1.3. □

Lema 5. *Sea E una curva elíptica definida sobre un cuerpo K y sea $C \subset E$ un subgrupo finito invariante por $\mathrm{Gal}(\overline{K}/K)$. Existe una única curva elíptica E' y una isogenia $\phi : E \to E'$, ambas definidas sobre K, tal que $\ker(\phi) = C$.*

Demostración. Ver [Sil86], Capítulo III, Proposición 4.12 y las observaciones inmediatamente después. □

Lema 6. *Sea $\varphi : E \to E'$ una isogenia de curvas elípticas, con E y E' definidas sobre un cuerpo K. Si cualquiera de las dos curvas es un curva de multiplicación compleja entonces la otra también lo es.*

Demostración. La prueba es sencilla y se encuentra en las notas de Sutherland, [Sut13], Lecture 23, Teorema 23.1. De hecho Sutherland muestra algo más fuerte asumiendo que la isogenia tiene grado primo, pero no lo vamos a necesitar. □

5. Prueba Teorema de Mazur usando el Lema Principal

Procedemos a la prueba del teorema. Vamos a asumir la existencia de una curva elíptica E definida sobre K con un punto K-racional de orden N. Suponiendo que valen los tres axiomas anteriores vamos a deducir que tal curva no puede existir.

Prueba del Teorema: Como la χ^{-1}-extensión $L/K[\zeta_N]$ es no ramificada, es trivial por el axioma 3. Por el Lema 3,

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mu_N$$

y podemos pasar al cociente $E' = E/\mu_N$.

Notamos que:

1. E' es una curva elíptica definida sobre K según el lema 5.
2. La imagen de P en E' es nuevamente un punto K-racional de orden N.

Como la curva E' cumple las mismas hipótesis que E, se aplica el Lema Principal una vez más. Así, obtenemos una sucesión de curvas elípticas:

$$E \to E' \to E'' \ldots \to E^{(j)} \to \ldots$$

Cada curva es la imagen de la anterior por una N-isogenia.

El Lema 4 implica que todas las curvas $E, E', ..., E^{(n)}, ...$ tienen *buena reducción* en un mismo conjunto de primos de K. Alcanza con tomar el conjunto de primos de buena reducción de cualquiera de las curvas, el cual tiene complemento finito. Entonces podemos aplicar el Teorema de Shafarevich (Proposición 8), el cual implica que entre las curvas $E^{(j)}$ solo hay representadas finitas clases de equivalencia de curvas elípticas sobre K. Por lo tanto, para cierto par $l < m$, se tiene $E^{(l)} \cong E^{(m)}$, y podemos asumir que la composición de isogenias

$$E^{(l)} \to E^{(l+1)} \to \ldots \to E^{(m-1)} \to E^{(m)}$$

es (a menos de isomorfismo) un endomorfismo $\alpha \in \mathrm{End}(E^{(l)})$.

Cada isogenia $\pi : E^{(j)} \to E^{(j+1)}$ tiene grado $N = |\ker(\pi)|$. Se deduce que $\alpha : E^{(l)} \to E^{(m)} \cong E^{(l)}$ tiene grado una potencia de N. Supongamos que la isogenia es la multiplicación por un entero. Entonces necesariamente $\alpha = [N^r]$ para alguna potencia N^r de N. Esto daría una contradicción, ya que el punto P no pertenece $\ker(\alpha)$ y sin embargo $[N^r] \cdot P = O$. Se deduce que α no es escalar ($\alpha \notin \mathbb{Z} \subseteq \mathrm{End}(E^{(l)})$), es decir que la curva $E^{(l)}$ tiene multiplicación compleja. La curva original, E, es isógena a $E^{(l)}$, y por lo tanto el Lema 6 implica que E tiene multiplicación compleja, contradiciendo la parte b) del Lema Principal.

□

Mazur hace la siguiente observación:

Observación 9. *En el argumento anterior se usó la parte a) del Lema Principal para mostrar que E es una curva con multiplicación compleja sobre K. Como no hay curvas con multiplicación compleja sobre $\mathbb{Q}$, el caso $K = \mathbb{Q}$ se obtiene solamente de la parte a).*

Capítulo 3

Algunos resultados preliminares

El objetivo más importante de este capítulo es introducir el Modelo de Néron. Para ello necesitamos definir rigurosamente un concepto que mencionamos en los dos capítulos anteriores: la *reducción* de una curva elíptica en un primo. La sección 1.3 trata la curva de Tate y su correspondiente teorema de uniformización. Esta sección no es esencial para este capítulo pero sí juega un papel importante en el capítulo 4.

En la sección 2 damos una introducción "amigable" a la teoría de esquemas, seguido de los esquemas de grupos, y presentamos un par de ejemplos.

Finalmente enunciamos algunas propiedades del modelo de Néron de una curva elíptica.

1. Reducción de curvas, cuerpos locales

1.1. Singularidades. Dada una curva elíptica con ecuación

$$0 = f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

habíamos visto que los puntos singulares se encuentran en el *plano afín* $Z \neq 0$, y satisfacen:

$$\frac{\partial}{\partial x}f(P) = 0 = \frac{\partial}{\partial y}f(P)$$

Si $P = (x_0, y_0)$ es singular, la expansión de Taylor de f en P no tiene término lineal:

$$f(x,y) = [(y-y_0) - \alpha(x-x_0)][(y-y_0) - \beta(x-x_0)] - (x-x_0)^3$$

Cuando $\alpha \neq \beta$ el punto P es un *nodo*, y la curva $f(x,y) = 0$ tiene dos tangentes distintas en P. Si $\alpha = \beta$ el punto P es una *cúspide*. Es decir que para distinguir si P es un nodo o una cúspide hace falta saber si es nulo o no el discriminante de la forma cuadrática en la expansión de Taylor anterior.

Usando que un punto singular (x_0, y_0) es afín, siempre podemos trasladarlo al origen $(0,0)$ mediante el cambio de variables

$$x = x' + x_0, \qquad\qquad y = y' + y_0.$$

De esta manera obtenemos

$$f(x,y) = (y - \alpha x)(y - \beta x) - x^3 = y^2 + a_1xy - a_2x^2 - x^3$$

a menos de un isomorfismo.

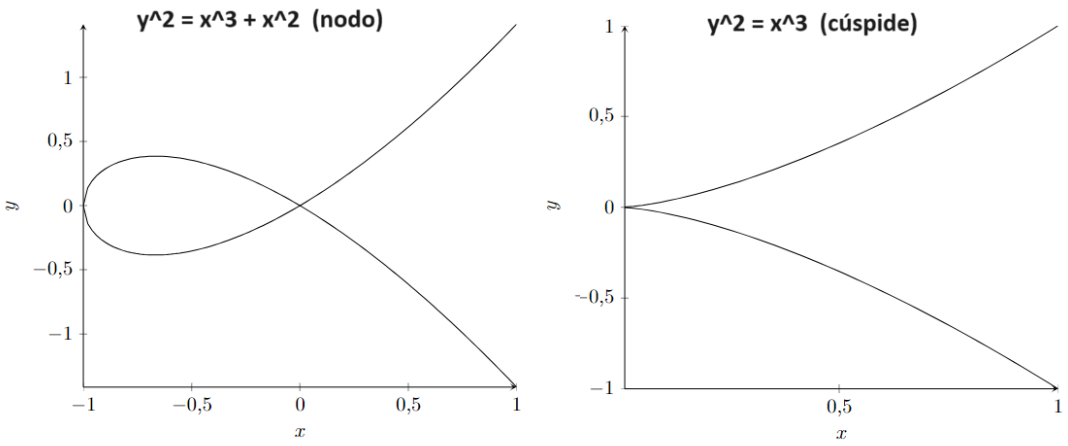


FIGURA 1. Tipos de singularidad nodo y cúspide

El discriminante de la parte cuadrática es

$$\mathrm{Disc}(y^2 + a_1xy - a_2x^2) = a_1^2 - 4a_2$$

e indica el tipo de singularidad.

En este caso, el cuadrado del discriminante coincide con una cantidad importante que llamamos c_4, la cual está definida de la siguiente manera:

$$c_4 = (a_1^2 - 4a_2)^2 - 24(2a_4 + a_1a_3)$$

Como esta cantidad es invariante por cambios de variable del tipo $x = x' + x_0$, $y = y' + y_0$, obtenemos que siempre indica el tipo de singularidad de una ecuación de Weierstrass, siempre que ésta tenga un punto singular, sin que sea necesario asumir que el punto es el origen. Otra cantidad importante es el *discriminante de la curva*, Δ. Una curva tiene puntos singulares si y solo si $\Delta = 0$.

Cuando la característica del cuerpo sobre el cual está definida la curva es distinta de 2 y 3, un cambio de coordenadas lineal convierte la ecuación de Weierstrass en

$$y^2 = x^3 + Ax + B$$

y a su vez el discriminante adquiere una expresión bastante compacta:

$$\Delta = -16(4A^3 + 27B^2)$$

Por último, existe a lo sumo un solo punto singular (una cúbica irreducible en $\mathbb{P}^2(k)$ tiene a lo sumo un punto singular con coordenadas en k).

La discusión anterior sobre los tipos de singularidad queda resumida en:

PROPOSICIÓN 9 (Silverman III.1.4). *Una curva de Weierstrass se puede clasificar de la siguiente forma:*

1. *Es no singular si* $\Delta \neq 0$.
2. *Tiene un nodo si* $\Delta = 0$ *y* $c_4 \neq 0$.
3. *Tiene una cúspide si* $\Delta = c_4 = 0$.

Aún cuando la curva es singular, los puntos no singulares de E, denotados E_{ns}, siguen formando un grupo con el producto usual. De hecho, este grupo es isomorfo al cuerpo base como grupo multiplicativo o bien como grupo aditivo.

PROPOSICIÓN 10. *Sea E una curva elíptica dada por una ecuación de Weierstrass con discriminante $\Delta = 0$, de modo que tiene un punto singular S.*

1. *Suponer que S es un nodo ($c_4 \neq 0$) y sean*

$$y = \alpha_1 x + \beta_1 \qquad\qquad y = \alpha_2 x + \beta_2$$

las tangentes de E en S.
El mapa

$$\begin{aligned} E_{ns} &\mapsto \overline{K}^{\times} \\ y &\mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2} \end{aligned}$$

es un isomorfismo de grupos.
2. *Suponer que S es una cúspide ($c_4 = 0$) y sea*

$$y = ax + b$$

la tangente a E en S.
El mapa

$$E_{ns} \to \overline{K}^{+} \qquad\qquad (x, y) \mapsto \frac{x - x(S)}{y - ax - b}$$

es un isomorfismo.

DEMOSTRACIÓN. Ver [Sil86] Proposición III.2.5. □

OBSERVACIÓN 10. *Notar que los isomorfismos de la proposición anterior están definidos o bien sobre k en el caso 2, o bien sobre una extensión cuadrática de k en el caso 1.*

1.2. Reducción y Torsión. Dada una curva elíptica E definida sobre $\mathbb{Q}$, hay una forma de *reducirla* sobre cualquier primo $p \in \mathbb{Z}$, obteniendo una curva de Weierstrass sobre el cuerpo residual $\mathbb{F}_p$. Esta curva puede ser singular o no, dependiendo de si la reducción en $\mathbb{F}_p$ del discriminante Δ es cero o no. Si la curva reducida es no singular, decimos que E tiene *buena reducción* en p, y de lo contrario decimos que tiene *mala*

reducción en p. Dentro de la mala reducción se distinguen dos casos segun la proposición (10): cuando S es un nodo la reducción es *multiplicativa* y de lo contrario es *aditiva*.

Al reducir solo nos interesa el comportamiento *local* de la curva en el primo p, por lo que bien podemos asumir que p es el único primo del anillo de enteros del cuerpo. En el ejemplo anterior, podríamos haber considerado los números p-ádicos $\mathbb{Q}_p$, cuyo anillo de enteros $\mathbb{Z}_p$ tiene a p como único primo. Los p-ádicos y sus extensiones finitas se llaman *cuerpos locales*. Generalmente es más fácil demostrar resultados locales en cuerpos locales, ya que éstos son mucho más sencillos de manejar, por ejemplo al trabajar con series de potencias. Por eso de aquí en más los resultados sobre reducción en un primo se presentan en el contexto de un cuerpo local K con:

- Valuación v
- Anillo de enteros $R = \{x \in K : v(x) > 0\}$
- Ideal maximal $M = \{x \in R : v(x) > 0\}$
- Cuerpo residual $k \cong R/M$

DEFINICIÓN 15. *En lo que respecta a este trabajo vamos a entender por cuerpo local a o bien los p-ádicos $\mathbb{Q}_p$ o bien a una extensión finita de $\mathbb{Q}_p$.*

Sea E una curva elíptica definida sobre un cuerpo local K. Suponiendo que E tiene ecuación de Weierstrass

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

entonces el cambio de variable $(x, y) = (x'u^2, y'u^3)$ cambia cada coeficiente a_i en a_i/u^i. De esta manera podemos encontrar siempre una ecuación para E con coeficientes en R, el anillo de enteros de K. El cambio de coordenadas transforma el discriminante como $\Delta \mapsto \Delta/u^{12}$

DEFINICIÓN 16. *Sea E una curva elíptica sobre un cuerpo local K y anillo de enteros R. Una ecuación de Weierstrass para E se dice **minimal** si minimiza la valuación del discriminante sujeto a la condición de tener coeficientes en R.*

Como la valuación v es discreta, es claro que existe siempre una ecuación minimal. ¿Cómo podemos saber si una ecuación es minimal? Supongamos que $v(\Delta) < 12$. Si la ecuación no fuera minimal, habría un cambio de variables que reducuría la valuación Δ, pero $v(\Delta)$ solo puede cambiar por múltiplos de 12, y obviamente la condición de que los coeficientes pertenezcan a R implica $v(\Delta) \geq 0$. Deducimos que si $v(\Delta) < 12$ la ecuación es minimal. Similarmente, como la valuación de c_4 solo cambia por múltiplos de cuatro, la condición $v(c_4) < 4$ también implica que la ecuación es minimal. El recíproco a estas condiciones solo vale para característica mayor a 3.

DEFINICIÓN 17. *Sea E/K una curva elíptica como antes, y sea $f(x, y) = 0$ una ecuación minimal de E. Al reducir los coeficientes de f módulo el ideal maximal de R obtenemos una ecuación con coeficientes en el cuerpo residual k. Esta ecuación define una curva sobre k, llamada la reducción de E. Esta curva se escribe $\widetilde{E}/k$.*

Se sabe ([Sil86] Capítulo 7, Prop 1.3) que la curva reducida es independiente de cuál ecuación minimal usamos. Reiteramos ahora la proposición (10) aplicada a la reducción de una curva elíptica ([Sil86] Capítulo VII Proposición 5.1):

PROPOSICIÓN 11. *Sea E/K una curva elíptica sobre un cuerpo local K con ecuación minimal*

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

Sea Δ el discriminante de esta ecuación y $c_4 = (a_1^2 - 4a_2)^2 - 24(2a_4 + a_1a_3)$

1. *Si $v(\Delta) = 0$, en cuyo caso $\widetilde{E}/k$ es una curva elíptica.*
2. *Si $v(\Delta) > 0$ y $v(c_4) = 0$, en cuyo caso $\widetilde{E}_{ns}$ es el grupo multiplicativo,*

$$\widetilde{E}_{ns}(\overline{k}) \cong \overline{k}^{\times}$$

3. *Si $v(\Delta) > 0$ y $v(c_4) > 0$, en cuyo caso $\widetilde{E}_{ns}$ es el grupo aditivo,*

$$\widetilde{E}_{ns}(\overline{k}) \cong \overline{k}$$

DEFINICIÓN 18. *En el primer caso se dice que E tiene buena reducción, y en caso contrario se dice que E tiene mala reducción. El caso 2 se llama reducción multiplicativa y el caso 3 se llama reducción aditiva.*

Mirar la reducción de una curva elíptica es útil cuando queremos estudiar su torsión debido a que, si la curva tiene buena reducción en p, entonces la m-torsión reduce inyectivamente para m coprimo con p. Veremos esto a continuación.

DEFINICIÓN 19. *Se define E^0 como el conjunto de puntos de E/K que reducen a puntos no singulares de $\widetilde{E}/k$, y E^1 como el subconjunto de E^0 formado por los puntos que reducen a la identidad. E^0 y E^1 son subgrupos de E.*

TEOREMA 8. *Sea E/K una curva elíptica y $m \geq 1$ un entero coprimo con* $\mathrm{car}(k)$.

1. *$E^1(K)$ no tiene puntos de m-torsión.*
2. *Si la curva reducida $\widetilde{E}/k$ es no singular entonces la reducción $E(K) \to \widetilde{E}(k)$ es inyectiva restringida a la m-torsión.*

DEMOSTRACIÓN. Ver [Sil86] VII proposición 3.1. □

EJEMPLO 2. *La curva $y^2 = x^3 + 1$ tiene torsión racional isomorfa a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, y no tiene otros puntos racionales que no sean de torsión. Su discriminante es $\Delta = -2^4 \cdot 3^3$ por lo que tiene buena reducción en 5. Efectivamente, la misma curva vista sobre el cuerpo finito $\mathbb{F}_5$ es isomorfa al grupo $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.*

EJEMPLO 3. *(Tomado de [Sil86] Capítulo VII) La curva $y^2 = x^3 + 3$ tiene discriminante $\Delta = -2^4 \cdot 3^5$, por lo tanto tiene buena reducción en p para todo primo $p > 3$. Es fácil verificar que*

$$\widetilde{E}(\mathbb{F}_5) = 6 \qquad\qquad \widetilde{E}(\mathbb{F}_7) = 13$$

Si la curva tuviera 5-torsión sobre $\mathbb{Q}$, ésta sería un subgrupo de $\widetilde{E}(\mathbb{F}_7)$, ya que la curva tiene buena reducción en 7, lo cual es imposible pues 5 no divide a 13. De forma

similar, no puede haber 7-torsión porque 7 no divide al cardinal de $\widetilde{E}(\mathbb{F}_5)$. Si $p \notin 5, 7$, la p-torsión tendría que ser un subgrupo en común de $\widetilde{E}(\mathbb{F}_5)$ y $\widetilde{E}(\mathbb{F}_7)$, lo cual es imposible. Se deduce que la curva no tiene torsión sobre $\mathbb{Q}$.

EJEMPLO 4. *La ecuación $y^2 = x^3 + 5$ es minimal sobre $\mathbb{Q}_5$, pues la valuación en 5 es 1, y luego $v(\Delta) = v(-16 \cdot 27 \cdot 5^2) = 2 < 12$. Si en vez de $\mathbb{Q}_5$ consideramos la curva sobre $\mathbb{Q}_5(5^{1/6}) = \mathbb{Q}_5(\pi)$, ahora el anillo de enteros contiene una raíz sexta de 5, que escribimos π, y la valuación en π es 1. La ecuación pasa a ser*

$$y^2 = x^3 + \pi^6$$

Con discriminante $v(-16 \cdot 27 \cdot \pi^{12}) = 12$.
Por lo tanto la ecuación no es minimal. Sin embargo el cambio de variables

$$x = x'\pi^2 \qquad\qquad y = y'\pi^3$$

transforma la ecuación en $y^2 = x^3 + 1$, que sí es minimal.

Los casos 2 y 3 se llaman de *mala reducción*. Los casos 1 y 2 también se llaman *reducción estable* y *semi-estable* respectivamente, y el 3 de *reducción inestable*. El siguiente ejemplo muestra por qué.

EJEMPLO 5. *Volvamos a la curva $y^2 = x^3+5$. Es fácil ver que tiene reducción aditiva en 5, ya que se convierte en el ejemplo canónico de nodo, $y^2 = x^3$. Sin embargo, sobre $\mathbb{Q}_5(\pi)$ la ecuación minimal tiene buena reducción.*

En general es cierto que, en una extensión de cuerpos de ramificación menor o igual a 6, la reducción aditiva pasa a ser buena reducción o por lo menos de tipo multiplicativo. De ahí el nombre *reducción inestable*. Por otro lado, los otros tipos de reducción son estables por extensiones de cuerpo.

PROPOSICIÓN 12. *(Teorema de reducción semiestable) Sea E una curva elíptica sobre un cuerpo local K.*

1. *Si K'/K es una extensión no ramificada entonces el tipo de reducción de E en K (buena, multiplicativa o aditiva) es igual que el tipo de reduccion de E en K'.*
2. *Sea K'/K una extensión finita cualquiera. Si E tiene reducción multiplicativa o buena reducción en K, el tipo de reducción es el mismo en K'.*
3. *Si E tiene reducción aditiva en K, entonces existe una extensión finita K'/K con $[K' : K] \leq 6$ y tal que E tiene reducción multiplicativa o buena reducción en K'.*

DEMOSTRACIÓN. Solo vamos a probar la parte 3, ya que tendrá especial importancia más adelante. La demostración completa está en [Sil86] Capítulo VII, Proposición 5.4.

Asumimos primero que la característica de K es distinta de 2. El resultado vale en general, pero cuando lo necesitemos va a ser solo en característica distinta de 2. Tomando una extensión de K (a lo sumo de grado 3) si es necesario, podemos escribir la ecuación en forma de Lagrange:

$$y^2 = x(x-1)(x-\lambda)$$

El discriminante Δ es igual por definición a 16 veces el discriminante del polinomio cúbico en x:

$$\Delta = 16 \cdot \lambda^2(1-\lambda)^2$$

Calculemos el término c_4. Primero expandimos la ecuación en términos de λ:

$$x(x-1)(x-\lambda) = x^3 - (1+\lambda)x^2 + \lambda x$$

Recordamos la fórmula

$$c_4 = (a_1^2 - 4a_2)^2 - 24(2a_4 + a_1a_3).$$

Ahora, reemplazando $a_1 = 0,\ a_2 = -(1+\lambda),\ a_4 = \lambda$, queda

$$\begin{aligned} c_4 &= 16(1+\lambda)^2 - 48\lambda \\ &= 16(\lambda^2 - \lambda + 1). \end{aligned}$$

Distinguimos tres casos:

1. Si $\lambda \in R$ y $\lambda \not\equiv 0, 1 \bmod M$ entonces $\Delta \notin M$ y la curva tiene buena reducción.
2. Si $\lambda \in R$ y $\lambda \equiv 0, 1 \bmod M$ entonces $\Delta \in M$, mientras que c_4 es invertible módulo M, ya que $\lambda^2 - \lambda + 1 \equiv 1 \bmod M$ y 16 es invertible módulo M (la valuación es cero en 2 pues asumimos que la característica del cuerpo es distinta de 2). Por lo tanto $v(c_4) = 0$ y deducimos que la ecuación es minimal con reducción multiplicativa.
3. Si $\lambda \notin R$, tomar el único $r > 0$ tal que $\lambda\pi^r \in R^\times$, es decir, tomar $r = -v(\lambda)$. Ahora el cambio de variables $x = \pi^{-r}x'$, $y = \pi^{-3r/2}$ nos da una ecuación con coeficientes en R:

$$(y')^2 = x'(x' - \pi^r)(x' - \pi^r\lambda)$$

Si $\pi^{r/2}$ no pertenece a K, de nuevo tomamos una extensión (a lo sumo de grado 2) que lo contenga.

Ahora $\Delta' = 16 \cdot \pi^{2r} \cdot (\pi^r\lambda)^2(\pi^r - \pi^r\lambda)^2 \in M$, y $(c_4)' = (\pi^{-r/2})^{-4}c_4 = \pi^{2r}c_4$ donde $v(c_4) = -2r$ ya que $v(\lambda) = -r$. Por lo tanto, $v((c_4)') = 0$, $(c_4)'$ es invertible y la nueva ecuación tiene reducción multiplicativa.

□

Definición 20. *Sea E/K una curva elíptica sobre el cuerpo local K. Se dice que E tiene reducción potencialmente buena si existe una extensión finita K'/K tal que E/K' tiene buena reducción.*

Observación 11. *El Teorema de reducción semiestable (12) afirma entonces que la reducción aditiva es potencialmente buena, mientras que la reducción multiplicativa no.*

Definición 21. *Para una curva elíptica E se define su j-invariante:*

$$j = (c_4)^3/\Delta$$

.

OBSERVACIÓN 12. *Se puede ver que todo cambio de coordenadas entre dos ecuaciones de Weierstrass debe ser de la forma*

$$x = u^2x' + r \qquad\qquad y = u^3y' + u^2sx' + t$$

Lo que nos concierne es el factor u. El cambio de variables transforma las cantidades ya mencionadas: $c_4 \mapsto c_4/u^4$, $\Delta \mapsto \Delta/u^{12}$. En particular, el j-invariante no cambia.

De ahí que el j-invariante realmente es un invariante por estos cambios de coordenadas.

Terminamos esta parte probando un resultado que será relevante luego en conexión con las curvas de multiplicación compleja.

PROPOSICIÓN 13. *Sea E/K una curva elíptica sobre el cuerpo local K. E tiene reducción potencialmente buena si y solo si su j-invariante es un entero algebraico de K, es decir si y solo si $j(E) \in R$.*

Utilizamos las mismas ideas de la prueba anterior:

DEMOSTRACIÓN. Supongamos que $j(E)$ es entero, i.e., $j \in R$, y extendamos K si es necesario para asegurar que K tiene una ecuación en forma de Legendre como antes. La relación $j = (c_4)^3/\Delta$ se puede escribir

$$16^3(\lambda^2 - \lambda + 1)^3 - j \cdot 16 \cdot \lambda^2(1 - \lambda)^2 = 0$$

Como j es un entero algebraico, se deduce que λ también lo es, es decir $\lambda \in R'$. Además $\lambda \not\equiv 0, 1 \bmod M$, pues de lo contrario la ecuación reduciría a $16^3 \equiv 0 \bmod M$, un absurdo pues 16 es invertible modulo M. Por la prueba de la proposición anterior, esto implica que E tiene buena reducción.

Recíprocamente, supongamos que E tiene buena reducción en la extensión K'. Entonces $\Delta' \in (R')^\times$. Ahora $j = c_4^3/\Delta \in R'$, pero sabemos que $j \in K$ ya que E está definida sobre K.

$$\implies j \in R' \cap K = R$$

□

Cerramos esta sección citando un teorema clásico que será relevante más adelante.

TEOREMA 9 (Teorema de Hasse). *Sea E una curva elíptica sobre el cuerpo finito $\mathbb{F}_p$. Entonces se tiene una cota para la cantidad de puntos de $E(\mathbb{F}_p)$:*

$$|E(\mathbb{F}_p) - (1 + p)| \leq 2 \cdot p^{1/2}$$

DEMOSTRACIÓN. Ver [Sut13], Lecture 7, Theorem 7.17. □

OBSERVACIÓN 13. *Si E/K es una curva elíptica con buena reducción en p, el Teorema de Hasse nos da una cota para la cantidad de puntos de la curva reducida:*

$$|\widetilde{E}(\mathbb{F}_p)| \leq 1 + 2 \cdot p^{1/2} + p$$

Para todo N coprimo con $\mathrm{car}(k)$, la N-torsión de E reduce inyectivamente por el Teorema (8) siendo k el cuerpo residual en p. Se deduce que E no puede tener N-torsión para un tal N mayor a $1 + 2 \cdot p^{1/2} + p$.

1.3. Curva de Tate. Recordamos el resultado fundamental ([Mil17], I.3) de que las curvas elípticas sobre $\mathbb{C}$ se corresponden con toros complejos $\mathbb{C}/\Lambda$ mediante un isomorfismo de grupos

$$E_\Lambda \cong \mathbb{C}/\Lambda$$

donde $\Lambda = \langle 1, \tau \rangle$ es un retículo que determina únicamente a E_Λ.

Si trabajamos sobre $\mathbb{Q}_p$ en vez de $\mathbb{C}$ no existe un resultado análogo, ya que $\mathbb{Q}_p$ no tiene retículos no triviales. Sin embargo, aplicando el mapa exponencial $z \mapsto e^{2\pi i z}$ podemos pasar de un retículo aditivo a uno multiplicativo,

$$\mathbb{C}/\Lambda \cong \mathbb{C}^\times / q^{\mathbb{Z}}$$

donde $q = e^{2\pi i \tau}$. Ahora, $\mathbb{Q}_p^\times$ tiene muchos subgrupos discretos, y sería deseable que éstos parametrizaran las curvas elípticas sobre $\mathbb{Q}_p$ de alguna manera. Resulta que éste es el caso, como vemos en el siguiente teorema de Tate ([Sil94], V.3.1):

Teorema 10 (Curva de Tate). *Sea K un cuerpo p-ádico con valor absoluto $|.|$ y $q \in K$ con $|q| < 1$. Definimos*

$$s_k(q) = \sum_{n \geq 1} \frac{n^k q^n}{1 - q^n} \qquad a_4(q) = -s_3(q) \qquad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}$$

1. *Las series $a_4(q)$ y $a_6(q)$ convergen en K. Se define la **curva de Tate** E_q por la ecuación*

$$y^2 + xy = x^3 + a_4(q)x + a_6(q) \tag{3}$$

2. *La curva de Tate es una curva elíptica con discriminante*

$$\Delta = q \prod (1 - q^n)^{24} \tag{4}$$

y j-invariante

$$j(E_q) = \frac{1}{q} + 744 + 196884 \cdot q + ...$$

3. *Se define el mapa $\phi : \overline{K}^\times \to E_q(\overline{K})$,*

$$\phi(u) = \begin{cases} (X_q(u), Y_q(u)) & u \notin q^{\mathbb{Z}} \\ O & u \in q^{\mathbb{Z}} \end{cases}$$

donde

$$X_q(u) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q)$$

$$Y_q(u) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} - s_2(q)$$

El mapa ϕ es un homomorfismo sobreyectivo con kernel $q^{\mathbb{Z}}$.

4. El mapa ϕ conmuta con la acción de Galois de la extensión $\overline{K}/K$, es decir

$$\phi(u^\sigma) = \phi^\sigma(u) \qquad\qquad u \in \overline{K}^\times, \sigma \in \mathrm{Gal}(\overline{K}/K).$$

En particular, para toda extensión L/K, se tiene

$$E_q(L) \cong L^\times/q^{\mathbb{Z}}$$

Observación 14. *Silverman nota de este teorema la particularidad de que ϕ conmute con la acción de Galois como un fenómeno puramente p-ádico, ya que depende del hecho de que se puede evaluar un automorfismo en las series de potencias que definen al mapa ϕ sencillamente aplicándolo término a término. El isomorfismo del caso complejo $\mathbb{C}^\times/e^{2\pi i\tau\mathbb{Z}} \cong E(\mathbb{C})$ no respeta Galois en este sentido.*

Observación 15. *Del factor q en la fórmula del discriminante (4) es evidente que $v(\Delta) > 0$, es decir la curva de Tate tiene mala reducción en q.*

Como $a_4(q) \equiv a_6(q) \equiv 0$ mod q, la curva reducida es

$$y^2 + xy = x^3,$$

la cual tiene un nodo en el origen.

Por lo tanto, E_q es una curva con reducción multiplicativa en q.

Observación 16. *La q-expansión del j-invariante de hecho puede invertirse para despejar q en función de j, siempre que $|j| > 1$. Podemos decir entonces que toda curva elíptica E sobre K con $|j(E)| > 1$ es isomorfa sobre K a una única curva de Tate por un isomorfismo que respeta la acción de Galois.*

Es claro que las series a_4 y a_6 convergen en K, dado que sus términos generales tienden a cero en valor absoluto según la norma p-ádica de K. No es tan evidente a primera vista que las series X_q, Y_q convergen, ya que se definen con $n \in \mathbb{Z}$, pero la valuación es acotada sobre todos los términos y también tiende a cero para valores grandes de n, como veremos.

Primero estudiamos el denominador en el término general de X_q. La valuación cumple la desigualdad ultramétrica para valuaciones:

$$v(a+b) \geq \min(v(a), v(b))$$

y vale la igualdad cuando $v(a) \neq v(b)$.

Cuando $v(q^n u) > 0$, $v(1-q^n u) = v(1) = 0$, y cuando $v(q^n u) < 0$ se tiene $v(1-q^n u) = v(q^n u)$.

$$v\left(\frac{q^n u}{(1-q^n u)^2}\right) = \begin{cases} v(q^n u) & v(q^n u) > 0 \\ -2v(1-q^n u) & v(q^n u) = 0 \\ -v(q^n u) & v(q^n u) < 0 \end{cases}$$

El único caso donde la valuación no es positiva es cuando $v(q^n u) = 0$, o equivalentemente cuando $q^n u \in \mathbb{Z}_p^\times$. Se deduce que hay a lo sumo un término en la serie de $X_q(u)$ con valuación no positiva. Si además tenemos $q^n u \equiv 1 \bmod \pi^r \mathbb{Z}_p$, entonces $v(1-q^n u) \geq r \geq 0$ y

$$v\left(\frac{q^n u}{(1-q^n u)^2}\right) = -2v(1-q^n u) \leq -2r \leq 0$$

Explícitamente,

$$v(q^n u) = 0 \implies v(1-q^n u) = R \geq 0 \qquad R = \text{máx}\{r \in \mathbb{Z} : q^n u \in 1 + \pi^r \mathbb{Z}_p\}$$

Por lo tanto,

$$v(X_q(u)) = \min_n v\left(\frac{q^n u}{(1-q^n u)^2}\right) = -2R$$

El número R corresponde a un subgrupo multiplicativo en la filtración

$$\mathbb{Z}_p^\times \supset 1 + \pi\mathbb{Z}_p \supset 1 + \pi^2\mathbb{Z}_p \supset 1 + \pi^3\mathbb{Z}_p \supset ...$$

considerada modulo $q^{\mathbb{Z}}$.

Es decir que si escribimos la filtración como

$$D_0 \supset D_1 \supset D_2 \supset ...$$

entonces R es el mayor entero tal que $q^{\mathbb{Z}} u \subseteq q^{\mathbb{Z}} D_R$.

Haciendo un cálculo similar para la serie de $Y_q(u)$ se tiene

$$v(X_q(u)) = -2R$$
$$v(Y_q(u)) = -3R$$

Ahora, de acuerdo a la definición de ϕ,

$$\phi(u) = (a/q^{2R}, b/q^{3R})$$

donde $a, b \in \mathbb{Z}_p^\times$.
El mismo punto en la curva proyectiva tiene expresión

$$(a/q^{2R} : b/q^{3R} : 1) \equiv (aq^R : b : q^{3R})$$

Pero cuando reducimos módulo q, este último punto es la identidad $(0:1:0)$, de modo que ϕ lleva D_1 en E_q^1.

A su vez, la imagen de $D_0 = \mathbb{Z}_p^\times/q^\mathbb{Z}$ en $E(K)$ cae justamente dentro de los puntos que reducen bien, ya que según nuestro estudio de la valuación de $X_q(u)$, $X_q(u) \not\equiv 0 \mod \pi\mathbb{Z}_p^\times$.

De hecho, se tiene algo más fuerte:

PROPOSICIÓN 14. *ϕ establece una correspondencia entre filtraciones*

$$E_q \supset E_q^0 \supset E_q^1 \longleftrightarrow K^\times/q^\mathbb{Z} \supset D_0 \supset D_1$$

donde de nuevo los conjuntos D_0 y D_1 se consideran módulo $q^\mathbb{Z}$.

2. Esquemas de grupos

2.1. Esquemas: breve introducción. Durante la prueba del Lema Principal se hará uso frecuente de *esquemas*. Éstos constituyen un objeto muy importante de la geometría algebraica y generalizan la noción de variedad algebraica. En esta parte presentamos algunas definiciones y propiedades básicas.

Recordemos primero la situación más familiar en la cual definimos una variedad algebraica afín sobre un cuerpo k algebraicamente cerrado. Dado un ideal $I \subseteq k[x_1, ..., x_n]$ se define el conjunto algebraico

$$X = V(I) = \{(x_1, ..., x_n) \in k^n : f(x_1, ..., x_n) = 0 \ \forall f \in I\}$$

Cuando I es primo el conjunto X es una *variedad afín*. Se define a su vez el correspondiente *anillo de funciones polinomiales*, o *anillo de coordenadas* de X,

$$k[X] = \frac{k[x_1, ..., x_n]}{I}$$

Este anillo es una k-álgebra, y como además I es primo, $k[X]$ es un dominio, y con esto es una *k-álgebra afín*.

El cuerpo de fracciones de $K[X]$, notado $K(X)$, se llama el *cuerpo de fracciones* de X y es intuitivamente un análogo al cuerpo de funciones meromorfas en una superficie de Riemann. Los elementos de $K(X)$ cuyo denominador no tiene raíces en X se llaman las *funciones regulares* en X, y son un análogo a las funciones holomorfas sobre una superficie de Riemann.

Los ideales maximales del anillo de funciones $k[X]$ están en biyección con los puntos de X:

$$(x_1, ..., x_n) \mapsto m_x = \langle x - x_1, ..., x - x_n\rangle \subseteq k[X]$$

A su vez los ideales primos de $k[X]$ corresponden a las subvariedades algebraicas de X:

$$J \text{ primo} \mapsto V_X(J) = \{(x_1, ..., x_n) \in X : f(x_1, ..., x_n) = 0 \ \forall f \in J\}$$

Se define la topología de Zariski en X de modo que los cerrados son los subconjuntos de la forma $V_X(J)$ con J un ideal arbitrario de $k[X]$.

Consideremos dos variedades algebraicas afines $X \subseteq k^n, Y \subseteq k^m$ con ideales correspondientes I_X, I_Y. Un morfismo $f : X \to Y$ es una m-tupla de funciones polinomiales de X, $f = (f_1(x_1, ..., x_n), ..., f_m(x_1, ...x_n))$ cuyas imágenes caen en Y. Esto puede expresarse equivalentemente como

$$g \in I_Y \implies g \circ f \in I_X$$

Esta última condición implica que $g \mapsto g \circ \phi$ induce un único homomorfismo de k-álgebras afines $k[Y] \to k[X]$, y recíprocamente todo tal homomorfismo viene de un morfismo $X \to Y$, es decir, hay una *correspondencia contravariante* entre ambos conjuntos de morfismos que se extiende a las categorías subyacentes. Sobre esto último solo es necesario tener en mente la propiedad de que a todo diagrama conmutativo entre variedades afines le corresponde un diagrama equivalente entre los anillos de coordenadas asociados, con las flechas dadas vuelta (veremos esta correspondencia en acción en esta subsección y la siguiente).

Podemos introducir la noción de *esquema* como una manera de ampliar el espacio X, agregando un punto por cada subvariedad, i.e., por cada ideal primo de $k[X]$. Más en general, partiendo de un anillo conmutativo A con unidad se define el espectro $\mathrm{Spec}(A)$ como el conjunto de los ideales primos de A. Si I es un ideal arbitrario de A, se define $V(I)$ como el conjunto de ideales primos de A que contienen a I.

La asociación $I \mapsto V(I)$ cumple las siguientes propiedades:

- Si I, J son ideales de A, $V(IJ) = V(I) \cup V(J)$
- Si (I_α) es una familia de ideales en A, $V(\sum_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$

Y en virtud de ellas se define en $\mathrm{Spec}(A)$ la topología de Zariski de modo que los $V(I)$ son los conjuntos cerrados. Si $f \in A$, se define el abierto $D(f)$ como el complemento de $V((f))$. Los abiertos $D(f)$ forman una base de la topología de $\mathrm{Spec}(A)$. Si $\mathfrak{a}$ es un ideal de A y $\mathfrak{p} \notin V(\mathfrak{a})$, existe $f \in \mathfrak{a}$ con $f \notin \mathfrak{p}$. Por lo tanto $\mathfrak{p} \in D(f)$ y $D(f) \cap V(\mathfrak{a}) = \emptyset$.

El espectro de un anillo, $\mathrm{Spec}(A)$, es un ejemplo de *esquema afín*, pero para entender la definición de esquema hace falta introducir cierta estructura extra sobre el espacio topológico, formando lo que se conoce como un *espacio anillado*. Las definiciones formales están en ([Har77] II.2). A cada abierto U de $\mathrm{Spec}(A)$ se le asocia un anillo $\mathcal{O}(U)$ que intuitivamente representa las *funciones regulares en* U. Por último, hay una definición adecuada de *morfismo de esquemas*, según la cual los morfismos de esquemas afines $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ se corresponden de manera contravariante con homomorfismos de anillos $B \to A$ ([Har77] II prop 2.3). Así, tenemos una equivalencia entre las categorías de esquemas afines y anillos conmutativos con unidad.

En lo que sigue de esta sección vamos a limitarnos a los esquemas afines.

Ejemplo 6. *Construimos el esquema* $\mathrm{Spec}(\mathbb{Z}_p)$ *sobre el anillo de los enteros p-ádicos. Como* $\mathbb{Z}_p$ *es un anillo local con ideal maximal* $\mathfrak{p} = p\mathbb{Z}_p$*, todos sus ideales son*

$$(0), \mathbb{Z}_p, \mathfrak{p}, \mathfrak{p}^2, ..., \mathfrak{p}^n, ...$$

y solo tiene dos ideales primos.

$$\mathrm{Spec}(\mathbb{Z}_p) = \{(0), \mathfrak{p}\}$$

Veamos cuales son los cerrados de la topología, es decir los conjuntos $V(\mathfrak{a})$*:*

$$\begin{aligned} V(\mathbb{Z}_p) &= \emptyset \\ V(\mathfrak{p}) &= V(\mathfrak{p}^n) = \{\mathfrak{p}\} \\ V((0)) &= \{(0), \mathfrak{p}\} \end{aligned}$$

La topología de Zariski es entonces

$$\tau = \{\emptyset, \{(0)\}, \{(0), \mathfrak{p}\}\}$$

El punto (0) *es abierto y denso, y se le llama* ***punto genérico****, mientras que* $\mathfrak{p}$ *es un punto cerrado, el* ***punto especial****.*

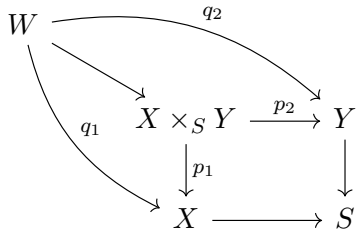
Definición 22 (S-esquema). *Sean* X, S *esquemas y* $f : X \to S$ *un morfismo de esquemas. Entonces se dice que el par* (X, f) *(o solo* X *para simplificar notación) es un* S*-esquema. Un morfismo de* S*-esquemas* $\phi : (X, f) \to (Y, g)$ *(o* S*-morfismo) es un morfismo que preserva los morfismos en* S*, es decir que hace conmutar el diagrama*

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ & \searrow^{f} & \downarrow{\scriptstyle g} \\ & & S \end{array}$$

Definición 23 (Producto fibrado). *Dados dos* S*-esquemas* X, Y*, el* ***producto fibrado*** *sobre* S*, denotado* $X \times_S Y$*, es un* S*-esquema junto con morfismos* $p_1 : X \times_S Y \to X$*,* $p_2 : X \times_S Y \to Y$ *que hace conmutar el diagrama*

$$\begin{array}{ccc} X \times_S Y & \xrightarrow{p_2} & Y \\ \downarrow{\scriptstyle p_1} & & \downarrow \\ X & \longrightarrow & S \end{array}$$

y que es universal respecto a esta propiedad. Es decir, si existe un S*-esquema* W *y morfismos de* S*-esquemas* $q_1 : W \to X$ *y* $q_2 : W \to Y$ *que también forman un cuadrado conmutativo, entonces existe un único* S*-morfismo* $W \to X \times_S Y$ *tal que el diagrama siguiente conmuta.*



OBSERVACIÓN 17. *El producto fibrado es único a menos de isomorfismo, lo cual se deduce de que satisface la propiedad universal.*

La existencia de productos fibrados se entiende como una consecuencia directa de la equivalencia de categorías anteriormente mencionada. Supongamos que $X = \mathrm{Spec}(A),\ Y = \mathrm{Spec}(B),\ S = \mathrm{Spec}(R)$. Recordar que los morfismos de X e Y en S corresponden a homomorfismos de álgebras de R en A, B. Por definicion el producto tensorial de álgebras $A \otimes_R B$ es universal respecto al siguiente diagrama

$$\begin{array}{ccc} A \otimes_R B & \longleftarrow & B \\ \uparrow & & \uparrow \\ A & \longleftarrow & R \end{array}$$

Reemplazando las algebras por sus espectros y dando vuelta las flechas obtenemos la propiedad universal del producto fibrado, por lo que se tiene

$$X \times_S Y = \mathrm{Spec}(A \otimes_R B)$$

PROPOSICIÓN 15. *Cuando $S = \mathrm{Spec}(\mathbb{Z})$ el producto fibrado sobre S es un* ***producto*** *en la categoría de los esquemas afines.*

DEMOSTRACIÓN. Lo que queremos ver es que se cumple la siguiente propiedad: para todo esquema W y par de morfismos $q_1 : W \to X$, $q_2 : W \to Y$, existe un único morfismo $W \to X \times_{\mathrm{Spec}(\mathbb{Z})} Y$ tal que el diagrama siguiente conmuta

$$\begin{array}{ccccc} & & W & & \\ & \swarrow^{q_1} & \downarrow & \searrow^{q_2} & \\ X & \xleftarrow[p_1]{} & X \times_{\mathrm{Spec}(\mathbb{Z})} Y & \xrightarrow[p_2]{} & Y \end{array}$$

La propiedad del producto fibrado requiere W, X, Y sean S-esquemas, y que q_1 y q_2 sean S-morfismos. Sin embargo, vamos a mostrar que *todo* esquema es un $\mathrm{Spec}(\mathbb{Z})$-esquema y que *todo* morfismo de esquemas es un $\mathrm{Spec}(\mathbb{Z})$-morfismo.

Para todo anillo A existe un único homomorfismo de anillos $\mathbb{Z} \to A$ (que preserve la unidad y el cero), dado por $1 \mapsto 1_A$. Es decir $\mathbb{Z}$ es un *objeto inicial* en la categoría de los anillos. Análogamente, $\mathrm{Spec}(\mathbb{Z})$ es un *objeto final* en la categoría de esquemas afines, es decir todo esquema afín X admite un único morfismo $X \to \mathrm{Spec}(\mathbb{Z})$, y todo esquema afín es un $\mathrm{Spec}(\mathbb{Z})$-esquema.

A su vez, todo morfismo de esquemas afines $X \to Y$ es un $\mathrm{Spec}(\mathbb{Z})$-morfismo. Para verificar esto último considerar el diagrama

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow & \downarrow \\ & & \mathrm{Spec}(\mathbb{Z}) \end{array}$$

y recordar que existe un único morfismo al objeto terminal $X \to \mathrm{Spec}(\mathbb{Z})$, por lo que la composición $X \to Y \to \mathrm{Spec}(\mathbb{Z})$ tiene que ser igual a este morfismo.

□

2.2. Esquemas de grupos. La siguiente sección se basa en el capítulo 5 de [CSS97].

Sea G un objeto en una categoría $\mathcal{C}$. Dado otro objeto T en $\mathcal{C}$, definimos $G(T) = \mathrm{Hom}_{\mathcal{C}}(T, G)$, el conjunto de morfismos de la categoría que van de T en G, también llamados "T-puntos de G". Supongamos ahora que podemos darle a los conjuntos $G(T)$ una estructura de grupo, de manera que para todo morfismo $f : T' \to T$, el pullback $f^* : G(T) \to G(T')$ dado por la precomposición $r \mapsto g \circ r$ es un homomorfismo de grupos. En tal caso decimos que G es un $\mathcal{C}$-grupo. Otra forma más sucinta de decir lo anterior es que un $\mathcal{C}$-grupo es un functor *contravariante* y *representable* de $\mathcal{C}$ en la categoría de grupos **Gr**.

Recordar que un functor $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ es:

- contravariante, si da vuelta las flechas, es decir para A, A' objetos en $\mathcal{A}$ y un morfismo $g : A \to A'$, la imagen es un morfismo $\mathcal{F}(g) : \mathcal{F}(A') \to \mathcal{F}(A)$.
- representable, si es (naturalmente isomorfo a) $X \mapsto \mathrm{Hom}_{\mathcal{A}}(A, X)$ para cierto A, o $X \mapsto \mathrm{Hom}_{\mathcal{A}}(X, A)$ en el caso contravariante.

Proposición 16. *Supongamos que $\mathcal{C}$ tiene productos finitos, y en particular admite un objeto final (el producto vacío) que denotamos S. G es un $\mathcal{C}$-grupo si y solo si existen morfismos*

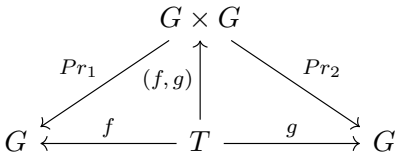
$$m : G \times G \to G \qquad Inv : G \to G \qquad \epsilon : S \to G$$

con las siguientes propiedades:

1. *$G(G)$ es un grupo con la operación*

$$f \cdot g = m \circ (f, g) \qquad f, g \in G(T) \tag{5}$$

donde (f, g) es el único mapa que hace conmutar el siguiente diagrama (i.e., es el producto cartesiano de los mapas f y g):



2. *Si $\pi : G \to S$ es el morfismo (único) de G en el objeto final S y $Id_G \in G(G)$ es el morfismo identidad, entonces*

$$\pi^*\epsilon \cdot Id_G = Id_G = Id_G \cdot \pi^*\epsilon$$

3. *el morfismo Inv cumple*

$$Inv \cdot Id_G = \pi^*\epsilon$$

Además, los morfismos m, ϵ, Inv_G están únicamente determinados por estas propiedades.

Demostración. Supongamos que G es un $\mathcal{C}$-grupo. Por definición, para todo $g : T' \to T$, el pullback

$$g^* : G(T) \to G(T') \qquad\qquad r \mapsto r \circ g$$

es un homomorfismo de grupos. Consideramos las proyecciones $\mathrm{Pr}_i : G \times G \to G$. Ahora, dados $f, g \in G(T)$ también tenemos el producto (f, g)

$$\begin{aligned} f =& Pr_1 \circ (f, g) = (f, g)^* Pr_1 \\ g =& Pr_2 \circ (f, g) = (f, g)^* Pr_2 \end{aligned}$$

Y luego

$$fg = (f, g)^* Pr_1 \cdot (f, g)^* Pr_2 = (f, g)^* (Pr_1 \cdot Pr_2) = (Pr_1 \cdot Pr_2) \circ (f, g)$$

Podemos tomar

$$m = Pr_1 \cdot Pr_2$$

Para ver que esta es la única elección posible de m, consideramos la composición con la identidad $Id_{G\times G}$.

$$\begin{aligned} m &= m \circ Id_{G\times G} \\ &= m \circ (Id_G, Id_G) \\ &= Id_G \cdot Id_G \\ &= (Pr_1 \cdot Pr_2) \circ (Id_G, Id_G) \\ &= (Pr_1 \cdot Pr_2) \circ Id_{G\times G} \\ &= Pr_1 \cdot Pr_2 \end{aligned}$$

Por otro lado, si tomamos ϵ igual al elemento neutro del grupo $G(S)$ tenemos que el pullback por π, $\pi^*\epsilon$, es el neutro de $G(G)$, y en particular

$$\pi^*\epsilon \cdot Id_G = Id_G = Id_G \cdot \pi^*\epsilon$$

El elemento Inv es simplemente el inverso de Id_G.

Recíprocamente, supongamos que tenemos mapas m, ϵ, Inv como antes. Primero notamos que la ley de grupo (5) inducida por m también define una operación binaria en los conjuntos $G(T)$. Veamos que de hecho $G(T)$ es un grupo para todo T.

Primero notar que los mapas pullback f^* respetan la operación binaria. Si $f : T' \to T$ y $r, s \in G(T)$,

$$\begin{aligned} f^*(rs) &= f^*(m \circ (r,s)) \\ &= m \circ (r,s) \circ f \\ &= m \circ (r \circ f, s \circ f) \\ &= m \circ (f^*r, f^*s) \\ &= f^*r \cdot f^*s \end{aligned}$$

Asociatividad:
Los magmas $G(T)$ son asociativos si y solo si el siguiente diagrama conmuta:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times Id} & G \times G \\ \downarrow{\scriptstyle Id \times m} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{\quad m \quad} & G \end{array}$$

Notar que implícitamente se está usando la identificación $G \times (G \times G) = G \times G \times G = (G \times G) \times G$

Por hipótesis, el producto en $G(G)$ es asociativo. La igualdad

$$(Id \cdot Id) \cdot Id = Id \cdot (Id \cdot Id)$$

Implica entonces la conmutatividad del diagrama, ya que

$$\begin{aligned} m \circ (Id \times m) &= m \circ (Id \times m) \circ (Id \times Id \times Id) \\ &= Id \cdot (Id \cdot Id) \\ &= (Id \cdot Id) \cdot Id \\ &= m \circ (m \times Id) \end{aligned}$$

(se usó que precomponer por $Id \times Id \times Id$ deja fijo cualquier morfismo con dominio $G \times G \times G$).

Ahora, como el diagrama conmuta, vale la asociatividad en general para $r, s, t \in G(T)$:

$$\begin{aligned} (rs)t = m \circ (rs, t) &= m \circ (m \times Id) \circ (r, s, t) \\ &= m \circ (Id \times m) \circ (r, s, t) \\ &= m \circ (r, st) \\ &= r(st) \end{aligned}$$

Elemento neutro:
Supongamos que $f \in G(T)$

$$\begin{aligned} f^*(\pi^*\epsilon) &= f^*\pi^*\epsilon \\ &= (\pi \circ f)^*\epsilon \\ &= (\pi_T)^*\epsilon \end{aligned}$$

donde π_T es el único morfismo de T al objeto final S. La identidad

$$\pi \circ f = \pi_T \tag{6}$$

es independiente del morfismo $f \in G(T)$, precisamente porque $\pi \circ f$ es un morfismo $T \to S$ y hay un único tal morfismo.

Verificamos que $(\pi_T)^*\epsilon$ es un elemento neutro en $G(T)$. Sea $r \in G(T)$. Usamos (6) con r en lugar de f:

$$\begin{aligned} (\pi_T)^*\epsilon \cdot r &= (r^*\pi)^*\epsilon \cdot r \\ &= r^*\pi^*\epsilon \cdot r^*Id_G \end{aligned}$$

Y ahora, usando que r^* respeta la ley de grupo y la propiedad 2,

$$\begin{aligned} (\pi_T)^*\epsilon \cdot r &= r^*(\pi^*\epsilon \cdot Id_G) \\ &= r^*Id_G \\ &= Id_G \circ r \\ &= r \end{aligned}$$

La existencia del neutro $\epsilon_T = (\pi_T)^*\epsilon$ se puede resumir diciendo que el siguiente diagrama conmuta:

$$\begin{array}{ccccc} G & \xrightarrow{Id\times\pi_T} & G \times S & \xrightarrow{Id\times\epsilon} & G \times G \\ \downarrow{\scriptstyle \pi_T\times Id} & \searrow^{Id} & & & \downarrow{\scriptstyle m} \\ S \times G & \xrightarrow{\epsilon\times Id} & G \times G & \xrightarrow{m} & G \end{array}$$

Ahora que mostramos que $\epsilon_T = (\pi_T)^*\epsilon$ es el neutro (necesariamente único) de $G(T)$ para cada T, podemos probar que para $f : U \to T$, el pullback $G(T) \to G(U)$ preserva el neutro. Notar nuevamente que el morfismo

$$f^*\pi_T : U \to S$$

no es otro que π_U, i.e., el único morfismo que va al objeto final.

$$\begin{aligned} f^*(\pi_T^*\epsilon) &= (f^*\pi_T)^*\epsilon \\ &= (\pi_U)^*\epsilon \end{aligned}$$

Hasta ahora hemos demostrado que f^* preserva elementos neutros y respeta el producto inducido por m, luego debe ser un homomorfismo de grupos para todo f, asumiendo que $G(T)$ es efectivamente un grupo para todo objeto T. Nos falta un paso para demostrar esto último:

Existencia de inversos:
Sea $g \in G(T)$. Usamos la propiedad (3) y el hecho de que g^* respeta el producto y preserva elementos neutros.

$$\begin{aligned} g \cdot g^*Inv &= g^*Id_G \cdot g^*Inv \\ &= g^*(Id_G \cdot Inv) \\ &= g^*(\pi^*\epsilon) \\ &= (\pi_T)^*\epsilon = \epsilon_T \end{aligned}$$

Luego $g^*Inv = Inv \circ g$ es el inverso de g.
La propiedad de Inv se puede resumir con el siguiente diagrama conmutativo:

$$\begin{array}{ccc} G & \xrightarrow{Inv\times Id} & G \times G \\ \downarrow{\scriptstyle Id\times Inv} & \searrow^{\epsilon_T} & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

Hay un abuso de notación: $f \times g$ quiere decir tanto el par $(f, g) : G \to G \times G$ como el morfismo *coordenada a coordenada* $G \times G \to G \times G$.

□

Definición 24. *Un R-esquema de grupos es un $\mathcal{C}$-objeto en la categoría de R-esquemas.*

Ejemplo 7. *A raíz de la equivalencia contravariante de categorías entre R-esquemas afines y R-álgebras, los morfismos m, ϵ, Inv corresponden a homomorfismos de álgebras*

$$\widetilde{m} : A \to A \otimes_R A, \qquad \tilde{\epsilon} : A \to R, \qquad \widetilde{Inv} : A \to A.$$

Dar una estructura de esquema de grupos a $\mathrm{Spec}(A)$ *es equivalente a construir los morfismos anteriores de manera que satisfagan los tres diagramas en la demostración anterior, pero con las flechas invertidas y cambiando G por A y $\times$ por $\otimes_R$.*

El mapa $\widetilde{m}$ se llama comultiplicación, $\tilde{\epsilon}$ se llama counidad o aumentación, y $\widetilde{Inv}$ la antípoda. Una R-álgebra (conmutativa) junto con estos homomorfismos es un álgebra de Hopf (conmutativa).

Supongamos que $T = \mathrm{Spec}(B)$ es un R-esquema afín. De acuerdo a la equivalencia de categorías anterior,

$$G(T) = \mathrm{Hom}_{Sch/R}(T, G) = \mathrm{Hom}_{R-alg}(A, B) = G(B)$$

Por lo tanto una forma de definir un $\mathcal{C}$-grupo sería como functor $B \mapsto G(B) = \mathrm{Hom}_{R-alg}(A, B)$, tal que $G(B)$ tenga una estructura de grupo para todo B y todo homomorfismo de álgebras $B \to C$ induzca un homomorfismo de grupos $\mathrm{Hom}_{R-alg}(A, B) \to \mathrm{Hom}_{R-alg}(A, C)$ por composición.

Sea $A = R[u]$, el álgebra libre en R generada por una variable indeterminada. Todo homomorfismo de R-álgebras $R[u] \to B$ está únicamente determinado por su valor en u. Esto quiere decir que hay una biyección

$$f \mapsto f(u) \qquad\qquad \mathrm{Hom}_{R-alg}(R[u], B) \cong B$$

la cual permite identificar a $G(B) = \mathrm{Hom}_{R-alg}(R[u], B)$ con el grupo aditivo $(B, +)$. Esta estructura de grupo es compatible con los homomorfismos de R-álgebras. Es decir, $h : B \to C$ induce por composición un homomorfismo de grupos

$$\mathrm{Hom}_{R-alg}(R[u], B) \to \mathrm{Hom}_{R-alg}(R[u], C)$$

$$\begin{aligned}(h \circ (f + g))(u) = h((f + g)(u)) &= h(f(u) + g(u)) \\ &= h \circ f(u) + h \circ g(u) \\ &= (h \circ f + h \circ g)(u)\end{aligned}$$

Así como m es el producto de las proyecciones Pr_1, Pr_2, podemos recuperar $\widetilde{m}$ como el producto en B (notación aditiva) de los elementos $\widetilde{Pr_i} : R[u] \to R[u] \otimes_R R[u]$.

$$\left.\begin{array}{l}\widetilde{Pr}_1(u) = u \otimes 1 \\ \widetilde{Pr}_2(u) = 1 \otimes u\end{array}\right\} \implies \widetilde{m} = u \otimes 1 + 1 \otimes u$$

Los homomorfismos $\tilde{\epsilon}$ y $\widetilde{Inv}$ evaluados en u dan el neutro de B y el inverso (aditivo) de u respectivamente.

$$\tilde{\epsilon}(u) = 0 \qquad\qquad \widetilde{Inv}(u) = -u$$

Obtenemos un esquema de grupos llamado el grupo aditivo, o $\mathbb{G}_a$:

$$B \mapsto \mathrm{Hom}_{R-alg}(R[u], B)$$

Ejemplo 8. *De manera similar, los homomorfismos de R-álgebras $R[u, u^{-1}] \to B$ también están determinados por su valor en u, pero este valor debe ser un elemento invertible de B:*

$$\mathrm{Hom}_{R-alg}(R[u, u^{-1}], B) = B^{\times}$$

Esta identificación nuevamente da una estructura compatible con los morfismos de R-álgebras, con

$$\widetilde{m}(u) = (u \otimes 1)(1 \otimes u) = u \otimes u \qquad \tilde{\epsilon}(u) = 1 \qquad \widetilde{Inv}(u) = u^{-1}$$

El esquema de grupos obtenido,

$$B \mapsto \mathrm{Hom}_{R-alg}(R[u, u^{-1}], B),$$

se llama el grupo multiplicativo, denotado $\mathbb{G}_m$.

Ejemplo 9. *De manera similar se define* μ_n*, las raíces n-ésimas de la unidad:*

$$B \mapsto \mathrm{Hom}_{R-alg}\left(\frac{R[u]}{u^n - 1}, B\right)$$

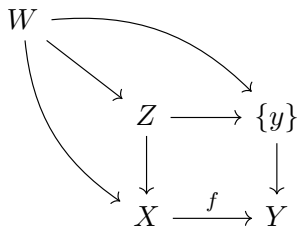
μ_n es un subgrupo del grupo multiplicativo $\mathbb{G}_m$.

3. El Teorema de Raynaud

3.1. Fibras y reducción. Anteriormente definimos el producto fibrado de esquemas afines y probamos que éste correspondía a tomar el espectro de un *producto tensorial* en la categoría de anillos. Olvidemos la estructura de esquemas por un momento y bajemos al nivel de conjuntos para entender qué objeto define un producto fibrado en esta categoría. Consideremos una función $f : X \to Y$ entre dos conjuntos, y un elemento $y \in Y$. Vamos a considerar el producto fibrado entre $f : X \to Y$ y la inclusión $\{y\} \to Y$. De acuerdo a la propiedad universal de producto fibrado, éste debería ser un conjunto Z más dos funciones $Z \to X$, $Z \to \{y\}$, formando un cuadrado conmutativo

$$\begin{array}{ccc} Z & \longrightarrow & \{y\} \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array}$$

el cual es universal, en el sentido de que todo otro cuadrado conmutativo se factoriza por Z de la siguiente manera



y la función $W \to Z$ es la *única* que hace al diagrama conmutativo.

Notar que la función $Z \to X$ es necesariamente inyectiva. Si no fuera asi, habría $z_1, z_2 \in Z$ tal que tienen la misma imagen en X. Sea ϵ la función $W \to Z$ en el diagrama anterior, y sea $\sigma : Z \to Z$ la permutación que intercambia los puntos z_1 y z_2. Es claro que si cambiamos ϵ por $\sigma \circ \epsilon$ el diagrama sigue siendo conmutativo ya que tanto ϵ como $\sigma \circ \epsilon$ compuestos con $Z \to X$ son iguales al mapa $W \to X$. Por lo tanto, si queremos que se cumpla la unicidad en la propiedad universal, $Z \to X$ debe ser inyectiva. En

consecuencia podemos asumir, a menos de un isomorfismo, que Z es un subconjunto de X y que el mapa $Z \to X$ es la inclusión i_Z. Además, a partir del diagrama es claro que Z está contenido en la preimagen de y por f. Cualquier otro subconjunto $W \subseteq f^{-1}(y)$ define un cuadrado conmutativo con la inclusión $i_W : W \to X$. Por la propiedad universal entonces existe una función $\epsilon : W \to Z$ tal que $i_W = i_Z \circ \epsilon$, y esto solo es posible si $W \subseteq Z$ y ϵ es la inclusión $W \to Z$. Es decir que en este caso el producto fibrado es el *mayor subconjunto de X cuya imagen por f es y*, i.e., la *fibra* de f en y. De ahí el nombre *producto fibrado*.

Ejemplo 10. *(Tomado de [Sil94], p.300) Sea R un anillo y $\mathfrak{p}$ un ideal maximal de R. Podemos dar a $\{\mathfrak{p}\}$ una estructura de $R/\mathfrak{p}$ esquema si al punto $\mathfrak{p}$ le asociamos como anillo el cuerpo residual $k(\mathfrak{p}) = R/\mathfrak{p}$. Nos referimos al esquema obtenido como $(\mathfrak{p}, k(\mathfrak{p}))$ o bien* $\mathrm{Spec}(k(\mathfrak{p}))$. *Notar que la reducción $R \to R/\mathfrak{p}$ induce un morfismo de esquemas* $\mathrm{Spec}(k(\mathfrak{p})) \to \mathrm{Spec}(R)$. *Si X es un R-esquema, se define la reducción módulo $\mathfrak{p}$ como*

$$X_{\mathfrak{p}} = X \times_R \{\mathfrak{p}\}.$$

En particular, $X_{\mathfrak{p}}$ es un $k(\mathfrak{p})$-esquema.

En lo que sigue vamos a explicar por qué es natural llamar a $X_{\mathfrak{p}}$ la reducción módulo $\mathfrak{p}$.

Proposición 17. *Sea E una R-álgebra. Si I es un ideal de R, entonces el mapa $(R/IR) \times E \to E/IE$ inducido por*

$$(r, x) \mapsto ax \ (mod\ IE) \qquad\qquad r \in R,\ x \in E$$

es bilineal e induce un isomorfismo

$$(R/IR) \otimes_R E \cong E/IE$$

Demostración. La prueba es rutinaria y se encuentra en [Lan02], p. 612. □

La proposición anterior implica que podemos usar el producto tensorial sobre un álgebra para *reducir coeficientes*. Por ejemplo, consideramos el anillo $\mathbb{Z}[X, Y]/(X^2 - 2Y^2 - 3)$ como $\mathbb{Z}$-álgebra y p un primo de $\mathbb{Z}$.

Entonces por la proposición

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}[X,Y]}{(X^2 - 2Y^2 - 3)} \cong \frac{\mathbb{Z}[X,Y]/(X^2 - 2Y^2 - 3)}{p \cdot (\mathbb{Z}[X,Y]/(X^2 - 2Y^2 - 3))} \cong \frac{(\mathbb{Z}/p\mathbb{Z})[X,Y]}{(X^2 - 2Y^2 - 3)}$$

El resultado es igual a considerar los polinomios con sus coeficientes reducidos módulo p. Esta nueva álgebra es igual al anillo de funciones de la curva $X^2 - 2Y^2 - 3 = 0$ considerada sobre el cuerpo finito $\mathbb{F}_p$. Dada una variedad algebraica V, llamemos $\mathrm{Aff}(V)$ al esquema afín $\mathrm{Spec}(K[V])$, el espectro del anillo de funciones regulares en V. Sea C a la curva $X^2 - 2Y^2 - 3 = 0$, hemos visto que

$$\mathrm{Spec}(\mathbb{F}_p) \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}\left(\frac{\mathbb{Z}[X,Y]}{(X^2 - 2Y^2 - 3)}\right) = \mathrm{Aff}(\widetilde{C}/\mathbb{F}_p)$$

Consideremos ahora el producto tensorial por $\mathbb{Q}$.

LEMA 7.

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[X] \cong \mathbb{Q}[X]$$

DEMOSTRACIÓN. Recordar que el producto tensorial sobre $\mathbb{Z}$ coincide con el coproducto en la categoria de anillos conmutativos ([Lan02] p. 630).

Sean entonces $f : \mathbb{Q} \to R$, $g : \mathbb{Z}[X] \to R$ dos homomorfismos de anillos, y consideremos ahora el mapa

$$\psi : \mathbb{Q}[X] \to R \qquad\qquad \psi\left(\sum \alpha_i X^i\right) = \sum f(\alpha_i) g(X^i).$$

Se verifica que ψ es un homomorfismo de anillos, el cual coincide con f restringido a $\mathbb{Q}$ y con g restringido a $\mathbb{Z}[X]$.

Además ψ está únicamente determinado por su valor en el elemento X y en $\mathbb{Q}$. □

De manera similar se puede ver que:

$$\mathbb{Q} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}[X,Y]}{(X^2 - 2Y^2 - 3)} \cong \frac{\mathbb{Q}[X,Y]}{(X^2 - 2Y^2 - 3)}$$

Entonces,

$$\mathrm{Spec}(\mathbb{Q}) \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}\left(\frac{\mathbb{Z}[X,Y]}{(X^2 - 2Y^2 - 3)}\right) = \mathrm{Aff}(C/\mathbb{Q})$$

Acabamos de probar lo siguiente: el espectro de un cuerpo residual es el esquema inducido por la curva considerada sobre dicho cuerpo. De esta manera, a partir de un $\mathrm{Spec}(\mathbb{Z}_p)$-esquema T obtenemos dos *fibras* $T_{/\mathbb{Q}} \to \mathrm{Spec}(\mathbb{Z}_p)$ y $T_{/\mathbb{F}_p} \to \mathrm{Spec}(\mathbb{Z}_p)$, los productos fibrados por $\mathrm{Spec}(\mathbb{Q})$ y $\mathrm{Spec}(\mathbb{F}_p)$ respectivamente. El primero se llama *fibra genérica* y el ultimo *fibra especial*. Nos interesa el contexto de una curva elíptica E sobre $\mathbb{Q}$, donde trabajaremos con un $\mathrm{Spec}(\mathbb{Z}_p)$-esquema $\mathcal{E}$ tal que sus dos fibras corresponden a la curva $E/\mathbb{Q}$ y a su reducción módulo el primo p.

EJEMPLO 11. *Consideremos el $\mathbb{Z}_p$-esquema de grupos μ_p (ejemplo (9)), con p primo: las raíces p-ésimas de la unidad.*

$$B \mapsto \mathrm{Hom}_{\mathbb{Z}_p - alg}\left(\frac{\mathbb{Z}_p[u]}{u^p - 1}, B\right),$$

El $\mathcal{C}$-objeto correspondiente, en la terminología de la definición (24) es el $\mathbb{Z}_p[\zeta_p]$-esquema afín

$$\mathrm{Spec}\left(\frac{\mathbb{Z}_p[u]}{u^p - 1}\right).$$

¿Cómo son sus fibras?

1. *La **fibra especial** colapsa a un solo punto, ya que* $u^p - 1 = (u-1)^p$ *en* $\mathbb{F}_p$*:*

$$\mathrm{Spec}\left(\frac{\mathbb{F}_p[u]}{u^p-1}\right) = \mathrm{Spec}\left(\frac{\mathbb{F}_p[u]}{(u-1)^p}\right) = \mathrm{Spec}\left(\frac{\mathbb{F}_p[u]}{u-1}\right) \cong \mathrm{Spec}(\mathbb{F}_p) = \{*\}$$

2. *La **fibra genérica** es disconexa porque* $u^p - 1$ *es separable sobre* $\mathbb{Q}_p$*. Como functor,* μ_p *asocia cada* $\mathbb{Q}_p$*-álgebra* A *con el grupo de homomorfismos*

$$\mathrm{Hom}_{\mathbb{Q}_p - alg}\left(\frac{\mathbb{Q}_p[u]}{u^p-1}, A\right) \cong \{a \in A : a^p = 1\}$$

.

con producto punto a punto $(f \cdot g)(x) = f(x)g(x)$*.*

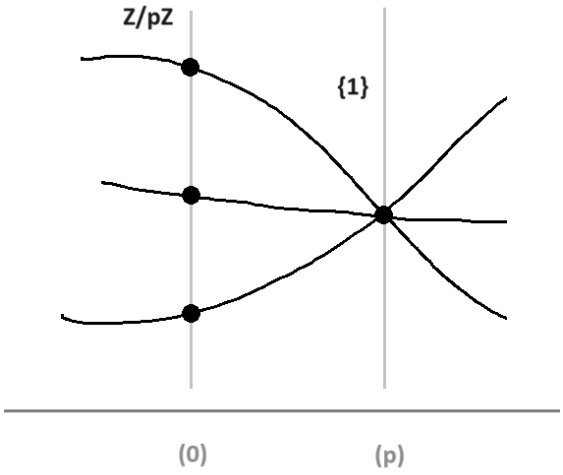


FIGURA 2. μ_p sobre $\mathrm{Spec}(\mathbb{Z}_p)$

OBSERVACIÓN 18. *Por otro lado, se puede construir un* $\mathbb{Z}_p$*-esquema constante igual a* $\mathbb{Z}/p\mathbb{Z}$*, el cual coincide con* μ_p *en la fibra genérica pero es distindo en la fibra especial. Una pregunta interesante es si bajo ciertas condiciones la fibra genérica determina totalmente a un* R*-esquema de grupos. Recordar que la fibra genérica viene del ideal* (0) *el cual es un punto denso en cualquier esquema afín* $\mathrm{Spec}(A)$ *(ver el ejemplo (6)), y tiene sentido preguntarse si una función está determinada por sus valores en un subconjunto denso del dominio. El Teorema de Raynaud da una condición suficiente de unicidad.*

OBSERVACIÓN 19. *El ejemplo anterior es un ejemplo de esquema de grupos **conexo**. El esquema de grupos constante* $(\mathbb{Z}/N\mathbb{Z})$ *es **disconexo** (ver figuras 2 y 3).*

Lo siguiente está tomado de las notas de [Sno13], *Lecture 7, "Raynaud's theorem"*.

Trabajamos con un tipo particular de esquemas de grupos llamados *finitos planos* (finite flat group schemes). Una definición rigurosa es demasiado técnica para incluir aquí, pero se puede encontrar en [CSS97], Capítulo 5.

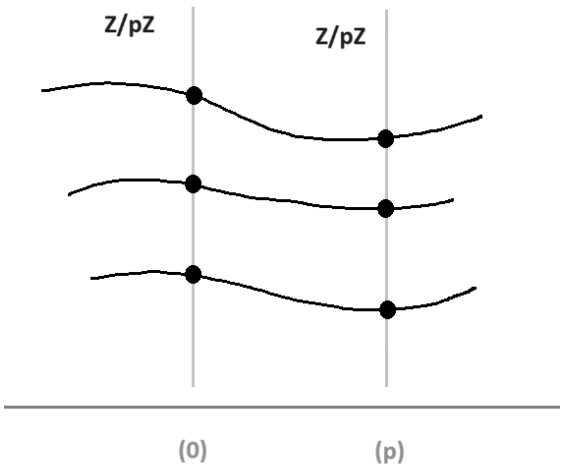


FIGURA 3. Esquema de grupos constante sobre $\mathrm{Spec}(\mathbb{Z}_p)$

DEFINICIÓN 25. *Sea R un anillo de valuación discreta con cuerpo de fracciones K de característica 0, y con cuerpo residual k de característica p (primo). Sea G_0 un K-esquema de grupos. Una prolongación de G_0 es un R-esquema de grupos G tal que su fibra genérica es G_0.*

TEOREMA 11 (Teorema de Raynaud). *En las hipótesis de la definición anterior, sea e la ramificación absoluta de p en R respectivamente. Supongamos que $e < p - 1$. Sea G un R-esquema de grupos **finito plano** conmutativo de orden una potencia de p. Entonces G es la única prolongación a menos de isomorfismo de su fibra genérica G_K.*

OBSERVACIÓN 20. *El ejemplo (11) considerado como $\mathbb{Z}_p[\zeta_p]$-esquema junto con la observación inmediatamente después muestran que la hipótesis de ramificación es necesaria en el Teorema de Raynaud. Tanto $\mathbb{Z}/p\mathbb{Z}$ como μ_p tienen fibras genéricas isomorfas sobre $\mathbb{Q}_p[\zeta_p]$ a pesar de tener distintas fibras sobre p. Sin embargo la ramificación de p en $\mathbb{Q}_p[\zeta_p]$ es $p - 1$, por lo que no satisface la hipótesis del teorema.*

4. El modelo de Néron

4.1. Introducción informal. Esta introducción se basa en el apéndice de [Sil86], (sección 15: *Néron Models and Tate's Algorithm*).

De acuerdo a lo expuesto hasta ahora, es natural pensar en un R-esquema como una familia de variedades parametrizadas por $\mathrm{Spec}(R)$. En el caso en que cada fibra es una curva se puede ver a un R-esquema como una superficie algebraica. Decimos que el R-esquema resultante es *regular* si su reducción en cada fibra no tiene puntos singulares.

Sea K un cuerpo local con anillo de enteros R y cuerpo residual k, y sea E/K una curva elíptica. Consideremos una ecuación minimal de E. Podemos considerar esta ecuación como definiendo un esquema sobre $\mathrm{Spec}(R)$. El esquema es regular si la curva tiene buena reducción en k. De lo contrario, se puede resolver la singularidad usando la

maquinaria de geometría algebraica (explosiones), hasta construir un R-esquema regular cuya fibra en k será una unión de curvas.

TEOREMA 12. *Con la notación anterior, existe un R-esquema regular $\mathcal{E}$ que cumple lo siguiente:*

1. *Sea $\mathcal{X}/R$ un R-esquema regular y sea $\varphi_K : \mathcal{X}_{/K} \to \mathcal{E}_{/K}$ un mapa racional definido sobre K. Entonces existe un único morfismo $\varphi_R : \mathcal{X}_{/R} \to \mathcal{E}_{/R}$ que extiende a φ_K.*
2. *La fibra especial $\mathcal{E}(k)$ es un grupo algebraico. Sea $\mathcal{E}^\circ(k)$ la componente conexa de la identidad en $\mathcal{E}(k)$. Entonces:*
   - $\mathcal{E}^\circ(k) \cong E_{ns}(k)$
   - $\mathcal{E}(k)/\mathcal{E}^\circ(k) \cong E(K)/E^0(K)$

DEMOSTRACIÓN. La demostración es difícil y se encuentra en [Nér80]. □

La figura 4 muestra la estructura del grupo de componentes en la fibra especial, $\mathcal{E}(k)/\mathcal{E}^\circ(k)$, de acuerdo al tipo de reducción. La primera columna indica buena reducción, la segunda es reducción multiplicativa y el resto aditiva. Una observación será muy importante en el próximo capítulo:

OBSERVACIÓN 21.

1. *Si la reducción es multiplicativa, el grupo de componentes es cíclico finito, i.e.:*
$$\mathcal{E}(k)/\mathcal{E}^\circ(k) \cong \mathbb{Z}/a\mathbb{Z}$$
para un $a \in \mathbb{N}$.
2. *Si la reducción es aditiva, el grupo de componentes tiene orden a lo sumo 4.*

Table 15.1

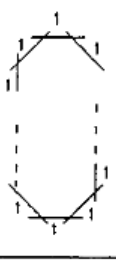
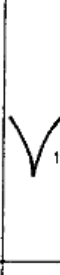
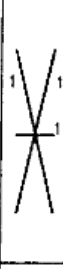
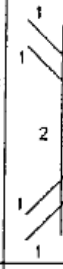
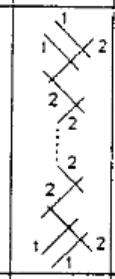
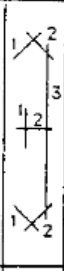
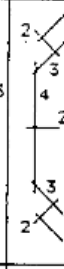
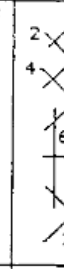
Kodaira symbol	I_0	I_υ ($\upsilon>0$)	II	III	IV	I_0	I_υ^* ($\upsilon>0$)	IV*	III*	II*
Special fiber $\overline{\mathcal{E}}$ (the numbers indicate multiplicities)										
m = number of irreducible components	1	υ	1	2	3	5	$5+\upsilon$	7	8	9
$E(K)/E_0(K) \cong \tilde{\mathcal{E}}(k)/\tilde{\mathcal{E}}^0(k)$	(0)	$\frac{\mathbb{Z}}{\upsilon\mathbb{Z}}$	(0)	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}}\times\frac{\mathbb{Z}}{2\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}}\times\frac{\mathbb{Z}}{2\mathbb{Z}}$ υ even; $\frac{\mathbb{Z}}{4\mathbb{Z}}$ υ odd	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	(0)
$\tilde{\mathcal{E}}^0(k)$	$\tilde{E}(k)$	k^*	k^+	k^+	k^+	k^+	k^+	k^+	k^+	k^+
Entries below this line are valid only for char(k) ≠ 2,3										
$ord_v(\Delta_v)$	0	υ	2	3	4	6	$6+\upsilon$	8	9	10
f_v = exponent of conductor = $ord_v(\Delta_v)+1-m$	0	1	2	2	2	2	2	2	2	2
behavior of j	$v(j)\geq 0$	$ord_v(j)=-\upsilon$	$\tilde{j}=0$	$\tilde{j}=1728$	$\tilde{j}=0$	$v(j)\geq 0$	$ord_v(j)=-\upsilon$	$\tilde{j}=0$	$\tilde{j}=1728$	$\tilde{j}=0$

FIGURA 4. Clasificación de Kodaira-Néron del grupo de componentes E/E^0 (imagen tomada de [Sil86], sección 15: *Néron Models and Tate's Algorithm*)

Capítulo 4

Prueba del Lema Principal

La demostración del Teorema de Mazur que dimos en el capítulo 2 estaba sujeta a ciertas hipótesis. Éstas eran tres Axiomas y un Lema Principal. Según mencionamos, los Axiomas se cumplen para $\mathbb{Q}$, aunque esto no es para nada trivial. Este capítulo se concentra en dar la idea de la prueba del Lema Principal a partir de los tres Axiomas. Primero veremos la parte (b), que es más fácil. Recordamos que la N-torsión de una curva elíptica es un módulo de Galois, es decir admite una acción por Galois la cual es compatible con la suma de puntos. Asumimos lo siguiente:

- $P \in E(K)$ es de orden N, un primo.
- E, K y N satisfacen los Axiomas de (3.1).

Fijamos algo de notación:

- E tiene un modelo de Néron $\mathcal{E}_{/S}$, con $S = \mathrm{Spec}(\mathcal{O}_K)$ y $\mathcal{O}_K$ el anillo de enteros de K.
- P genera un módulo de Galois $\mathbb{Z}/N\mathbb{Z} \subseteq E(K)$.
- $(\mathbb{Z}/N\mathbb{Z})_{/S}$ es el esquema de grupos constante igual a $\mathbb{Z}/N\mathbb{Z}$ en todas sus fibras.
- Usaremos tanto la notación $T_{/\,\mathrm{Spec}(R)}$ como $T_{/R}$ para decir que T es un esquema sobre $\mathrm{Spec}(R)$-esquema para un anillo R.
- Para $r \in \mathrm{Spec}(R)$ el cuerpo residual en r se nota $k(r)$.
- Llamamos $T_{/r}$ a $T \times_{\mathrm{Spec}(R)} \mathrm{Spec}(k(r))$, la fibra de T en $r \in \mathrm{Spec}(R)$.

1. Parte (b) del Lema Principal

Por la propiedad universal del modelo de Néron, la inclusión $\mathbb{Z}/N\mathbb{Z} \to E(K)$ se extiende a un morfismo

$$(\mathbb{Z}/N\mathbb{Z})_{/S} \to \mathcal{E}_{/S}$$

el cual es un isomorfismo sobre su imagen restringido a la fibra genérica $(\mathbb{Z}/N\mathbb{Z})_{/K}$.

Mediante este morfismo, $(\mathbb{Z}/N\mathbb{Z})_{/S}$ va a parar a la clausura de Zariski de $(\mathbb{Z}/N\mathbb{Z})_{/K} \subseteq \mathcal{E}_{/K}$ en $\mathcal{E}_{/S}$, la cual llamamos $G_{/S}$.

Notar que $G_{/S}$, al igual que $(\mathbb{Z}/N\mathbb{Z})_{/S}$ es una prolongación de la fibra $(\mathbb{Z}/N\mathbb{Z})_{/K}$ (se puede probar que ambos son esquemas de grupos del tipo finito plano). Según el Teorema de Raynaud (Teorema 11) hay una única tal prolongación, ya que por hipótesis tenemos $d < N - 1$, y esto fuerza a la ramificación de K sobre N a ser menor a $N - 1$.

Por lo tanto, necesariamente $G_{/S} \cong (\mathbb{Z}/N\mathbb{Z})_{/S}$ y podemos identificar ambos esquemas de grupos.

En lo que sigue asumimos que $N > 13$. Para cada $s \in S$ tenemos una fibra $(\mathbb{Z}/N\mathbb{Z})_{/s} \subset \mathcal{E}_{/s}$.

Definición 26. *Decimos que el modelo de Néron de una curva elíptica es estable (resp. semiestable o inestable) en un punto $s \in S$ si la curva tiene reducción estable (resp. semiestable o inestable) en dicho punto. Decimos que el modelo $\mathcal{E}_{/S}$ es estable (resp. semiestable) si lo es en todo punto $s \in S$.*

Lema 8. *$\mathcal{E}_{/S}$ es semiestable. Es decir, para todo $s \in S$, $\mathcal{E}_{/s}$ es o bien una curva elíptica, o bien su componente conexa principal $(\mathcal{E}_{/s})^\circ$ es de tipo multiplicativo.*

Demostración. Supongamos que $(\mathcal{E}_{/s})^\circ$ es de tipo aditivo. Por el Teorema 12 el grupo de componentes conexas para el caso de reducción aditiva tiene tamaño a lo sumo 4. Se deduce que $(\mathbb{Z}/N\mathbb{Z})_{/s}$ está contenido en $(\mathcal{E}_{/s})^\circ$. Si cualquier elemento del subgrupo estuviera en otra componente, entonces N veces ese elemento no podría caer en la componente principal ya que N es primo mayor a 4. Sin embargo la componente principal $(\mathcal{E}_{/s})^0$ es por definición la componente conexa que contiene a la identidad de E (o más precisamente a su reducción en la fibra por s).

Sea $k(s)$ el cuerpo residual asociado a s. Si la reducción es aditiva hay un isomorfismo entre la componente $(\mathcal{E}_{/s})^\circ$ y el grupo aditivo de $k(s)$. La existencia del subgrupo de orden N, $(\mathbb{Z}/N\mathbb{Z})_{/s}$ implica que la característica de $k(s)$ es el primo N.

Ahora llamemos K_s a la completación de K en s. Vamos a usar que existe una extensión K'_s/K_s con índice de ramificación relativa menor o igual a 6 (ver la Proposición (12)), tal que $E_{/K'_s}$ posee un modelo de Néron semiestable $\mathcal{E}_{/\mathcal{O}'_s}$, donde $\mathcal{O}'_s$ es el anillo de enteros de K'_s. Se deduce la existencia de un morfismo

$$E_{/\mathcal{O}'_s} \xrightarrow{\varphi} \mathcal{E}_{/\mathcal{O}'_s}$$

el cual es un isomorfismo en las fibras genéricas, por la propiedad universal de Néron de $\mathcal{E}_{/\mathcal{O}'_s}$, donde $E_{/\mathcal{O}'_s}$ denota el pullback de $E_{/S}$ a $\mathcal{O}'_s$ (para entender este paso es útil tener en mente el Ejemplo 12 más abajo).

El morfismo φ es cero en la componente principal de la fibra especial de $E_{/\mathcal{O}'_s}$, porque no hay morfismos no nulos del grupo aditivo de un cuerpo k a su grupo multiplicativo $k^\times = k - \{0\}$, o a una curva elíptica sobre el cuerpo. Esto requiere un poco de explicación: El mapa exponencial constituye un homomorfismo del entre k y $k^\times$. ¿Por qué no es esto una contradicción? La razón es que estamos considerando más que la estructura de grupo: cuando hablamos de morfismo, estamos implícitamente considerando a k y $k - \{0\}$ como variedades algebraicas (grupos algebraicos). El mapa exponencial no es un morfismo porque no tiene una expresión como función racional, es decir, no pertenece al anillo de funciones regulares. Por otro lado, un cuerpo k como variedad tiene género 0, mientras

que una curva elíptica tiene género 1. Por lo tanto no puede existir un morfismo de k en en una curva elíptica.

Hemos construido un morfismo que es cero en la fibra especial y es un isomorfismo en la fibra genérica. Su imagen es una prolongación de $(\mathbb{Z}/N\mathbb{Z})_{/K}$ en $\mathcal{E}_{/\mathcal{O}'_S}$. Otra prolongación es el esquema constante $(\mathbb{Z}/N\mathbb{Z})_{/\mathcal{O}'_S}$ tal que todas sus fibras son iguales al grupo $\mathbb{Z}/N\mathbb{Z}$. El Teorema de Raynaud dice que dicha prolongación es la única posible a menos que la ramificación sea suficientemente grande. Podemos acotar la ramificación de K'_s sobre $\mathbb{Q}$ por los grados de las extensiones $[K'_s : K_s] = 6$, $[K : \mathbb{Q}] = d$ (la completación K_s es una extensión K que no es ni finita ni algebraica, pero aún así "no tiene ramificación" sobre K, en el sentido de que preserva la valuación[1]). Luego $N - 1 > 6d$ por el axioma 1 y se aplica el Teorema de Raynaud.

Concluimos que la *única* prolongación del esquema de grupos $(\mathbb{Z}/N)_{/K'_s}$ en $\mathcal{E}_{/\mathcal{O}'_s}$ es $(\mathbb{Z}/N)_{/\mathcal{O}'_s}$, y ésta no es cero en ninguna fibra. Esto es una contradicción.

□

Ejemplo 12. *Pensar en el ejemplo $y^2 = x^3 + p$. En una extensión donde existe una raíz sexta de p, la ecuación pasa a escribirse $y^2 = x^3 + \pi^6$. Esta ecuación ya no es minimal, pero el cambio de variables $y = \pi^3 y'$, $x = \pi^2 x'$ es un isomorfismo con la curva $y^2 = x^3 + 1$, cuya ecuación sí es minimal. Por la propiedad universal del modelo de Néron, este isomorfismo se levanta a un morfismo de esquemas, el cual es un isomorfismo en las fibras genéricas.*

Lema 9. *Sea $s \in S$ un punto de característica 2 o 3. Entonces E tiene mala reducción (multiplicativa) en s, y $(\mathbb{Z}/N)_{/s} \not\subseteq (\mathcal{E}_{/s})^\circ$.*

Demostración. Sean $d = [K : \mathbb{Q}]$ y l la característica de s. El cuerpo $k(s)$ tiene cardinal menor o igual a l^d. Si E tuviera buena reducción en s, entonces la cantidad de puntos de la curva reducida $\widetilde{E}(k(s)) = (\mathcal{E}_{/s})^\circ$ sería a lo sumo $1 + l^d + 2l^{d/2}$ debido a la cota de Hasse (9). Luego el Axioma 1 hace imposible tener $\mathbb{Z}/N \subseteq \widetilde{E}(k(s)) = (\mathcal{E}_{/s})^\circ$ para $l \in \{2, 3\}$. Deducimos que E tiene mala reducción en s.

Supongamos que vale la inclusión $(\mathbb{Z}/N)_{/s} \subseteq (\mathcal{E}_{/s})^\circ$. Sabemos que E tiene mala reducción en s por lo anterior, y en particular la reducción es multiplicativa debido al Lema (8). El Teorema (10) y la observación inmediatamente posterior, sabemos que sobre una extensión cuadrática $\widetilde{k(s)}$ de $k(s)$ hay un isomorfismo $\widetilde{E}(\widetilde{k(s)})_{\mathrm{ns}} \cong \widetilde{k(s)}^\times$. Este último grupo tiene cardinal $l^{2r} - 1$ donde $r \leq d$, luego N divide a $(l^r + 1)(l^r - 1) = l^{2r} - 1$, y por ser primo divide a uno de los factores, lo cual de nuevo contradice el Axioma 1.

□

Proposición 18. *(Lema Principal, parte (b)) La curva E no tiene multiplicación compleja.*

[1]Si K es un cuerpo local con $m \in K$ y valuación v, entonces para toda extensión finita de cuerpos $L \supset K$ con ramificación e la valuación en L es $e \cdot v$. Si la valuación permanece constante no puede haber ramificación. En particular, la completación K_v de K respecto a v no tiene ramificación.

DEMOSTRACIÓN. Si E es una curva de multiplicación compleja entonces es un resultado fundamental, aunque para nada trivial, que su j-invariante es un entero algebraico (Ver el capítullo de multiplicación compleja en [Sil94]). En la proposición (13) probamos que una curva tiene j-invariante en el anillo de enteros si y solo si tiene reducción potencialmente buena. Sin embargo sabemos que E tiene un modelo semiestable, por lo que su reducción es buena o multiplicativa (ver la observación (11)). □

2. Parte (a) del Lema Principal

La matemática más difícil está escondida en esta sección. Específicamente en la demostración del Lema (10). Intentar explicar la maquinaria involucrada superaría ampliamente los propósitos de este trabajo. Sin embargo presentamos los ingredientes y la idea de cómo éstos contribuyen a la prueba del Lema Principal.

2.1. Lema técnico:

La demostración del siguiente Teorema se encuentra en [OT70]. Vamos a aceptarlo como un resultado técnico que extiende el Teorema (8) al contexto de esquemas de grupos.

TEOREMA 13. *Sea T un subesquema de* $\mathrm{Spec}(\mathbb{Z})$ *donde* 2 *es invertible (por ejemplo* $\mathrm{Spec}(\mathbb{Z}[1/2])$*). Sea A un T-esquema de grupos abeliano, y sea p un primo que da un punto cerrado en T. Entonces la reducción*

$$A(T)_{tors} \to A(\mathbb{F}_p)$$

es inyectiva.

LEMA 10. *Si $s \in S$ es cualquier punto de mala reducción entonces $(\mathbb{Z}/N)_{/s} \not\subseteq (\mathcal{E}_{/s})^\circ$.*

Seguimos la prueba de [Sch04], Lema 5.5.

ESBOZO DE LA PRUEBA: Sea s un punto de mala reducción y supongamos $(\mathbb{Z}/N)_{/s} \subset (E_{/s})^0 \implies N \mid l^{2r}-1 = (l^r-1)(l^r+1)$. Como en la prueba del Lema (9), existe una extensión cuadrática de $k(s)$ tal que:

$$(\mathcal{E}_{/s})^\circ(\widetilde{k(s)}) = \widetilde{E}(\widetilde{k(s)})_{\mathrm{ns}} \cong \widetilde{k(s)}^\times$$

$$(\mathbb{Z}/N)_{/s} \subset (\mathcal{E}_{/s})^\circ \implies N \mid l^{2r}-1 = (l^r-1)(l^r+1)$$

Esta última condición no puede darse si $l = 2, 3$ por el Lema 9, pero tampoco si $l = N$.

Esto prueba el lema para $l = \mathrm{car}(s) \in \{2, 3, N\}$.

En lo que sigue vamos a mirar solo el caso $K = \mathbb{Q}$ y ahora l es un primo racional con $l \notin \{2, 3, N\}$. Supongamos entonces $(\mathbb{Z}/N)_{/l} \subset (E_{/l})^0$. Consideramos el esquema $S = \mathrm{Spec}(\mathbb{Z}[1/2N])$. Recordamos de 3.1 el Axioma 2, el cual da un morfismo no trivial $f : X_0(N)_{/S} \to A_{/S}$ definido sobre $\mathbb{Q}$. De acuerdo al Teorema 13 anterior se necesita que el 2 sea invertible en (el anillo de) S para garantizar que la reducción de la torsión $A(\mathbb{Q})_{\mathrm{tors}} \to A(\mathbb{F}_p)$ sea inyectiva para p primo racional. El Axioma 2 dice además que $A(\mathbb{Q})$ es de torsión, osea que todo $A(\mathbb{Q})$ va a reducir inyectivamente.

Consideramos el S-punto x de la curva modular $X_0(N)$ determinado por el par $(E_{/S}, (\mathbb{Z}/N\mathbb{Z})_{/S})$. Los puntos no cuspidales de la curva $X_0(N)$ codifican pares $[E, C]$, donde E es una curva elíptica y C un subgrupo de orden N. Cuando N es un primo impar, $X_0(N)$ tiene dos puntos cuspidales, llamados 0 e ∞. Estos puntos tienen una interpretación como pares $[E, C]$, donde E es una "curva elíptica generalizada." Sean $0_{/3}, 0_{/l}$ las *secciones* de 0 en las fibras de $X_0(N)$ por 3 y l, y lo mismo para ∞.

La *sección* de x en cada fibra de S está determinada por el tipo de reducción de E, de tal manera que se cumple lo siguiente: sea q un primo de reducción multiplicativa. Entonces:

- Si $(\mathbb{Z}/N\mathbb{Z})_{/q} \subseteq \mathcal{E}(\mathbb{F}_q)^0$ entonces $x = [E, (\mathbb{Z}/N\mathbb{Z})]$ reduce a ∞ en $X_0(N)$ mod q.
- Si $(\mathbb{Z}/N\mathbb{Z})_{/q} \not\subseteq \mathcal{E}(\mathbb{F}_q)^0$ entonces $x = [E, (\mathbb{Z}/N\mathbb{Z})]$ reduce a 0 en $X_0(N)$ mod q.

De acuerdo a nuestro análisis de las fibras de $(\mathbb{Z}/N\mathbb{Z})_{/S}$ en $\mathcal{E}_S$, tenemos:

$$x \equiv \infty \bmod 3 \qquad\qquad x \equiv 0 \bmod l$$

El mapa f es la composición $X_0(N) \to J \to A$ donde J es el jacobiano de $X_0(N)$, A es un cociente de J, y el morfismo $X_0(N) \to J$ es el usual $y \mapsto [y] - [\infty]$.

$$X_0(N) \longrightarrow J \longrightarrow A \qquad\qquad y \mapsto [y] - [\infty] \mapsto \overline{[y] - [\infty]}$$

$$f(x) = \overline{[x] - [\infty]} \equiv \begin{cases} \overline{[\infty] - [\infty]} & \bmod 3 \\ \\ \overline{[0] - [\infty]} & \bmod l \end{cases}$$

La primera congruencia implica que $f(x)$ debe ser igual a $[\infty] - [\infty]$ debido a que la torsión reduce inyectivamente y $f(x)$ es de torsión por hipótesis (Axioma 2). Sin embargo, el mismo argumento junto con la segunda congruencia implica que $f(x)$ debe ser igual a $[0] - [\infty]$, un absurdo.

□

2.2. Ramificación. Antes de pasar a la última prueba hacemos una breve digresión sobre extensiones no ramificadas.

Recordar que dada una extensión K'/K, del cuerpo local K, tenemos las inclusiones correspondientes entre los anillos de enteros y los ideales maximales (de acuerdo a la notación introducida al principio de la sección 1.2):

$$K \subseteq K' \implies \begin{cases} R \subseteq R' \\ M \subseteq M' \end{cases}$$

Por lo tanto la inclusión $R \to R'$ induce un homomorfismo (inyerctivo) de cuerpos locales:

$$k \cong R/M \to R'/M' \cong k'$$

De manera similar, todo automorfismo $\sigma \in \mathrm{Gal}(K'/K)$ induce un automorfismo de la extensión residual, $\widetilde{\sigma} \in \mathrm{Gal}(k'/k)$. Por lo tanto tenemos un mapa:

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{k}/k)$$
$$\sigma \mapsto \widetilde{\sigma}$$

La siguiente proposición implica que este mapa es sobreyectivo.

PROPOSICIÓN 19. *Sea k'/k una extensión finita separable. Entonces existe una extensión de cuerpos K'/K no ramificada cuya correspondiente extensión residual es isomorfa a k'/k.*

DEMOSTRACIÓN. Ver [Ser80] III.5, *Unramified Extensions*, Teorema 2. De hecho Serre prueba no solo existencia sino también unicidad de la extensión K'/K a menos de isomorfismo, pero la unicidad requiere más hipótesis. □

La proposición dice además que la extensión K'/K puede tomarse no ramificada. Si K^{nr} es la mayor extensión no ramificada de K y $\sigma \in \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$, entonces su restricción a toda extensión no ramificada de K es la identidad y $\widetilde{\sigma} = 1$.

DEFINICIÓN 27. *Se define el grupo de inercia $I = \mathrm{Gal}(\overline{K}/K^{nr})$, donde K^{nr} es la mayor extensión no ramificada de K.*

De la discusión anterior se tiene:

PROPOSICIÓN 20. *El grupo de inercia I actúa trivialmente sobre k, el cuerpo residual.*

Ahora podemos probar:

PROPOSICIÓN 21. *Si E/K de buena reducción y N es coprimo con* $\mathrm{car}(k)$*, entonces $E[N]$ es fijo por el grupo de inercia. En particular*

$$K(E[N]) \subseteq K^{nr}.$$

DEMOSTRACIÓN. Sea K' una extensión de K tal que $K(E[N]) \subseteq K'$. Como la reducción E/k es no singular entonces E tiene una ecuación minimal con coeficientes en R y tal que $v(\Delta) = 0$. Como la extensión de la valuación, v', es un múltiplo de v, entonces también $v'(\Delta) = 0$ y E/k' es no singular, es decir, la curva E/K' tiene buena reducción y, por el Teorema (8), la N-torsión reduce inyectivamente.

Sea $R \in E$ y llamemos $\widetilde{R}$ a su reducción en k. Dado un automorfismo $\sigma \in I$, sabemos que su reducción $\widetilde{\sigma} \in \mathrm{Gal}(\overline{k}/k)$ es trivial.

Tenemos

$$\widetilde{(R - R^{\sigma})} = \widetilde{R} - (\widetilde{R})^{\widetilde{\sigma}} = \widetilde{R} - \widetilde{R} = \widetilde{R - R} = \widetilde{O} \implies R - R^{\sigma} = O$$

donde la última implicación viene del hecho de que la reducción $E[N] \to E/k'$ es inyectiva.

□

El final de esta sección sigue en parte la exposición de [Sch04]. Usaremos el siguiente lema:

LEMA 11. *Sea $X/\mathbb{Q}$ un esquema, y sea X' el esquema $X/\mathbb{Q}_p$ para un primo p. Entonces $X(\overline{\mathbb{Q}})$ es no ramificado sobre p si y solo si $X(\overline{\mathbb{Q}_p})$ es no ramificado sobre p.*

DEMOSTRACIÓN. Ver [Sch04] Lema 5.6. □

PROPOSICIÓN 22 (Lema Principal, parte (a)). *La extensión $\mathbb{Q}(E[N])/\mathbb{Q}(\zeta_N)$ es no ramificada.*

ESBOZO DE LA DEMOSTRACIÓN. Separamos la prueba en cuatro casos:

Caso 1: Buena reducción en $p \neq N$.

Este caso es la proposición (21) aplicada en $\mathbb{Q}_p$ para cada primo $p \neq N$.

Caso 2: Mala reducción en $p \neq N$.

Por el Lema (10) tenemos que $\mathbb{Z}/N\mathbb{Z} \not\subset \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) = \mathcal{E}^\circ(\mathbb{F}_p)$. La idea es mostrar que

$$E(\overline{\mathbb{Q}}_p)[N] = \mu_N \times \mathbb{Z}/N\mathbb{Z}$$

para deducir que

$$\mathbb{Q}_p(E[N]) = \mathbb{Q}_p(\zeta_N)$$

y, trivialmente, no hay ramificación en p.

Entonces el lema anterior implica que la extensión $\mathbb{Q}(E[N]) \supseteq \mathbb{Q}(\zeta_N)$ tampoco tiene ramificación sobre p.

Consideramos la sucesión

$$0 \to \mathcal{E}^\circ(\overline{\mathbb{Q}}_p) \to \mathcal{E}(\overline{\mathbb{Q}}_p) \to \mathcal{E}(\overline{\mathbb{Q}}_p)/\mathcal{E}^\circ(\overline{\mathbb{Q}}_p) \to 0 \tag{7}$$

Vamos a ver que $\mathcal{E}^\circ(\overline{\mathbb{Q}}_p)$ contiene un subgrupo de orden N. Recordar que, por el Lema (10), $\mathbb{Z}/N\mathbb{Z} \not\subseteq \mathcal{E}^\circ(\overline{\mathbb{Q}}_p)$, es decir el punto racional de N-torsión no está contenido en $\mathcal{E}^\circ(\overline{\mathbb{Q}}_p) = E^0(\overline{\mathbb{Q}}_p)$. Sin embargo, dicho punto genera un submódulo $\mathbb{Z}/N\mathbb{Z} \subseteq \mathcal{E}(\overline{\mathbb{Q}}_p)/\mathcal{E}^\circ(\overline{\mathbb{Q}}_p)$. Como consecuencia la N-torsión se parte como el producto de dos módulos de Galois.

Sabemos que la reducción es multiplicativa, i.e., $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_{p^2}) \cong \mathbb{F}_{p^2}^\times$ (y a su vez para toda extensión de $\mathbb{F}_{p^2}$). El grupo multiplicativo de la clausura algebraica, $\overline{\mathbb{F}}_p^\times$ tiene subgrupos de cualquier orden N coprimo con p. Por lo tanto existe un punto $\widetilde{R}$ en $\widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}}_p)$ de orden N.

Recordar la sucesión exacta

$$0 \to E^1 \to E^0 \to \widetilde{E}_{\mathrm{ns}} \to 0$$

donde E^0 son los los puntos que reducen a los puntos no singulares de $\widetilde{E}$, y E^1 son los puntos que reducen a la identidad. Tomar un punto $R \in E^0(\overline{\mathbb{Q}}_p)$ en la preimagen de $\widetilde{R}$. El punto R tiene orden N módulo $E^1(\overline{\mathbb{Q}}_p)$, es decir N es el menor entero tal que

$$[N]R \in E^1(\mathbb{Q}_p)$$

.

En particular, $[N]R$ tiene orden una potencia de p ([Sil86] VII Teorema 3.4).

Luego, para cierto α se tiene

$$[N][p^\alpha]R = [p^\alpha][N]R = O$$

y $[p^\alpha]R$ es un punto de orden exactamente N. En particular, $E^0 \subseteq E$ contiene un submódulo de Galois de orden N en alguna extensión de $\mathbb{Q}_p$.

Hemos mostrado, al menos para $p \neq N$, que $\mathcal{E}^0(\mathbb{F}_{p^2})[N]$ es no trivial.

Se tiene entonces que la sucesión (7) restringida a $E(\overline{\mathbb{Q}}_p)[N]$ es no trivial.

Se deduce que $\mathbb{Q}_p(E[N])$ es no ramificada sobre $\mathbb{Q}_p(\zeta_N)$ en todos los primos sobre p.

El Lema (11) muestra que de hecho $\mathbb{Q}(E[N])$ es no ramificada sobre $\mathbb{Q}(\zeta_N)$ en todos los primos sobre p.

Caso 3: Mala reducción en $p = N$.

Por el teorema de uniformización de Tate tenemos un isomorfismo de grupos

$$\overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}} \cong E(\overline{\mathbb{Q}}_p)$$

el cual conmuta con la acción de Galois.

Las raíces N-ésimas de la unidad forman un subgrupo multiplicativo μ_N de $\overline{\mathbb{Q}}_p^\times$ y todas tienen clases distintas en $\overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$ (tienen valuación cero).

Es fácil ver que la N-torsión de $\overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$ se parte en dos subgrupos: uno es μ_N y el otro es el generado por una raíz N-ésima de q.

Podemos escribir

$$E(\overline{\mathbb{Q}}_p)[N] \cong \{q^{(1/N)a} \cdot \zeta_N^b \ : \ 0 \leq a, b < N\}$$

con ζ_N una raíz N-ésima de la unidad. Eligiendo $q^{1/N}$ correctamente, de modo que sea fija por Galois, es evidente que la torsión se parte:

$$E(\overline{\mathbb{Q}}_p)[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mu_N$$

como módulos de Galois.

Caso 4: Buena reducción en p con $p = N$.

Consideramos la sucesión de la observación (3) con $m = p$:

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$$

Para probar este caso Mazur usa que la p-torsión $E[p]$ es un $\mathbb{Z}_p$-*esquema de grupos finito plano* y que para este tipo de esquemas tomar la componente conexa de la identidad es functorial y respeta sucesiones exactas. Aplicando dicho functor a la sucesión anterior obtenemos

$$0 \to 0 \to E^0[p] \to \mu_p \to 0.$$

Se usaron dos propiedades:

1. $\mathbb{Z}/p\mathbb{Z}$ es totalmente disconexo
2. μ_p es conexo (ver las figuras 2 y 3 y la observación 18).

□

Capítulo 5

Epílogo, panorama actual

En los capítulos anteriores se presentaron varios elementos importantes para la demostración de Mazur y el papel que juegan en dicha demostración. No es en absoluto una exposición exhaustiva de la prueba y es mucho lo que se ha omitido. Esto es natural dado la complejidad de los elementos involucrados: lo referente a la teoría de esquemas de grupos requiere de una sólida formación en geometría algebraica para comprenderse a fondo y solo hemos arañado la superficie; la verificación del axioma 2 no aparece en este trabajo pero es la parte más difícil y fundamental de todas. Mazur lo demuestra en un artículo de 150 páginas ([Maz77a]), para lo cual introduce técnicas que permitieron a Andrew Wiles probar el Teorema de Modularidad. Sin embargo se espera haber logrado transmitir, al menos en parte, la riqueza de variedad de ideas y métodos que intervienen en la demostración de un resultado profundo de matemática.

Para cerrar el último capítulo vamos a presentar algunos resultados más recientes.

1. El Teorema de Mazur más allá de $\mathbb{Q}$

Desde la publicación de su demostración en 1977, el teorema de Mazur se ha podido generalizar en cierta medida, aunque todavía se está lejos de llegar a una clasificación completa de la torsión en cuerpos de números arbitrarios.

Definición 28. *Para todo entero $d > 0$ se llama $S(d)$ al conjunto de los números primos p tal que para cierta extensión de cuerpos $K/\mathbb{Q}$ de grado d existe una curva elíptica E definida sobre K con un punto K-racional de orden p.*

El teorema de Mazur implica que

$$S(1) = \text{Primos}(7),$$

donde Primos(n) es el conjunto de todos los primos de $\mathbb{N}$ menores o iguales a n.

Se sabe también ([Kam92]) que

$$S(2) = \text{Primos}(13).$$

Para mayores valores de d Oesterlé ([Oes94]) probó la cota

$$S(d) \subseteq \text{Primos}((3^{d/2} + 1)^2)$$

para $d \geq 4$ y válida para $d = 3$ excepto posiblemente si $43 \in S(3)$, aunque de hecho se sabe ([Par00],[Par03]) que

$$S(2) = \text{Primos}(13).$$

Recientemente ([Der+23]) se encontraron algunos valores más de $S(d)$ para d pequeño:

$$S(4) = \text{Primos}(17) \quad S(5) = \text{Primos}(19) \quad S(6) = \text{Primos}(19) \cup \{37\} \quad S(7) = \text{Primos}(23)$$

Respecto a la estructura de grupo, existe una versión del teorema de Mazur para extensiones cuadráticas de $\mathbb{Q}$ debido a Kenku y Momose ([KM88]):

TEOREMA 14. *Sea E una curva elíptica definida sobre $K = \mathbb{Q}(\sqrt{D})$ con $D \in \mathbb{Z}$. Sea $C_n = \mathbb{Z}/n\mathbb{Z}$. El grupo de torsión K-racional es una de las siguientes 26 posibilidades:*

$$E(K)_{torsion} \cong \begin{cases} C_n & 1 \leq n \leq 16 \text{ o } n = 18 \\ C_n \times C_{2n} & 1 \leq n \leq 6 \\ C_n \times C_{3n} & 1 \leq n \leq 2 \\ C_4 \times C_4 & \end{cases}$$

Para extensiones de grado mayor, sin embargo, la clasificación de la torsión sigue siendo un problema abierto.

Bibliografía

[Ser68] J-P. Serre. *Abelian l-adic representations and elliptic curves*. 1968.

[OT70] F. Oort y J. Tate. "Group schemes of prime order". En: *Algebra amp; Number Theory* (1970).

[Har77] R. Hartshorne. *Algebraic geometry*. 1977.

[Maz77a] B. Mazur. "Modular curves and the Eisenstein ideal". En: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* (1977).

[Maz77b] B. Mazur. "Rational points on modular curves". En: *Modular Functions of one Variable V*. Ed. por J-P. Serre y D. B. Zagier. Berlin, Heidelberg: Springer Berlin Heidelberg, 1977, págs. 107-148. ISBN: 978-3-540-37291-2.

[Nér80] André Néron. *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*. 1980.

[Ser80] J-P Serre. *Local fields*. 1980.

[Sil86] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 1986.

[KM88] M. A. Kenku y F. Momose. *Torsion points on elliptic curves defined over quadratic fields*. 1988.

[Kam92] S. Kamienny. *Torsion points on elliptic curves and q -coeficients of modular forms*. 1992.

[Oes94] S. Oesterlé. *Torsion des courbes elliptiques sur les corps de nombres*. 1994.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. 1994.

[CSS97] G. Cornell, J.H. Silverman y G Stevens. *Modular curves and Fermat's last theorem*. 1997. ISBN: 978-0-387-94609-2.

[Par00] P. Parent. *Torsion des courbes elliptiques sur les corps cubiques*. 2000.

[Lan02] S. Lang. *Algebra*. 2002.

[Par03] P. Parent. *No 17-torsion on elliptic curves over cubic number fields*. 2003.

[Sch04] A. B. Schwartz. "Elliptic Curves, Group Schemes, and Mazur's Theorem". En: (2004). https://legacy-www.math.harvard.edu/theses/senior/schwartz/thesis.pdf.

[Sno13] A. Snowden. *Course on Mazur's Theorem*. Notas y videos de un curso sobre el teorema de Mazur, https://public.websites.umich.edu/ asnowden/teaching/2013/679/index.html. 2013.

[Sut13] A. V. Sutherland. *Elliptic curves*. Notas de un curso dictado en el MIT, disponible en https://math.mit.edu/classes/18.783/2013. 2013.

[Mil17] J. S. Milne. *Modular Functions and Modular Forms (v1.31)*. Notas de un curso, PDF disponible en www.jmilne.org/math/. 2017.

[Gal22] C. Gallardo. *Formas Modulares*. Tesis de grado, https://www.cmat.edu.uy/biblioteca/monografias-y-tesis/monografias/uy24-20381.pdf/view. 2022.

[Der+23] M. Derickx et al. "Torsion points on elliptic curves over number fields of small degree". En: *Algebra amp; Number Theory* 17.2 (mar. de 2023), págs. 267-308. ISSN: 1937-0652. DOI: 10.2140/ant.2023.17.267. URL: http://dx.doi.org/10.2140/ant.2023.17.267.