El Grupo de Tate-Shafarevich

Miguel Pineda Martín

El Grupo de Tate-Shafarevich

Miguel Pineda Martín

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Prof. Tutor José M. Tornero

Índice general

English Abstract **1**

1. Introducción **3**

1.1. Puntos racionales sobre cónicas 3

1.2. El principio de Hasse 4

1.3. Los números p-ádicos 5

1.4. Género de una curva 9

2. Preliminares de geometría algebraica **11**

2.1. Variedades afines 11

2.2. Variedades proyectivas 15

2.3. Curvas algebraicas 20

3. Curvas elípticas **23**

3.1. El grupo de una curva elíptica 23

3.1.1. Existencia de puntos racionales 24

3.1.2. Operación de grupo 25

3.2. La forma normal de Weierstrass 27

3.3. Estructura de $C(\mathbb{Q})$ 33

4. Construcción del grupo de Tate-Shafarevich 39

4.1. Cohomología de grupos 39

4.1.1. Cohomología de grupos finitos 39

4.1.2. Cohomología de Galois 42

4.1.3. Cohomología no abeliana 43

4.2. Cohomología de Galois en curvas elípticas 44

4.3. Twisting 46

4.4. Espacios homogéneos 48

4.5. Reflexiones finales 53

English Abstract

The main purpose of this project is to develop the necessary theory to understand the Birch and Swinnerton-Dyer conjecture. In order to give a good explanation,we will need some tools of algebraic geometry. We will introduce the basic theory of elliptic curves and we will give the construction of Tate-Shafarevich group, which is the most complex structure that appears in the conjecture.

1 Introducción

En este trabajo desarrollaremos la teoría necesaria sobre curvas elípticas para entender la conjetura de Birch-Swinnerton-Dyer, uno de los problemas del milenio. El objeto que requiere un mayor desarrollo teórico para su comprensión es el grupo de Tate-Shafarevich, que da nombre a este trabajo.

A grandes rasgos nuestro interés se centrará en encontrar los puntos de coordenadas racionales de las curvas elípticas, objetos que por ahora se pueden pensar como polinomios cúbicos en dos variables.

1.1 Puntos racionales sobre cónicas

Para empezar vamos a resolver el problema para cónicas. Trabajaremos sobre $\mathbb{A}^2(\mathbb{Q})$.

Definición 1.1. *Diremos que un punto (a,b) es racional si* $a,b \in \mathbb{Q}$. *Diremos que una recta es racional si* $\exists c, d, e \in \mathbb{Q}$ *tales que*

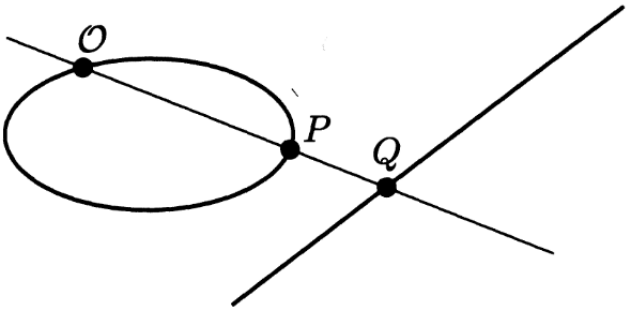
$$cx + dy + e = 0 \tag{1.1}$$

es una ecuación implícita de dicha recta. Análogamente, diremos que una cónica es racional si existe alguna ecuación suya con todos los coeficientes racionales.

Notemos que la recta que une dos puntos racionales es racional y que las intersecciones de rectas racionales distintas son puntos racionales. Sin embargo, una cónica racional y una recta racional, en caso de cortarse no tienen por qué hacerlo en puntos racionales. Esto se deduce de que para calcular dichos puntos de corte hay que resolver una ecuación de segundo grado. De esta manera, los puntos serán racionales si y solo si las raíces de la ecuación lo son. Sin embargo, basta que una raíz sea racional

para que la otra también lo sea, ya que el coeficiente lineal de la ecuación es la suma de las raíces. Esta sencilla idea nos permitirá determinar todos los puntos racionales sobre una cónica.

Dada una cónica racional, la primera pregunta que surge es si, en efecto, dicha cónica tiene puntos racionales. Esta pregunta la resolveremos más adelante. Por ahora supongamos que existe un punto racional O sobre la cónica. Consideremos una recta racional y proyectamos los puntos racionales de la cónica sobre la recta para obtener una correspondencia uno a uno.



Dado un punto racional Q sobre la recta, la recta OQ es racional y corta a la cónica en O. Por tanto, debe cortar a la cónica en otro punto P y este debe ser racional. Recíprocamente, si P es otro punto racional de la cónica la recta OP es racional y corta en un punto Q también racional a la otra recta. De esta manera, hemos probado que hay una correspondencia 1 a 1 (al menos, genéricamente) entre los puntos racionales de una cónica racional que tenga puntos racionales y los de una recta racional.

1.2 El principio de Hasse

Vamos a tratar ahora el problema de la existencia de puntos racionales. Veamos primero que existen cónicas racionales sin puntos racionales.

Consideramos la circunferencia $x^2 + y^2 = 3$. Hacemos el cambio de variable $x = X/Z,\ y = Y/Z$, con $X, Y, Z \in \mathbb{Z}$ y considearmos entonces la ecuación $X^2 + Y^2 = 3Z^2$. Podemos suponer que X, Y y Z no tienen factores comunes. Ni X ni Y son múltiplos de 3 pues si uno lo fuera el otro también lo sería y esto contradice que X y Y no tengan factores comunes. Así,

$$X^2 \equiv 1 \mod 3; \quad Y^2 \equiv 1 \mod 3. \tag{1.2}$$

Por tanto, $3Z^2 \equiv 2 \mod 3$ pero esto es una contradicción. Por tanto, la circunferencia $x^2 + y^2 = 3$ no tiene puntos racionales.

El argumento que hemos usado para demostrar que $x^2 + y^2 = 3$ no tenía puntos racionales nos da la clave para el caso general. Disponemos de un resultado de Legendre que nos dice si una cónica racional dada tiene algún punto racional en un número finito de pasos resolviendo una serie de congruencias. Este resultado se puede obtener mediante métodos elementales del siguiente resultado [9].

Teorema 1.1 (Principio de Hasse). *Una ecuación cuadrática homogénea tiene una solución entera no trivial si, y solo si, tiene solución no trivial en $\mathbb{R}$ y en los números p-ádicos para cada primo p.*

Para entender este resultado y los capítulos posteriores vamos a dar una breve descripción de qué son los números p-ádicos.

1.3 Los números p-ádicos

Definición 1.2. *Sean K un cuerpo y $|\cdot| : K \longrightarrow \mathbb{R}$ una aplicación tal que:*

1. $|r| \geq 0;\ \forall r \in K.$
2. $|r| = 0 \iff r = 0.$
3. $|rs| = |r||s|;\ \forall r, s \in K.$
4. $|r + s| \leq |r| + |s|;\ \forall r, s \in K.$

Diremos que $|\cdot|$ es una norma sobre el cuerpo K.

Observación 1.1. De las propiedades (1), (2) y (4) se deduce que $|-1| = 1$ y, por tanto, tenemos $|-r| = |r|, \quad \forall r \in K$ usando (3).

El valor absoluto es una norma sobre $\mathbb{Q}$, pero no es la única.

Definición 1.3 (Norma p-ádica). *Sea $p \in \mathbb{N}$ un primo. Todo número racional $r \in \mathbb{Q} \setminus \{0\}$ es de la forma:*

$$r = p^{\sigma} u/v, \quad u, v, \sigma \in \mathbb{Z},\ p \nmid u,\ p \nmid v. \tag{1.3}$$

Definimos la norma p-ádica sobre $\mathbb{Q}$ como

$$|r|_p = p^{-\sigma}, \quad \text{con } |0|_p = 0. \tag{1.4}$$

Proposición 1.1. La norma p-ádica es una norma sobre $\mathbb{Q}$ para todo primo p.

Demostración. La definición claramente satisface (1), (2) y (3). Sean $r, s \in \mathbb{Q}$, con

$$r = p^{\sigma} u/v, \quad u, v, \sigma \in \mathbb{Z}, \ p \nmid u, \ p \nmid v, \tag{1.5}$$

$$s = p^{\rho} m/n, \quad m, n, \rho \in \mathbb{Z}, \ p \nmid m, \ p \nmid n. \tag{1.6}$$

De esta manera, $|r|_p = p^{-\sigma}$ y $|r|_p = p^{-\rho}$. Sin pérdida de generalidad, supongamos que $\sigma \geq \rho$. De lo que deducimos que

$$|s|_p \geq |r|_p. \tag{1.7}$$

Luego,

$$r + s = p^{\rho}(un + p^{\sigma-\rho} mv)/vn. \tag{1.8}$$

El primo p no divide al denominador y el numerador es un número entero. Para $\sigma = \rho$ p puede dividir al numerador. Por tanto, tenemos

$$|r + s|_p \leq p^{-\rho}, \tag{1.9}$$

esto es,

$$|r + s|_p \leq \text{máx}\{|r|_p, |s|_p\}. \tag{1.10}$$

Esta desigualdad implica claramente la desigualdad triangular. Por tanto, $|\cdot|_p$ es una norma sobre $\mathbb{Q}$.

Observación 1.2. La desigualdad (1.10) se conoce como desigualdad ultramétrica. Una norma que cumple la desigualdad ultramétrica se dice que es no arquimediana.

Cada una de las normas p-ádicas le da a $\mathbb{Q}$ una estructura de espacio métrico, por lo que tiene sentido considerar sucesiones de Cauchy. Como en el caso del valor absoluto, hay sucesiones de números racionales que son de Cauchy y no son convergentes en el sentido de las normas p-ádicas. Veamos un ejemplo, vamos a construir una sucesión $\{a_n\} \subset \mathbb{Z}$ tal que

$$a_n^2 + 1 \equiv 0 \mod 5^n, \qquad a_{n+1} \equiv a_n \mod 5^n. \tag{1.11}$$

Comenzamos con $a_1 = 2$. Por inducción, supongamos que tenemos a_n tal que cumple nuestras condiciones. Construimos $a_{n+1} = a_n + b5^n$ donde debemos hallar $b \in \mathbb{Z}$. Imponemos

$$(a_n + b5^n)^2 + 1 \equiv 0 \mod 5^{n+1}, \tag{1.12}$$

esto es,

$$2a_n b + (a_n^2 + 1)/5^n \equiv 0 \mod 5. \tag{1.13}$$

Notemos que $(a_n^2 + 1)/5^n$ es un entero por hipótesis de inducción. Además, de nuevo por hipótesis de inducción, $5 \nmid a_n$. Luego la congruencia anterior se puede resolver en b y ese es el b buscado. La sucesión $\{a_n\}$ que acabamos de construir es una sucesión de Cauchy para la norma 5-ádica. En efecto, si $m \geq n$, por construcción se tiene que

$$|a_m - a_n|_5 \leq 5^{-n}. \tag{1.14}$$

Sin embargo, esta sucesión no es convergente. En efecto, si existiera $e \in \mathbb{Q}$ tal que a_n tendiera a e en el sentido 5-ádico, entonces

$$a_n^2 + 1 \longrightarrow e^2 + 1. \tag{1.15}$$

Pero por construcción

$$a_n^2 + 1 \longrightarrow 0. \tag{1.16}$$

Por tanto, $e^2 + 1 = 0$, pero esto es imposible en $\mathbb{Q}$. Como acabamos de ver, no todas las sucesiones de Cauchy son convergentes con nuestras nuevas normas. Inspirándonos en la construcción de los reales tenemos las siguientes definiciones.

Definición 1.4. *Un cuerpo K se dice completo respecto a una norma si toda sucesión de Cauchy es convergente respecto a dicha norma.*

Definición 1.5. *Un cuerpo K con una norma $||\cdot||$ se dice que es una completación de otro cuerpo k con una norma $|\cdot|$ si existe una inyección $\lambda : k \longrightarrow K$ tal que*

1. $||\lambda(a)|| = |a|$, $\forall a \in k$.
2. *K es completo con respecto a $||\cdot||$.*
3. *K es la clausura de $\lambda(k)$ con respecto a la topología inducida por $||\cdot||$.*

La completación siempre existe y es única, salvo un isomorfismo que también es único, para una prueba de esto ver [1] (cap. 10). Por tanto, podemos identificar k con $\lambda(k)$, $|\cdot|$ con $||\cdot||$ restringida a k y ver k como un subcuerpo de K.

Para cada primo p, hemos definido entonces una norma p-ádica $|\cdot|_p$ sobre $\mathbb{Q}$. A las completaciones de $\mathbb{Q}$ con estas normas las llamaremos cuerpos p-ádicos y los denotaremos por $\mathbb{Q}_p$. Estudiemos la estructura de estos cuerpos.

Lema 1.1. Sea $p \in \mathbb{Z}$ un primo. Se tiene:

1. Si $|b|_p < |a|_p$ con $a, b \in \mathbb{Q}_p$, entonces $|a + b|_p = |a|_p$.

2. Si $\alpha \in \mathbb{Q}_p \setminus \{0\}$, entonces $\exists a \in \mathbb{Q}$ tal que $|\alpha|_p = |a|_p$. Es decir, la norma p-ádica toma los mismos valores sobre $\mathbb{Q}$ que sobre $\mathbb{Q}_p$.

Demostración. 1. Por la desigualdad ultramétrica $|a+b|_p \leq |a|_p$. Como $a = (a+b)+(-b)$, si $|a+b|_p < |a|_p$ tendríamos la contradicción $|a+b|_p < |a|_p \leq |a+b|_p$.

2. Sea $\alpha \in \mathbb{Q}_p \setminus \{0\}$. Por definición de completación α está en la clausura de $\mathbb{Q}$ con respecto a la topología inducida por $|\cdot|_p$. Por tanto, existe $a \in \mathbb{Q}$ tal que $|a-\alpha|_p < |\alpha|_p$. Aplicando (1) obtenemos el resultado deseado. ∎

Definición 1.6. *El conjunto de los $\alpha \in \mathbb{Q}_p$ tales que $|\alpha|_p \leq 1$ se denomina el conjunto de los enteros p-ádicos y se denota por $\mathbb{Z}_p$. Los números $\epsilon \in \mathbb{Q}_p$ tales que $|\epsilon|_p = 1$ se llaman unidades p-ádicas.*

Observación 1.3. De la desigualdad ultramétrica se deduce que $\mathbb{Z}_p$ es un anillo.

$$|\alpha|_p \leq 1,\ |\beta|_p \leq 1 \implies |\alpha\beta|_p \leq 1,\ |\alpha+\beta|_p \leq 1. \tag{1.17}$$

Observación 1.4. Del punto (2) del lema anterior se deduce que cualquier $\beta \in \mathbb{Q}_p$, se puede escribir de la forma $\beta = p^n\epsilon$, para algún $n \in \mathbb{Z}$ y ϵ una unidad p-ádica. De lo que se sigue que las unidades p-ádicas son los elementos $\epsilon \in \mathbb{Z}_p$ tales que $\epsilon^{-1} \in \mathbb{Z}_p$, o sea las unidades de $\mathbb{Z}_p$ como anillo.

Pasamos ahora a dar algunos resultados de interés sobre los números p-ádicos.

Proposición 1.2. En $\mathbb{Q}_p$ la serie $\sum_{n=0}^{\infty} \beta_n$ converge si, y solo si, $\beta_n \longrightarrow 0$.

Demostración. La demostración de que la convergencia de la serie implica que su término general tiende a cero es conocida. Recíprocamente, supongamos que $\beta_n \longrightarrow 0$. Dados N y M números naturales con $M > N$, se tiene:

$$\left|\sum_{n=0}^{M} \beta_n - \sum_{n=0}^{N} \beta_n\right|_p = \left|\sum_{n=N+1}^{M} \beta_n\right|_p \leq \max_{N<n\leq M} |\beta_n|_p \tag{1.18}$$

por la desigualdad ultramétrica. De esta manera, la sucesión $\left\{\sum_0^N \beta_n\right\}$ es de Cauchy y, por tanto, convergente por la completitud de $\mathbb{Q}_p$. ∎

Con este resultado podemos dar la siguiente descripción explícita de $\mathbb{Z}_p$. Llamamos $\mathcal{A} = \{0, 1, \ldots, p-1\}$.

Proposición 1.3. Los elementos de $\mathbb{Z}_p$ son precísamente las sumas

$$\alpha = \sum_{n=0}^{\infty} a_n p^n, \text{ con } a_n \in \mathcal{A}. \tag{1.19}$$

Demostración. Por la proposición anterior las series de esta forma convergen y, claramente están en $\mathbb{Z}_p$.

Recíprocamente, dado $\alpha \in \mathbb{Z}_p$, existe un único $b \in \mathbb{Q}$ tal que $|b-\alpha|_p < 1$. Veamos que existe un $a_0 \in \mathcal{A}$ tal que $|a_0 - b|_p < 1$.

Tenemos que $|b|_p \leq 1$, ya que en caso contrario $|b|_p \geq p$ de lo que se deduce,

$$1 > |b - \alpha_0|_p \geq |b|_p - |\alpha|_p \geq p - 1 \geq 1 \tag{1.20}$$

Luego b es de la forma $b = p^\sigma r/q$ con $p \nmid r$, $p \nmid q$ y $\sigma \geq 0$. Entonces,

$$\left|a_0 - p^\sigma \frac{r}{q}\right|_p = \left|\frac{a_0 q - p^\sigma r}{q}\right|_p < 1 \iff a_0 q - p^\sigma r \equiv 0 \mod p. \tag{1.21}$$

Por tanto, si $\sigma = 0$ tomamos el único $a_0 \in \mathcal{A}$ tal que $a_0 \equiv q^{-1} r \mod p$ y si $\sigma \geq 1$ tomamos $a_0 = 0$ que es el único elemento de $\mathcal{A}$ que cumple la congruencia (1.21).

De esta manera, por la desigualdad ultramétrica:

$$|\alpha - a_0|_p = |\alpha - b + b - a_0|_p < 1, \tag{1.22}$$

de lo que se deduce que

$$\alpha = a_0 + p\alpha_1 \tag{1.23}$$

con $|\alpha_1| \leq 1$, i.e. $\alpha_1 \in \mathbb{Z}_p$. Iterando este proceso obtenemos la siguiente sucesión, que claramente converge a α:

$$\alpha = a_0 + a_1 p + \cdots + a_N p^N + \alpha_N p^{N+1}, \tag{1.24}$$

con $\alpha_N \in \mathbb{Z}_p$. ∎

1.4 Género de una curva

Con esta pequeña introducción de los números p-ádicos ya podemos entender adecuadamente el principio de Hasse. De hecho, del principio de Hasse se puede deducir que la cuestión de la existencia de puntos racionales sobre cónicas se puede reducir a resolver una cantidad finita de congruencias.

Una vez resuelto el caso de las cónicas, cabe preguntarse si podemos conocer los puntos racionales de una curva algebraica definida por un polinomio de grado arbitrario. Para ello vamos a dar algunas definiciones.

Definición 1.7. *Sean K un cuerpo y C la curva de $\mathbb{A}^2(K)$ definida por la ecuación*

$$C : f(x, y) = 0 \tag{1.25}$$

para algún $f \in K[x, y]$. Un punto P de la curva se dice que es singular si

$$\frac{\partial f(P)}{\partial x} = \frac{\partial f(P)}{\partial y} = 0. \tag{1.26}$$

En nuestro estudio de los puntos racionales sobre curvas nos restringiremos al caso en que las curvas no tengan puntos singulares por simplicidad.

Para estudiar los puntos racionales sobre curvas algebraicas, se vuelve necesario hablar del género de una curva. Las curvas de $\mathbb{P}^2(\mathbb{C})$ se pueden ver como superficies compactas orientables. Por la clasificación de este tipo de superficies sabemos que cada superficie de este tipo es homeomorfa a una esfera con una cantidad finita de asas. Al número de asas se le llama género de la superficie. Esta definición topológica no es suficiente para nuestros propósitos, por lo que usaremos la siguiente caracterización en términos puramente algebraicos [7].

Teorema 1.2. *Sea una curva de $\mathbb{P}^2(\mathbb{C})$ sin puntos singulares definida por un polinomio de grado d. Sea g el género de esta curva vista como superficie. Entonces,*

$$g = \frac{1}{2}(d-1)(d-2). \tag{1.27}$$

El género de una curva nos da información sobre la complejidad de esta. En 1983, Gerd Faltings demostró el siguiente resultado [4].

Teorema 1.3 (Faltings). *Toda curva racional de género mayor que 1 tiene una cantidad finita de puntos racionales.*

Con este resultado parece que el problema está casi resuelto, pues solo queda saber qué pasa cuando el género es 1. Sin embargo, este caso es mucho más complicado de lo que parece a simple vista y es al que le dedicaremos el resto del trabajo. Para continuar nuestro estudio, se hace necesario precisar ciertos conceptos, algunos de los cuales ya han sido usados implícitamente.

2 Preliminares de geometría algebraica

En este capítulo se expondrán los conceptos y resultados de geometría algebraica necesarios para nuestros propósitos. Buena parte de los resultados y conceptos del capítulo han sido estudiados en la asignatura del grado "Álgebra Conmutativa y Geometría Algebraica", a pesar de ello este capítulo se hace necesario tanto por el contenido nuevo como por el cambio de notación y enfoque.

Durante este capítulo trabajaremos sobre un cuerpo K perfecto, i.e. toda extensión finita de K es separable, $\overline{K}$ denotará la clausura algebraica de K y $G_{\overline{K}/K}$ el grupo de Galois de $\overline{K}/K$, esto es, el grupo de automorfismos de $\overline{K}$ que dejan fijos los elementos de K.

2.1 Variedades afines

Definición 2.1. *Entenderemos el espacio afín n-dimensional sobre $\overline{K}$ como el conjunto de n-uplas*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \left\{(x_1, \dots, x_n) \ : \ x_i \in \overline{K}\right\}. \tag{2.1}$$

Análogamente, el conjunto de los puntos K-racionales en $\mathbb{A}^n$ es el conjunto

$$\mathbb{A}^n(K) = \left\{(x_1, \dots, x_n) \ : \ x_i \in K\right\}. \tag{2.2}$$

Observación 2.1. Notemos que $G_{\overline{K}/K}$ actúa sobre $\mathbb{A}^n(\overline{K})$. Sean $\sigma \in G_{\overline{K}/K}$ y $P \in \mathbb{A}^n(\overline{K})$, entonces

$$\sigma P = (\sigma x_1, \dots, \sigma x_n). \tag{2.3}$$

De esta manera, $\mathbb{A}^n(K)$ se puede caracterizar como

$$\mathbb{A}^n(K) = \left\{ P \in \mathbb{A}^n \ : \ \sigma P = P, \ \forall \sigma \in G_{\overline{K}/K} \right\}. \tag{2.4}$$

Definición 2.2. *Sea $S \subset \overline{K}[x_1, \dots, x_n]$, consideramos el conjunto*

$$\mathcal{V}(S) = \left\{ (x_1, \dots, x_n) \in \mathbb{A}^n \ : \ f(x_1, \dots, x_n) = 0, \ \ \forall f \in I \right\}. \tag{2.5}$$

Llamamos conjunto algebraico (afín) a todo conjunto de la forma $\mathcal{V}(S)$.

Es elemental probar que, de hecho, $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$, donde $\langle S \rangle$ es el menor ideal de $\overline{K}[x_1, \dots, x_n]$ que contiene a S.

Como primeros ejemplos de conjuntos algebraicos tenemos a las variedades lineales, ya que se pueden representar como los ceros de una cantidad finita de ecuaciones lineales. Entre ellas son particularmente interesantes los puntos. Dado un punto $P = (a_1, \dots, a_n) \in \mathbb{A}^n$ este punto lo podemos construir como

$$P = \mathcal{V}\left(x_1 - a_1, \dots, x_n - a_n\right).$$

Los ideales definidos de esta forma se denotán $M_P = \langle x_1 - a_1, \dots, x_n - a_n \rangle$.

Definición 2.3. *Sea $V \subset \mathbb{A}^n$ un conjunto algebraico, definimos su ideal asociado como*

$$\mathcal{I}(V) = \left\{ f \in \overline{K}[x_1, \dots, x_n] \ : \ f(P) = 0, \ \forall P \in V \right\}. \tag{2.6}$$

Diremos que un conjunto algebraico V está definido sobre K, y lo denotaremos por V/K, si su ideal $\mathcal{I}(V)$ se puede generar con polinomios de $K[x_1, \dots, x_n]$. Si V está definido sobre K, el conjunto de los puntos K-racionales de V es el conjunto

$$V(K) = V \cap \mathbb{A}^n(K). \tag{2.7}$$

Con estas definiciones podemos construir una correspondencia entre álgebra y geometría, que viene dada por el siguiente teorema:

Teorema 2.1 (Nullstellensatz). *Si $I \subset K[x_1, \dots, x_n]$ es un ideal. Entonces,*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

Demostración. Ver [12]. ∎

Recordemos que, dado un ideal I de un anillo R,

$$\sqrt{I} = \left\{ r \in R \ : \ \exists n \in \mathbb{Z}_{\geq 0} \text{ tal que } r^n \in I \right\}.$$

Los ideales que verifican $\sqrt{I} = I$ se denominan ideales radicales. Los ideales maximales y primos son ejemplos sencillos de ideales radicales.

Corolario 2.1. Las aplicaciones $I \mapsto \mathcal{V}(I)$ y $X \mapsto \mathcal{I}(X)$ definen una biyección entre ideales radicales de $\overline{K}[x_1, \ldots, x_n]$ y subconjuntos algebraicos de $\mathbb{A}^n$ que invierte las contenciones.

Corolario 2.2. La biyección anterior restringida a los puntos, nos da una correspondencia biyectiva entre los puntos $P \in \mathbb{A}^n$ y los ideales de la forma M_P.

Observación 2.2. Notemos que los ideales de la forma $M_P = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ son ideales maximales ya que

$$\frac{\overline{K}(x_1, \ldots, x_n)}{\langle x_1 - a_1, \ldots, x_n - a_n \rangle} \cong \frac{\overline{K}(x_2, \ldots, x_n)}{\langle x_2 - a_2, \ldots, x_n - a_n \rangle} \cong \cdots \cong \frac{\overline{K}(x_n)}{\langle x_n - a_n \rangle} \cong \overline{K}.$$

Usando los conjuntos algebraicos podemos darle topología al espacio afín. De manera, más precisa tenemos el siguiente lema:

Lema 2.1. Se tiene:

1. $\varnothing$ y $\mathbb{A}^n$ son conjuntos algebraicos.
2. Sean $S_1, S_2 \subset \overline{K}[x_1, \ldots, x_n]$. Entonces, $\mathcal{V}(S_1) \cup \mathcal{V}(S_2) = \mathcal{V}(S_1 S_2)$.
3. Sea $\{X_i\}_{i \in I}$ una familia de subconjuntos algebraicos de $\mathbb{A}^n$ con $X_i = \mathcal{V}(S_i)$. Entonces $\bigcap_{i \in I} X_i = \mathcal{V}(\bigcup_{i \in I} S_i)$.

Demostración. Ver [3] (Tema 1). ∎

De esta manera los conjuntos algebraicos son los cerrados de una topología.

Definición 2.4 (Topología de Zariski). *Para cada $n \geq 1$ llamamos topología de Zariski sobre $\mathbb{A}^n$ a la topología cuyos cerrados son los conjuntos algebraicos.*

Sea $X \subset \mathbb{A}^n$ un conjunto algebraico, decimos que es una variedad algebraica si es irreducible como cerrado de la topología de Zariski.

Proposición 2.1. Sea $X \subset \mathbb{A}^n_K$ un conjunto algebraico. Las condiciones siguientes son equivalentes:

1. X es irreducible y no vacío.
2. $\mathcal{I}(X)$ es un ideal primo.

Demostración. Ver [3] (Tema 1). ∎

Definición 2.5. *Dado $X \subset \mathbb{A}^n_K$ un conjunto algebraico. Diremos que $\mathcal{A}(X) = K[x_1, \dots, x_n]/\mathcal{I}(X)$ es el anillo de coordenadas de X.*

Observación 2.3. El anillo de coordenadas de una variedad algebraica X se puede entender como las funciones polinómicas de X en $\overline{K}$.

Observación 2.4. Sea $V \subset \mathbb{A}^n_K$ una variedad algebraica. Por la proposición anterior $\mathcal{I}(V)$ es un ideal primo y, por tanto, $\mathcal{A}(V)$ es un dominio de integridad y tiene sentido la siguiente definición.

Definición 2.6. *Definimos la dimensión de una variedad algebraica como la dimensión de Krull de su anillo de coordenadas.*

Definición 2.7. *Sea $V \subset \mathbb{A}^n_K$ una variedad algebraica. Al cuerpo de fracciones de $\mathcal{A}(V)$ lo llamamos cuerpo de funciones de V y lo denotamos por $K(V)$.*

Definición 2.8. *Sean $V \subset \mathbb{P}^n$ una variedad y $P \in \mathbb{P}^n$. Definimos el anillo local de V en P, denotado $\mathcal{A}(V)_P$, como la localización de $\mathcal{A}(V)$ en M_P. En otras palabras,*

$$\mathcal{A}(V)_P = \left\{ F \in \overline{K}(V) \ : \ F = \frac{f}{g} \text{ para algunos } f, g \in \mathcal{A}(V) \text{ con } g(P) \neq 0 \right\}. \quad (2.8)$$

Notemos que si $F = f/g \in \mathcal{A}(V)_P$, entonces $F(P) = f(P)/g(P)$ está bien definido. Decimos que $F \in K(V)$ es regular, o está definida, en P si $F \in \mathcal{A}(V)_P$.

Observación 2.5. Notemos que en las condiciones de la definición anterior $M_P \subset \mathcal{A}(V)_P$ es un ideal maximal y de hecho se puede probar que su único ideal maximal, por lo que $\mathcal{A}(V)_P$ es un anillo local.

Cuando estudiamos objetos geométricos es usual imponer la condición de que sean "suaves" y no tengan "picos" para ello usaremos la siguiente definición de punto singular (que generaliza la vista en el capítulo anterior).

Definición 2.9. *Sean V una variedad, $P \in V$, y $f_1, \dots, f_m \in \overline{K}(x_1, \dots, x_n)$ unos generadores de $\mathcal{I}(V)$. Entonces V es no singular en P si la matriz $m \times n$*

$$\left(\frac{\partial f_i}{\partial x_j}(P) \right)_{1 \leq i \leq m, 1 \leq j \leq n} \quad (2.9)$$

tiene rango $n - \dim(V)$. Si V es no singular en todo punto se dice que V es no singular o regular.

Como es natural, esta definición no depende del sistema generador escogido para $\mathcal{I}(V)$.

2.2 Variedades proyectivas

Definición 2.10. *El espacio proyectivo n-dimensional, que denotaremos por $\mathbb{P}^n$ o $\mathbb{P}^n(\overline{K})$, es el conjunto de las (n+1)-uplas*

$$(x_0, \dots, x_n) \in \mathbb{A}^{n} \tag{2.10}$$

con algún x_i no nulo, módulo la relación de equivalencia dada por

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \tag{2.11}$$

si existe un $\lambda \in \overline{K} \setminus \{0\}$ tal que $x_i = \lambda y_i$ para todo i. A las clases de equivalencia $\{(\lambda x_0, \dots, \lambda x_n)\}$ las denotaremos por $[x_0, \dots, x_n]$. El conjunto de los puntos K-racionales de $\mathbb{P}^n$ será

$$\mathbb{P}^n(K) = \left\{ [x_0, \dots, x_n] \in \mathbb{P}^n \ : \ x_i \in K, \ \forall i \in \{0, \dots, n\} \right\}. \tag{2.12}$$

Es decir, son los puntos $P = [x_0, \dots, x_n]$ proyectivos tales que existe un representante $(x_0, \dots, x_n)$ con todas sus coordenadas en K.

Definición 2.11. *Un polinomio $f \in \overline{K}[x_0, \dots, x_n]$ es homogéneo de grado d si*

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n) \tag{2.13}$$

para todo $\lambda \in \overline{K}$. Un ideal $I \subset \overline{K}[x_0, \dots, x_n]$ es homogéneo si está generado por polinomios homogéneos.

Notemos que para un polinomio homogéneo $f \in \overline{K}[x_0, \dots, x_n]$, está bien definido decir que $f(P) = 0$ en un punto $P \in \mathbb{P}^n$. Por lo que, a cada ideal homogéneo I le podemos asociar

$$\mathcal{V}(I) = \left\{ P \in \mathbb{P}^n \ : \ f(P) = 0 \text{ para todo polinomio homogéneo } f \in I \right\}. \tag{2.14}$$

Definición 2.12. *Llamamos conjunto algebraico (proyectivo) a cualquier conjunto de la forma $\mathcal{V}(I) \subset \mathbb{P}^n$, con I homogéneo. Si $V \subset \mathbb{P}^n$ es un conjunto algebraico, definimos su ideal homogéneo asociado como*

$$\mathcal{I}(V) = \left\langle \left\{ f \in \overline{K}[x_0, \dots, x_n] \ : \ f \text{ es homogéneo y } f(P) = 0, \ \forall P \in V \right\} \right\rangle. \tag{2.15}$$

Diremos que V está definido sobre K si su ideal $\mathcal{I}(V)$ se puede generar con polinomios homogéneos de $K[x_0, \dots, x_n]$. Si V está definido sobre K, el conjunto de los puntos K-racionales de V es el conjunto

$$V(K) = V \cap \mathbb{P}^n(K). \tag{2.16}$$

Definición 2.13. *Llamamos variedad algebraica (proyectiva) a un conjunto algebraico V si $\mathcal{I}(V)$ es un ideal primo de $\overline{K}[x_0, \dots, x_n]$.*

Vamos a relacionar ahora los conceptos que hemos definido en el espacio proyectivo con los del espacio afín. Para empezar, consideramos la aplicación

$$\begin{aligned} \varphi : \mathbb{A}^n &\longrightarrow \mathbb{P}^n \\ (y_1, \dots, y_n) &\longmapsto [1, y_1, \dots, y_n]. \end{aligned}$$

Como es habitual, llamamos hiperplano del infinito a

$$H_\infty = \left\{[x_0, \dots, x_n] \in \mathbb{P}^n : x_0 \neq 0\right\}. \tag{2.17}$$

De esta manera tenemos la biyección

$$\varphi^{-1} : \mathbb{P}^n \setminus H_\infty \longrightarrow \mathbb{A}^n$$

dada por

$$[a_0, \dots, a_n] \mapsto \left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right),$$

con la cual identificaremos el espacio afín con su imagen en el proyectivo por φ.

Observación 2.6. Podemos llamar

$$U_i = \left\{[x_0, \dots, x_n] \in \mathbb{P}^n \ : \ x_i \neq 0\right\}.$$

De esta manera, $\bigcup_{i=0}^n U_i = \mathbb{P}^n$. La aplicación φ tiene como imagen U_0 con el que identificamos $\mathbb{A}^n$. Análogamente, podemos identificar $\mathbb{A}^n$ con cualquiera de los U_i, pero solo con uno a la vez. Usualmente trabajaremos con la inmersión φ del espacio afín en el proyectivo, pero a veces necesitaremos usar una arbitraria.

Sea ahora V un conjunto algebraico proyectivo con ideal homogéneo $\mathcal{I}(V) \subset \overline{K}[x_0, \dots, x_n]$. Entonces, $V \cap \mathbb{A}^n$ es un conjunto algebraico afín cuyo ideal asociado $\mathcal{I}(V \cap \mathbb{A}^n) \subset \overline{K}[y_1, \dots, y_n]$ es

$$\mathcal{I}(V \cap \mathbb{A}^n) = \left\{f(1, y_1, \dots, y_n) \ : \ f(x_0, \dots, x_n) \in \mathcal{I}(V)\right\}. \tag{2.18}$$

Al paso de $f(x_0, \dots, x_n)$ a $f(1, y_1, \dots, y_n)$ se denomina deshomogeneización de f. El proceso se puede invertir. Sea $f \in \overline{K}[y_1, \dots, y_n]$, consideramos

$$f^*(x_0, \dots, x_n) = x_0^d f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \tag{2.19}$$

donde $d = \deg(f)$ es el entero más pequeño para el que f^* es un polinomio. Llamamos a f^* el homogeneizado de f.

Definición 2.14. *Sea $V \subset \mathbb{A}^n$ un conjunto algebraico afín con ideal $\mathcal{I}(V)$. Si vemos V como subconjunto de $\mathbb{P}^n$, definimos la clausura proyectiva de V, que denotaremos por $\overline{V}$, como el conjunto algebraico proyectivo cuyo ideal $\mathcal{I}(\overline{V})$ está generado por*

$$\{f^*(x_0, \dots, x_n) \ : \ f \in \mathcal{I}(V)\}. \tag{2.20}$$

La relación que guarda una variedad afín con su clausura proyectiva viene dada por la siguiente proposición.

Proposición 2.2. Se cumplen los siguientes enunciados:

1. Sea V una variedad afín. Entonces $\overline{V}$ es una variedad proyectiva, y $V = \overline{V} \cap \mathbb{A}^n$.
2. Sea V una variedad proyectiva. Entonces $V \cap \mathbb{A}^n$ es una variedad afín, y $V \cap \mathbb{A}^n = \varnothing$ o $V = \overline{V \cap \mathbb{A}^n}$.
3. Si una variedad afín V (resp. proyectiva) está definida sobre K, entonces $\overline{V}$ (resp. $V \cap \mathbb{A}^n$) también está definida sobre K.

Demostración. [3] (Tema 2). ∎

A la vista de este resultado, cada variedad afín se puede identificar con una única variedad proyectiva. En los siguientes capítulos estaremos trabajando con curvas en el proyectivo, pero por simplicidad trabajaremos con sus ecuaciones afines, entendiendo que tiene puntos en el infinito.

Observación 2.7. Un punto en $\mathbb{P}^n(\mathbb{Q})$ es de la forma $[x_0, \dots, x_n]$ con $x_i \in \mathbb{Q}$. Multiplicando por un $\lambda \in \mathbb{Q}$ adecuado, podemos eliminar los denominadores de los x_i. De esta manera, todo punto $P \in \mathbb{Q}$ se puede escribir como $P = [x_0, \dots, x_n]$ con

$$x_0, \dots, x_n \in \mathbb{Z} \text{ y } \gcd(x_0, \dots, x_n) = 1. \tag{2.21}$$

Por tanto, encontrar los puntos racionales de una variedad proyectiva definida sobre $\mathbb{Q}$ y dada por polinomios homogéneos $f_1, \dots, f_m \in \mathbb{Q}[x_0, \dots, x_n]$ es equivalente a encontrar las soluciones enteras no triviales de las ecuaciones

$$f_1(x_0, \dots, x_n) = \cdots = f_m(x_0, \dots, x_n) = 0 \tag{2.22}$$

con $x_0, \dots, x_n$ primos relativos. Este procedimiento es el que usamos en la introducción para demostrar que $x^2 + y^2 = 3$ no tiene puntos racionales.

Definición 2.15. *Sea V una variedad proyectiva y consideremos una inmersión $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $V \cap \mathbb{A}^n \neq \emptyset$. Definimos el cuerpo de funciones de V, denotado por $K(V)$, como el cuerpo de funciones de $V \cap \mathbb{A}^n$. Análogamente definimos $\overline{K}(V)$.*

Observación 2.8. El cuerpo de funciones de $V \subset \mathbb{P}^n$ una variedad proyectiva también se puede entender como el cuerpo de funciones racionales $F = f/g$ tales que

1. f y g son polinomios homogéneos del mismo grado.
2. $g \notin \mathcal{I}(V)$.
3. Identificamos dos funciones f/g y f'/g' si $fg' - f'g \in \mathcal{I}(V)$.

Vamos ahora a definir las aplicaciones entre variedades que nos serán de interés.

Definición 2.16. *Sean $V_1, V_2 \subset \mathbb{P}^n$ variedades proyectivas. Una aplicación racional de V_1 a V_2 es una aplicación*

$$\phi = [f_0, \dots, f_n] : V_1 \longrightarrow V_2$$

donde $f_0, \dots, f_n \in \overline{K}(V_1)$ tienen la propiedad de que para cada punto $P \in V_1$ en el que $f_0, \dots, f_n$ están todos definidos,

$$\phi(P) = \left[f_0(P), \dots, f_n(P)\right] \in V_2. \tag{2.23}$$

Si V_1 y V_2 están definidas sobre K, entonces $G_{\overline{K}/K}$ actúa sobre ϕ de la siguiente forma,

$$\sigma\phi(P) = \left[\sigma f_0(P), \dots, \sigma f_n(P)\right], \text{ para } \sigma \in G_{\overline{K}/K}. \tag{2.24}$$

Notemos que se tiene la siguiente formula,

$$\sigma(\phi(P)) = \sigma\phi(\sigma P), \quad \forall \sigma \in G_{\overline{K}/K}, \quad \forall P \in V_1. \tag{2.25}$$

Si existe $\lambda \in \overline{K}^*$ tal que $\lambda f_0, \dots, \lambda f_n \in K(V_1)$ decimos que ϕ está definida sobre K.

Lema 2.2. Sea ϕ una aplicación racional. Entonces, ϕ está definida sobre K si y solo si $\phi = \sigma\phi$ para todo $\sigma \in G_{\overline{K}/K}$.

Demostración. Una indicación de la prueba de este hecho se puede encontrar en [10] (I. Ejercicio 1.12).

Observación 2.9. Una aplicación racional $\phi : V_1 \longrightarrow V_2$ no es necesariamente una función sobre todo V_1. Es posible que algunos f_i no estén definidos en un punto $P \in V_1$, pero que multiplicando por un $g \in \overline{K}(V_1)$ apropiado, todos los gf_i sí estén definidos en P.

Definición 2.17. *Sean $V_1, V_2 \subset \mathbb{P}^n$ variedades proyectivas y $\phi : V_1 \longrightarrow V_2$ una aplicación racional. Se dice que ϕ es una aplicación birracional si existe otra aplicación racional $\psi : V_2 \longrightarrow V_1$ tal que sus composiciones en el sentido de las aplicaciones racionales, i.e. restrigiendonos a conjuntos donde ambas aplicaciones estén definidas y se puedan componer, son la identidad.*

En caso de que existan tales aplicaciones decimos que V_1 y V_2 son birracionalmente equivalentes.

Observación 2.10. La idea de las aplicaciones birracionales es muy útil para nuestro propósito. Por ejemplo, es fácil comprobar que en nuestro estudio de los puntos racionales de las cónicas del capítulo anterior, hemos pasado de estudiar los puntos en las cónicas racionales a las rectas racionales mediante una aplicación birracional.

La definición puede ser un poco abstracta, por lo que la ilustraremos con un ejemplo. Consideramos la curva

$$C : X^2 - Y^2 = (X - 2Y)(X^2 + Y^2) \tag{2.26}$$

y la recta $X = sY$ en $\mathbb{A}^2$. La recta corta a la curva en (0,0) y donde se cumpla

$$Y^2(s^2 - 1) = Y^3(s - 2)(s^2 + 1), \tag{2.27}$$

por lo que corta en el punto (x, y) con

$$x = \frac{s(s^2 - 1)}{(s - 2)(s^2 + 1)}, \quad y = \frac{s^2 - 1}{(s - 2)(s^2 + 1)} \tag{2.28}$$

Recíprocamente, podemos recuperar s haciendo $s = x/y$. Por lo que hemos probado que esta curva es birracionalmente equivalente a una recta. Notemos que la condición de que se tenga una biyección salvo un número finito de puntos la estamos usando, pues $s = 2$ no corresponde a ningún punto.

Definición 2.18. *Una aplicación racional*

$$\phi = [f_0, \dots, f_n] : V_1 \longrightarrow V_2 \tag{2.29}$$

se dice que es regular, o está definida, en $P \in V_1$ si existe una función $g \in \overline{K}(V_1)$ tal que

1. *Cada gf_i es regular en P.*
2. *Para algún i, $(gf_i)(P) \neq 0$.*

Esta g puede ser distinta para puntos distintos. Una aplicación racional que es regular en todo punto se dice morfismo.

Definición 2.19. *Sean $V_1, V_2 \subset \mathbb{P}^n$ variedades. Decimos que son isomorfas si existen unos morfismos $\phi : V_1 \longrightarrow V_2$ y $\psi : V_2 \longrightarrow V_1$ tales que $\psi \circ \phi$ y $\phi \circ \psi$ son las correspondientes identidades.*

Además, diremos que $V_1(K)$ y $V_2(K)$ son isomorfas sobre K si ϕ y ψ están definidas sobre K.

2.3 Curvas algebraicas

Nuestro principal objeto de estudio serán las curvas elípticas que son un caso particular de curvas algebraicas. En esta sección daremos algunos resultados de la teoría general de curvas algebraicas que nos serán necesarios para nuestro objetivo. Por curva algebraica entenderemos una variedad algebraica de dimensión 1.

Definición 2.20. *Sean C una curva y $P \in C$ un punto no singular. Definimos la valoración orden en P como*

$$\begin{aligned} \mathrm{ord}_P : \mathcal{A}(C) &\longrightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\} \\ f &\longmapsto \text{máx}\left\{d \in \mathbb{Z} : f \in M_P^d\right\} \end{aligned}$$

Haciendo $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, podemos extender la definición a $\overline{K}(C)$,

$$\mathrm{ord}_P : \overline{K}(C) \longrightarrow \mathbb{Z} \cup \{\infty\}. \tag{2.30}$$

Por último, diremos que $t \in \overline{K}(C)$ es un parámetro de uniformización para la curva C en P si $\mathrm{ord}_P(t) = 1$ (es decir, si es un elemento de M_P).

Definición 2.21. *Sean C una curva, $P \in C$ un punto no singular y $f \in \overline{K}(C)$. Si el orden de f en P es 0, $f(P) \neq 0$. Si no, sea $m = \mathrm{ord}_P(f)$. Tenemos dos casos:*

1. *Si $m > 0$ decimos que f tiene un cero de orden m en P.*
2. *Si $m < 0$ decimos que f tiene un polo de orden $-m$ en P.*

Observación 2.11. Notemos que, si $\mathrm{ord}_P(f) \geq 0$, f es regular en P y podemos calcular $f(P)$. Si f tiene un polo en P, escribimos $f(P) = \infty$.

Proposición 2.3. Sea C una curva no singular y $f \in \overline{K}(C)$. Entonces solo hay una cantidad finita de puntos donde $\mathrm{ord}_P(f) \neq 0$.

Demostración. Para una prueba de la finitud del número de polos, ver [6] (I.6.5). Para los ceros basta hacer lo mismo con $1/f$.

Proposición 2.4. Sea C una curva, $V \subset \mathbb{P}^n$ una variedad, $P \in C$ un punto no singular y $\phi : C \longrightarrow V$ una aplicación racional. Entonces ϕ es regular en P.

Demostración. La aplicación racional es de la forma $\phi = [f_0, \ldots, f_n]$ con $f_i \in \overline{K}(C)$. Sea t un parámetro de uniformización de C en P. Tomamos

$$n = \min_{0 \leq i \leq N} \mathrm{ord}_P(f_i). \tag{2.31}$$

Entonces

$$\mathrm{ord}_P\left(t^{-n} f_i\right) \geq 0, \ \forall i, \ \text{y} \ \mathrm{ord}_P\left(t^{-n} f_j\right) > 0 \text{ para algún } j, \tag{2.32}$$

por lo que $t^{-n} f_i$ es regular en P y $(t^{-n} f_j)(P) \neq 0$. Por tanto, hemos probado que ϕ es regular en P.

Corolario 2.3. Sea C una curva regular y $V \subset \mathbb{P}^n$ una variedad. Entonces toda aplicación racional $\phi : C \longrightarrow V$ es un morfismo.

Observación 2.12. En este trabajo solo estudiaremos curvas no singulares, por lo que este último corolario nos será muy útil. A partir de aquí, cuando trabajemos con curvas regulares usaremos indistintamente morfismo y aplicación racional.

Proposición 2.5. Sea $\phi : C_1 \longrightarrow C_2$ un morfismo entre curvas. Entonces es constante o sobreyectivo.

Demostración. Ver [6] (II.6.8).

Sean C_1/K y C_2/K dos curvas y sea $\phi : C_1 \longrightarrow C_2$ una aplicación racional definida sobre K. Esto induce, mediante la composición con ϕ, un homomorfismo de cuerpos,

$$\begin{array}{rccc} \phi^* : & K(C_2) & \longrightarrow & K(C_1) \\ & f & \longmapsto & f \circ \phi \end{array}$$

Proposición 2.6. Sean C_1/K y C_2/K dos curvas. Si $\phi : C_1 \longrightarrow C_2$ es un morfismo no constante, entonces $K(C_1)$ es una extensión finita de $\phi^*(K(C_2))$.

Demostración. Ver [6] (I.6.12).

Esta proposición motiva la siguiente definición.

Definición 2.22. *Sean $C_1/K, C_2/K$ dos curvas y $\phi : C_1 \longrightarrow C_2$ un morfismo definido sobre K no constante. Por la proposición anterior sabemos que $K(C_1)$ es una extensión finita de $\phi^*(K(C_2))$. Definimos el grado de ϕ como*

$$\deg \phi = \left[K(C_1) : \phi^* K(C_2)\right]$$

El grado de las aplicaciones constantes se define como 0.

El siguiente resultado nos será de utilidad más adelante para probar que ciertos morfismos en realidad son isomorfismos.

Proposición 2.7. Sean C_1 y C_2 curvas regulares y $\phi : C_1 \longrightarrow C_2$ un morfismo de grado 1. Entonces, ϕ es un isomorfismo.

Demostración. Ver [10] (II.2.4.1).

Con esto acabamos el desarrollo de la geometría algebraica que necesitamos para construir el grupo de Tate-Shafarevich. Procedemos en el siguiente capítulo a definir las curvas elípticas y desarrollar la teoría general de estas.

3 Curvas elípticas

En este capítulo vamos a presentar nuestro principal objeto de estudio: las curvas elípticas, que serán las curvas regulares de género 1. Por la fórmula del grado serán las curvas de grado 3 sin puntos singulares.

3.1 El grupo de una curva elíptica

Por ahora consideraremos un curva cúbica general:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{3.1}$$

con $a, b, \ldots, j \in \mathbb{Q}$.

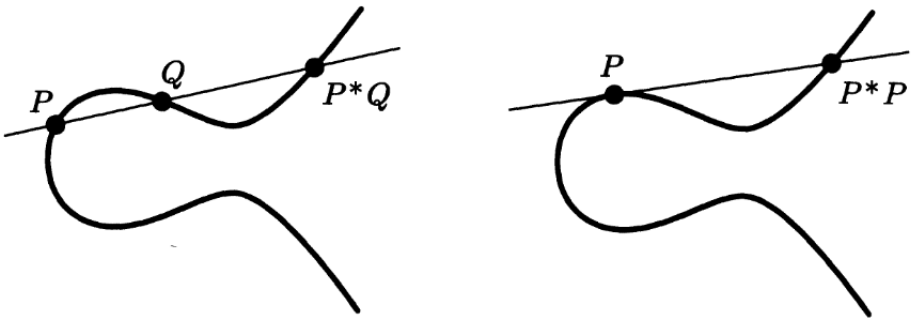
La idea usada en la introducción para encontrar los puntos racionales de las cónicas no funciona en este caso. En general, una recta puede cortar a una cúbica en tres puntos. Una recta racional puede cortar a una cúbica racional en un punto racional y que los otros dos no lo sean. Sin embargo, podemos usar el siguiente lema.

Lema 3.1. Sean C una cúbica racional y $P, Q \in C$ puntos racionales. Entonces, la recta que pasa por P y Q corta a C en tres puntos racionales.

Demostración. Para calcular los puntos de corte de C y la recta que pasa por P y Q, basta resolver una ecuación cúbica que tiene dos soluciones racionales dadas por P y Q. Por las fórmulas de Cardano-Vieta tenemos que la tercera también debe ser racional. ∎

De esta manera, dados dos puntos racionales P y Q sobre una cúbica racional, tenemos un método para encontrar otro. Este método consiste en trazar la recta que pasa por P y Q y por el lema 3.1 esta recta corta a la cúbica en otro punto racional

que denotaremos $P * Q$. Si solo tenemos un punto racional P y consideramos la recta tangente a la curva en P, razonando de manera análoga a como lo hemos hecho en el lema deducimos que esta recta corta a la cúbica en otro punto también racional que denotaremos $P * P$. Esto sucede porque a la hora de resolver la ecuación cúbica, para hallar los puntos de la intersección, la hipótesis de que la recta sea tangente hace que la ecuación tenga una solución doble (al menos).



De esta manera, hemos construido una operación $*$ que le da cierta estructura a los puntos racionales de la cúbica. Una pregunta natural que surge es si los puntos racionales de la curva forman un grupo con la operación $*$. La respuesta es que no, en esencia el problema es que no hay elemento neutro. Sin embargo, podemos usar la operación $*$ para construir una operación de grupo.

3.1.1 Existencia de puntos racionales

Para continuar con nuestra construcción necesitaremos asumir la existencia de un punto racional, por lo que vamos a tratar ligeramente el tema. Al igual que en el caso de las cónicas hay cúbicas racionales sin puntos racionales. Sin embargo, para comprobar si una cúbica tiene puntos racionales no basta estudiar la existencia de puntos reales y p-ádicos. Selmer demostró el siguiente resultado

Teorema 3.1. *La ecuación*

$$3X^3 + 4Y^3 + 5Z^3 = 0 \tag{3.2}$$

no tiene soluciones racionales distintas de (0,0,0), pero para cada p primo la ecuación tiene soluciones no triviales sobre $\mathbb{Q}_p$.

Actualmente, no hay ningún algoritmo conocido para determinar si una cúbica tiene puntos racionales. Nuestro objetivo es definir el grupo de Tate-Shafarevich, que de alguna manera le da estructura a los puntos que "impiden" que se cumpla el principio de Hasse.

3.1.2 Operación de grupo

Supondremos que nuestra curva cúbica C tiene, al menos, un punto racional que llamaremos $\mathcal{O}$. Si fijamos este punto y consideramos otros dos puntos racionales P y Q, definimos la siguiente operación:

$$P + Q := O * (P * Q). \tag{3.3}$$

Observación 3.1. Denotamos por

$$C(\mathbb{Q}) = \{(x, y) \in C \mid x, y \in \mathbb{Q}\}. \tag{3.4}$$

Vamos a probar que $(C(\mathbb{Q}), +)$ tiene estructura de grupo.

Lema 3.2. La operación $+$ es conmutativa y el punto $\mathcal{O}$ actúa como elemento neutro para esta.

Demostración. La operación $+$ es conmutativa porque la operación $*$ lo es, ya que dados $P, Q \in \mathbb{Q}$ la recta que pasa por P y Q es la misma que la que pasa por Q y P. Veamos que $\mathcal{O}$ es elemento neutro de $+$. Sea $P \in \mathbb{Q}$

$$P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) \tag{3.5}$$

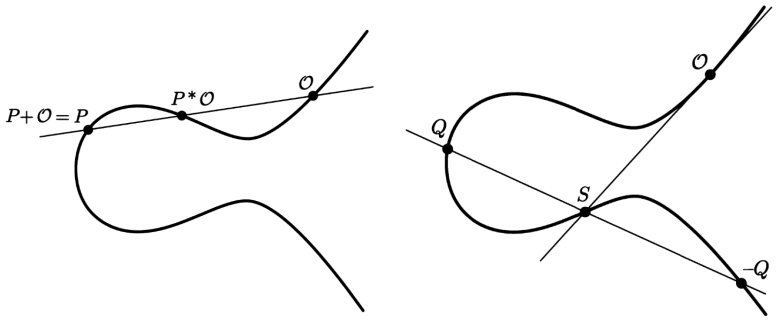
La recta que pasa por P y $\mathcal{O}$ corta a C en P, $\mathcal{O}$ y $P * \mathcal{O}$. La recta que pasa por P y $\mathcal{O}$ es la misma que la que pasa por $\mathcal{O}$ y $P * \mathcal{O}$. Por tanto, el punto $\mathcal{O} * (P * \mathcal{O})$ necesariamente debe ser P. ∎

Lema 3.3 (Elemento Inverso). Sea $Q \in C(\mathbb{Q})$, existe $R \in \mathbb{Q}$ tal que $Q + R = \mathcal{O}$. A R lo denotamos, como es habitual, $-Q$.

Demostración. Sea $Q \in C(\mathbb{Q})$, consideramos la recta tangente a C en $\mathcal{O}$ que corta a C en otro único punto que llamaremos S. El punto buscado es $Q * S$. En efecto,

$$Q + Q * S = \mathcal{O} * (Q * (Q * S)) = \mathcal{O} * S = \mathcal{O}. \tag{3.6}$$

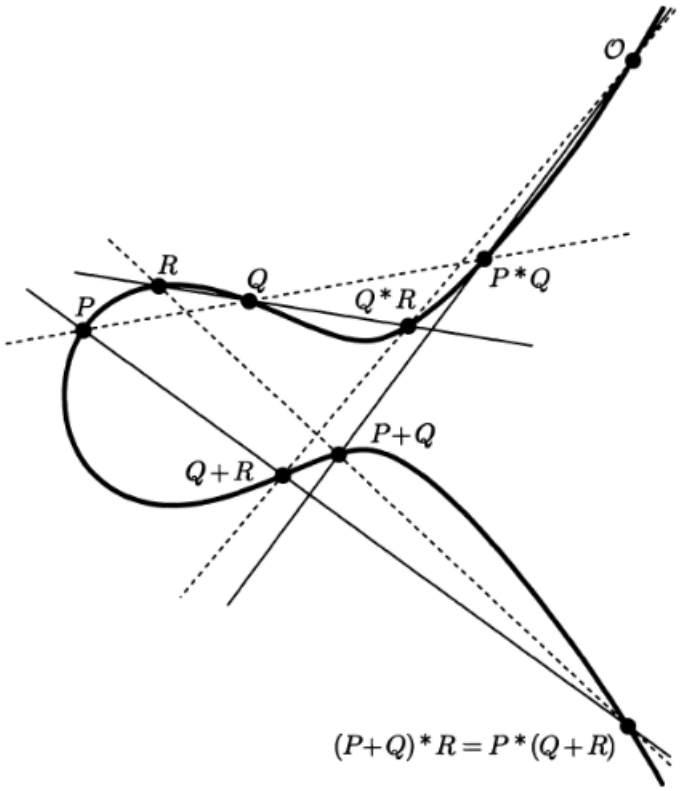
∎



Nos queda probar la asociatividad, para ello usaremos el siguiente lema auxiliar que daremos sin demostración y que es una consecuencia más o menos directa del Teorema de Bezout [5].

Lema 3.4. Sean C, C_1, C_2 tres curvas cúbicas. Supongamos que C_1 y C_2 se cortan en nueve puntos y que C pasa por ocho de los nueve. Entonces C también pasa por el noveno.

Lema 3.5. La operación $+$ en $C(\mathbb{Q})$ es asociativa.



Demostración. Daremos una idea genérica de la demostración, ya que para dar una prueba completa con estas técnicas necesitamos cubrir muchos casos especiales (tipo $P = Q$).

Tenemos que probar que $P + (Q + R) = (P + Q) + R$ para cualesquiera $P, Q, R \in C(\mathbb{Q})$. Se tiene que:

$$\begin{aligned} (P + Q) + R) &= \mathcal{O} * (R * (P + Q)), \\ P + (Q + R) &= \mathcal{O} * (P * (Q + R)). \end{aligned} \tag{3.7}$$

Por tanto, basta probar que $R * (P + Q) = P * (Q + R)$. Consideramos la recta que pasa por R y $(P + Q)$ y la que pasa por P y $Q + R$. Basta demostrar que estas rectas se cortan en un punto de la curva. Si hacemos toda la construcción tenemos ocho puntos sobre la curva: $\mathcal{O}, P, Q, R, P * Q, P + Q, Q * R$ y $Q + R$.

Tenemos que demostrar que el punto de corte con las rectas también está en la curva. Para hacer la construcción hay que trazar seis rectas como en el dibujo. Por un lado la unión de las tres rectas trazadas en línea continua es una cúbica y la unión de las tres rectas trazadas en línea discontinua es otra cúbica.

La intersección de estas dos cúbicas son los ocho puntos anteriores y la intersección de la recta que pasa por R y $P + Q$ y la que pasa por P y $Q + R$. Como nuestra cúbica pasa por esos ocho puntos, por el lema anterior debe pasar por el noveno.

De esta manera, hemos probado que $(C(\mathbb{Q}), +)$ tiene estructura de grupo. Notemos que la elección de $\mathcal{O}$ no cambia el grupo. Si elegimos $\mathcal{O}'$ otro punto racional para que sea el elemento neutro, el grupo que obtenemos es isomorfo al que tiene como elemento neutro a $\mathcal{O}$. En efecto, la aplicación

$$P \mapsto P + (\mathcal{O}' - \mathcal{O}) \tag{3.8}$$

es un isomorfismo de "$C(\mathbb{Q})$ con $\mathcal{O}$ como elemento neutro" en "$C(\mathbb{Q})$ con $\mathcal{O}'$ como elemento neutro".

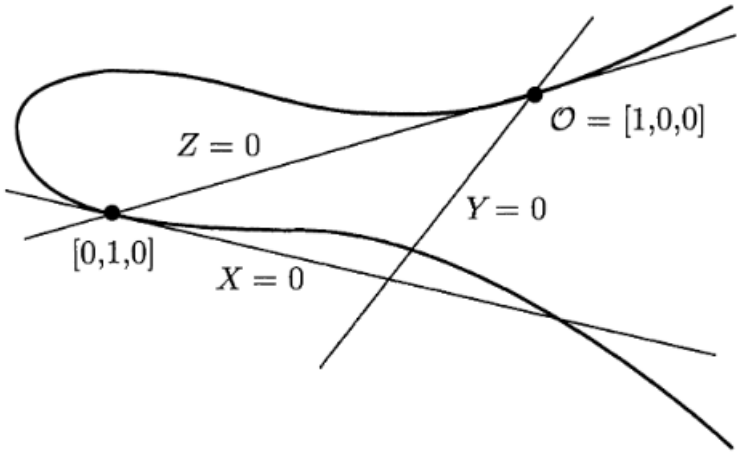
3.2 La forma normal de Weierstrass

Trabajar con cúbicas como las que hemos considerando se hace realmente difícil debido a la cantidad excesiva de parámetros. Por lo que vamos a probar que siempre

podemos trabajar con una cúbica más simple. Una cúbica genérica es de la forma

$$\mathcal{C} : a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x^2 + a_6xy + a_7y^2 + a_8x + a_9y + a_{10} = 0. \quad (3.9)$$

Como antes, suponemos que nuestra curva tiene un punto racional $\mathcal{O}$. Homogeneizamos nuestra curva para trabajar en el proyectivo en las variables $[X, Y, Z]$. Tomamos un sistema de referencia de manera que la recta tangente a $\mathcal{C}$ en $\mathcal{O}$ sea $Z = 0$. Esta recta corta a la curva en otro punto, imponemos que $X = 0$ sea la recta tangente a $\mathcal{C}$ en dicho punto. Por último, tomamos como recta $Y = 0$ a una recta cualquiera que pase por $\mathcal{O}$ y que no sea $Z = 0$.



Cambiando a este sistema de referencia la ecuación de la curva en el plano afín queda de la siguiente forma

$$xy^2 + axy + bx = cx^2 + dx + e. \quad (3.10)$$

Multiplicando por x y renombrando xy por y obtenemos

$$y^2 + (ax + b)y = cx^3 + dx^2 + ex. \quad (3.11)$$

Hacemos ahora el cambio de variables lineal $y \to y-(ax+b)/2$ (notemos que para hacer esto el cuerpo sobre el que estemos trabajando no puede ser de característica 2)

$$y^2 = cx^3 + dx^2 + ex. \quad (3.12)$$

Por último, haciendo ahora un cambio lineal dejamos la curva en la forma

$$\mathcal{C} : y^2 = x^3 + Ax + B. \quad (3.13)$$

A esta forma se la conoce como forma normal (breve) de Weierstrass. En el lenguaje de la geometría algebraica hemos probado que toda curva racional es birracionalmente equivalente a una en forma normal de Weierstrass. Esto quiere decir que nos basta estudiar los puntos racionales de las cúbicas en la forma normal de Weiestrass para entender los puntos racionales de las cúbicas en general.

Como dijimos en la introducción nuestro objetivo es estudiar las curvas de género 1 sin puntos singulares. Por la fórmula del género, tenemos que todas las curvas de género 1 sin puntos singulares tienen grado 3. Todas las curvas de grado 3 las podemos pasar a su forma normal de Weierstrass. Veamos cuando las curvas de esta forma tienen puntos singulares. Llamamos $f(x) = x^3 + Ax + B$ y $F(x, y) = y^2 - f(x)$

$$\frac{\partial F(x,y)}{\partial x} = -f'(x), \qquad \frac{\partial F(x,y)}{\partial y} = 2y. \tag{3.14}$$

Por lo que $P = (x, y)$ es singular si, y solo si, $y = 0$ y $f'(x) = 0$. Notemos que en ese caso, $0 = y^2 = f(x)$. De esta manera, C tiene puntos singulares si, y solo si, f tiene raíces múltiples.

Definición 3.1. *Sea C una cúbica en forma normal, diremos que C es una curva elíptica si $f(x)$ no tiene raíces multiples.*

Observación 3.2. La condición de que f no tenga raíces múltiples se puede caracterizar con los coeficientes por medio del discriminante de $f(x)$. Esto es, $f(x)$ tiene raíces múltiples si, y solo si, $\Delta(f) = 4A^3 + 27B^2 = 0$. A este discriminante también se le llama el discriminante de la curva.

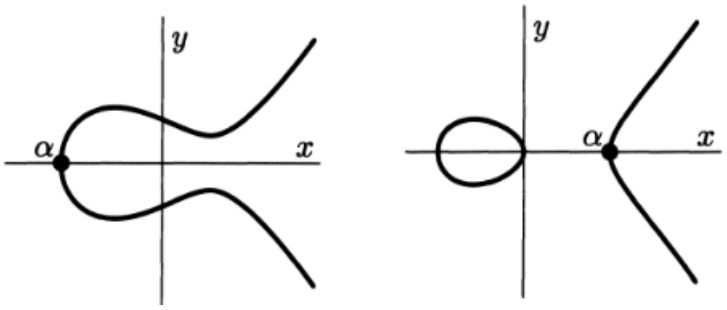
Nuestros esfuerzos se centrarán a partir de ahora en estudiar los puntos racionales de las cúbicas en forma normal. Al estudiar las cúbicas en esta forma la operación de grupo es un poco más sencilla. En primer lugar debemos elegir el punto $\mathcal{O}$ que actuará como elemento neutro. Veamos primero cuáles son los puntos del infinito de las curvas en forma normal. Calculamos $C \cap \{Z = 0\} \subset \mathbb{P}^n$,

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \qquad Z = 0.$$

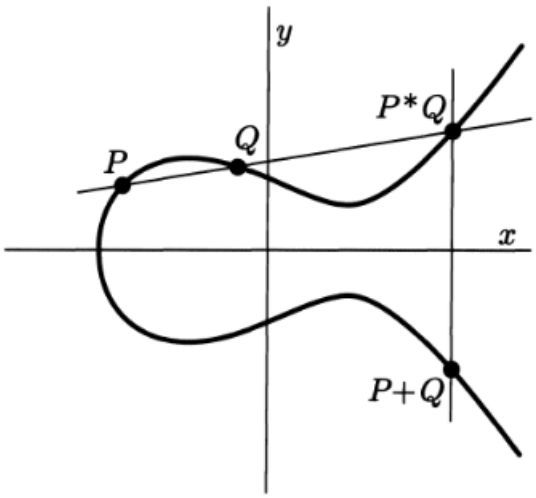
De las ecuaciones se deduce que $X = 0$ y $Z = 0$. Por tanto, C solo tiene un punto proyectivo en el infinito, $[0, 1, 0]$. Este punto es el punto del infinito donde se cortan todas las rectas paralelas al eje Y. De hecho, C tiene un contacto de orden 3 con la recta del infinito, por lo que $[0, 1, 0] * [0, 1, 0] = [0, 1, 0]$.

Esta propiedad simplifica los cálculos y la construcción geométrica a la hora de calcular la suma de puntos. Por lo que siempre que tengamos una curva en su forma normal entenderemos que el elemento neutro del grupo es $\mathcal{O} = [0, 1, 0]$. Vamos a ver geométricamente tanto las curvas como la suma de puntos en esta forma.

La gráfica de la restricción al plano afín real de la curva $y^2 = f(x)$ depende de las raíces de $f(x)$. Si las raíces de $f(x)$ son todas reales la curva tiene dos componentes y si tiene una ráiz la curva solo tiene una componente. En ambos casos la curva es simétrica con respecto al eje x. Estos dos casos se muestran en las siguientes figuras.



Sean ahora $P, Q \in C$ distintos de $\mathcal{O}$, para construir $P + Q$ consideramos la recta PQ que corta a la curva en un punto $P * Q$. Trazamos ahora la recta $O(P * Q)$ que como hemos visto antes es paralela al eje Y. Además la curva es simétrica con respecto al eje X, por lo que el punto $O(P * Q)$ es el simétrico a $P * Q$ con respecto al eje X. De esta manera, para construir el punto correspondiente a la suma de dos puntos afines no necesitamos hacer referencia al punto proyectivo $\mathcal{O}$.



Con esta simplificación de las curvas no será más sencillo estudiar $C(\mathbb{Q})$. Para poder usar las herramientas del capítulo anterior vamos a probar que la operación de grupo que hemos definido es un morfismo entre curvas. Para ello, primero vamos a dar fórmulas explícitas de la suma apoyandonos en como funciona la operación de grupo en las curvas en forma normal normal de Weierstrass.

Sea C una curva elíptica en forma normal de Weierstrass,

$$C : y^2 = x^3 + Ax + B. \tag{3.15}$$

Sea $P_0 = (x_0, y_0)$, es fácil comprobar que $-P_0 = (x_0, -y_0)$. En efecto, la recta que pasa por P_0 y $(x_0, -y_0)$ es paralela al eje Y, por lo que pasa por el punto $\mathcal{O}$. Este punto está en la curva, así que $P_0 * (x_0, -y_0) = \mathcal{O}$. Por la elección del punto $\mathcal{O}$, se tiene que $\mathcal{O} * \mathcal{O} = \mathcal{O}$. De esta manera, $P_0 + (x_0, -y_0) = \mathcal{O}$.

Pasamos a dar ahora formulas para la suma de puntos.Sean $P_i = (x_i, y_i)$ con $i = 1, 2, 3$ tales que:

$$P_1 + P_2 = P_3.$$

Para dar fórmulas, diferenciamos en tres casos:

1. Si $x_1 \neq x_2$, la recta que pasa por P_1 y P_2 es la recta $y = \lambda x + \nu$, con

   $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ y con } \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

   Para calcular la intersección de dicha recta con la curva sustituimos,

   $$y^2 = (\lambda x + \nu)^2 = x^3 + Ax + B.$$

   Las raíces de dicha ecuación son x_1, x_2 y x_3, por lo que tenemos

   $$x^3 - \lambda^2 x^2 + (A - 2\lambda\nu)x + B - \nu^2 = (x - x_1)(x - x_2)(x - x_3).$$

   Por las fórmulas de Cardano-Vieta, $x_1 + x_2 + x_3 = \lambda^2$. De esta manera, hemos conseguido una fórmula para el punto $P_3 = (x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu)$.
2. Si $x_1 = x_2$ y $y_1 = -y_2$, es el caso que acabamos de tratar y $P_1 + P_2 = \mathcal{O}$.
3. Si $P_1 = P_2$, consideramos la recta tangente a la curva en P_1. Nuestra curva está en forma normal, así que mediante derivación implícita, la recta tangente es $y = \lambda x + \nu$, donde

   $$\lambda = \frac{3x_1^2 + A}{2y_1}, \ \nu = y_1 - \lambda x_1.$$

Ahora podemos demostrar lo siguiente:

Teorema 3.2. *Sea $C/\mathbb{Q}$ una curva elíptica. Entonces, la aplicación que suma dos puntos,*

$$\begin{aligned} + : C \times C &\longrightarrow C && (3.16)\\ (P, P) &\longmapsto P + P, && (3.17)\end{aligned}$$

y la que manda cada punto a su opuesto,

$$\begin{aligned} - : C &\longrightarrow C && (3.18)\\ P &\longmapsto -P, && (3.19)\end{aligned}$$

son morfismos.

Demostración. En primer lugar, la aplicación que manda a cada punto a su opuesto, hemos visto que es

$$(x, y) \mapsto (x, -y).$$

Esta aplicación es claramente racional. Como C es una curva regular, por el corolario (2.3) del capítulo anterior, esta aplicación es un morfismo.

Pasamos ahora a estudiar la aplicación que suma dos puntos cualesquiera. Fijamos un punto $\mathcal{O} \neq Q$ sobre C y consideramos la aplicación "traslación por Q",

$$\begin{aligned} \tau_Q : C &\longrightarrow C && (3.20)\\ P &\longmapsto P + Q. && (3.21)\end{aligned}$$

Por las fórmulas de la suma de puntos, esta aplicación es racional. De nuevo, por el corolario (2.3) del capítulo anterior, esta aplicación es un morfismo. De hecho, es un isomorfismo pues tiene inversa.

Por último, consideramos la aplicación $+ : C \times C \longrightarrow C$. Por las fórmulas de la suma de puntos que hemos calculado antes, tenemos que dicha aplicación está definida como un cociente de polinomios en las coordenadas de los puntos de partida, salvo para los pares de puntos de la forma,

$$(P, P), \quad (P, -P), \quad (P, \mathcal{O}), \quad (\mathcal{O}, P).$$

Por tanto, salvo en estos pares, la aplicación es un morfismo. Veamos que en estos puntos también está definida. Sean $Q_1, Q_2 \in E$ puntos arbitrarios, consideramos la siguiente composición,

$$\phi : C \times C \xrightarrow{\tau_{Q_1} \times \tau_{Q_2}} C \times C \xrightarrow{+} C \xrightarrow{\tau_{Q_1}^{-1}} C \xrightarrow{\tau_{Q_2}^{-1}} C.$$

Gracias a la asociatividad y conmutatividad del grupo tenemos que la aplicación se comporta de la siguiente manera,

$$(P_1, P_2) \xrightarrow{\tau_{Q_1} \times \tau_{Q_2}} (P_1 + Q_1, P_2 + Q_2) \tag{3.22}$$

$$\xrightarrow{+} P_1 + Q_1 + P_2 + Q_2 \tag{3.23}$$

$$\xrightarrow{\tau_{Q_1}^{-1}} P_1 + P_2 + Q_2 \tag{3.24}$$

$$\xrightarrow{\tau_{Q_2}^{-1}} P_1 + P_2. \tag{3.25}$$

Como τ_{Q_1} y τ_{Q_2} son isomorfismos, tenemos que ϕ es un morfismo salvo, quizás, en los puntos de la forma,

$$(P - Q_1, P - Q_2), \quad (P - Q_1, -P - Q_2), \quad (P - Q_1, -Q_2), \quad (-Q_1, P - Q_2).$$

Ahora bien, Q_1 y Q_2 son puntos arbitrarios, luego haciendolos variar podemos encontrar un conjunto finito de aplicaciones racionales,

$$\phi_1, \dots, \phi_n : C \times C \longrightarrow C,$$

con las siguientes propiedades:

1. ϕ_1 es la aplicación suma dada por las fórmulas que hemos visto para puntos distintos.
2. Para cada $(P_1, P_2) \in C \times C$, algún ϕ_i está definida en (P_1, P_2).
3. Si ϕ_i y ϕ_j están ambas definidas en (P_1, P_2), entonces $\phi_i(P_1, P_2) = \phi(P_1, P_2)$.

Por tanto, la suma es una aplicación racional definida en todo $C \times C$, luego es un morfismo.

3.3 Estructura de $C(\mathbb{Q})$

En las secciones anteriores hemos simplificado nuestra curva y le hemos dado estructura de grupo abeliano al conjunto de puntos racionales de la curva. Estudiar esta estructura nos será muy útil para obtener información acerca de los puntos racionales de la curva. En esta sección vamos a dar los resultados principales acerca de la estructura de este grupo.

El resultado principal sobre la estructura de $C(\mathbb{Q})$ es el siguiente.

Teorema 3.3 (Mordell-Weil). *Sea C una curva elíptica, entonces $C(\mathbb{Q})$ es un grupo abeliano finitamente generado.*

Observación 3.3. En otras palabras lo que este resultado nos dice es que dada una curva elíptica existe un conjunto finito de puntos racionales sobre la curva de manera que podemos construir todos los demás mediante el procedimiento descrito en las secciones anteriores.

Este teorema fue demostrado por Louis Mordell en 1922 y fue generalizado por André Weil en 1928, en su tesis. Weil probó que $C(K)$ es un grupo abeliano finitamente generado donde K es cualquier extensión finita de $\mathbb{Q}$, lo que se conoce como cuerpo de números. Aunque dar una prueba completa de este teorema se sale de nuestros objetivos, vamos a dar la idea de esta ya que nos ayudará a entender la motivación de ciertas ideas en capítulos posteriores.

La prueba del teorema se divide en dos partes. La primera consiste en demostrar:

Teorema 3.4 (Teorema de la base finita débil). *Sea C una curva elíptica, entonces $C(\mathbb{Q})/2C(\mathbb{Q})$ es finito.*

La segunda parte de la prueba es un argumento de descenso infinito. Para ello, usaremos el siguiente concepto:

Definición 3.2. *Sea $P = [a, b, c] \in C(\mathbb{Q})$ (como curva proyectiva), con $a, b, c \in \mathbb{Z}$ tales que son coprimos 2 a 2. Se define la altura de P como*

$$H(P) = \max\left\{|a|, |b|, |c|\right\}. \tag{3.26}$$

Definimos la altura logarítmica $h(P)$ de P como $\log(H(P))$.

La altura de un punto de racional nos da una medida intuitiva de cómo de complicado es este punto. Para demostrar el teorema se usan los siguientes lemas:

Lema 3.6. Para cada $M \in \mathbb{R}$, el conjunto $\{P \in C(\mathbb{Q}) \ : \ h(P) \leq M\}$ es finito.

Lema 3.7. Sea P_0 un punto racional. Existe una constante real κ_0 que depende de P_0 y de la curva tal que

$$h(P + P_0) \leq 2h(P) + \kappa_0, \quad \forall P \in C(\mathbb{Q}). \tag{3.27}$$

Lema 3.8. Existe una constante real κ que depende de la curva tal que

$$h(2P) \geq 4h(P) - \kappa, \quad \forall P \in C(\mathbb{Q}). \tag{3.28}$$

Con estos lemas ya podemos probar que $C(\mathbb{Q})$ es finitamente generado. De hecho, podemos probar que todo grupo abeliano Γ, con $\Gamma/2\Gamma$ finito y para el que haya definida una función de altura que cumpla los lemas anteriores, es finitamente generado.

Teorema 3.5 (Teorema del Descenso). *Sea Γ un grupo abeliano, y supongamos que existe una función*

$$h : \Gamma \longrightarrow [0, \infty)$$

que cumple las siguientes propiedades:

1. *Para cada número real M, el conjunto $\{P \in \Gamma : h(P) \leq M\}$ es finito.*
2. *Para cada $P_0 \in \Gamma$ existe una constante real κ_0 tal que*

$$h(P + P_0) \leq 2h(P) + \kappa_0, \quad \forall P \in \Gamma. \tag{3.29}$$

3. *Existe una constante real κ tal que*

$$h(2P) \geq 4h(P) - \kappa, \quad \forall P \in \Gamma. \tag{3.30}$$

4. *El grupo $\Gamma/2\Gamma$ es finito.*

Entonces Γ es un grupo finitamente generado.

Demostración. Primero vamos a elegir un representante de cada clase de equivalencia de $\Gamma/2\Gamma$: pongamos $Q_1, \ldots, Q_n$. Esto significa que para cada $P \in \Gamma$ existe i_1 tal que $P - Q_{i_1} \in 2\Gamma$. Luego existe $P_1 \in \Gamma$ tal que $P - Q_{i_1} = 2P_1$.

Análogamente, podemos escribir:

$$\begin{array}{rcl} P_1 - Q_{i_2} & = & 2P_2 \\ P_2 - Q_{i_3} & = & 2P_3 \\ & \vdots & \\ P_{m-1} - Q_{i_m} & = & 2P_m \end{array}$$

Despejando de las ecuaciones anteriores obtenemos

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m. \tag{3.31}$$

En particular, P está en el subgrupo generado por los Q_i y P_m. Veamos que para m suficientemente grande la altura de P_m está acotada. De esta forma los Q_i junto con los puntos cuya altura sea menor que la cota serán los generadores de Γ.

Aplicamos (2) con $P_0 = -Q_i$ y obtenemos que existe κ_i tal que

$$h(P - Q_i) \leq 2h(P) + \kappa_i, \quad \forall P \in \Gamma. \tag{3.32}$$

Tomamos

$$\kappa' = \max_{1 \leq i \leq n} \kappa_i,$$

y sea κ la constante de (3). Consideramos la sucesión $\{P_i\}$ construida como al comienzo de la prueba. De (2) y (3) deducimos lo siguiente:

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1}) - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa,$$

y dividiendo por 4 obtenemos

$$h(P_j) \leq \frac{h(P_{j-1})}{2} + \frac{\kappa' + \kappa}{4} = \frac{3h(P_{j-1})}{4} - \frac{h(P_{j-1}) - (\kappa + \kappa')}{4}.$$

De esta manera, si para algún j, $h(P_j) \geq \kappa + \kappa'$, entonces $h(P_{j+1}) \leq 3h(P_j)/4$. Luego para algún m suficientemente grande $h(P_m) \leq \kappa + \kappa'$. De esta manera, hemos probado que el conjunto

$$\{Q_1, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa + \kappa'\} \tag{3.33}$$

genera Γ.

Con esto hemos demostrado el Teorema de Mordell. Los lemas que hemos usado son relativamente sencillos de probar. Sin embargo, el teorema débil de la base finita es más difícil y es la clave de que funcione esta prueba. Más adelante veremos que hay mucha relación entre el comportamiento de la curva y los grupos $C(\mathbb{Q})/mC(\mathbb{Q})$.

Por ahora vamos a desarrollar qué se puede deducir de $C(\mathbb{Q})$ en virtud de este teorema. Recordemos el Teorema de Estructura de los grupos abelianos finitamente generados.

Teorema 3.6 (Teorema de Estructura de los grupos abelianos finitamente generados). *Sea $\mathcal{G}$ un grupo abeliano finitamente generado. Entonces, de manera única salvo orden:*

$$\mathcal{G} \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_s\mathbb{Z}) \times \mathbb{Z}^r \tag{3.34}$$

con $s, r \geq 0$, $d_i > 0$ y tales que $d_i | d_{i+1}$, $1 \leq i < s$.

Gracias al teorema de Mordell-Weil, podemos aplicar el teorema de estructura a $C(\mathbb{Q})$, esto es

$$C(\mathbb{Q}) \cong T \times \mathbb{Z}^r \tag{3.35}$$

donde T es la torsión. Para entender los puntos racionales de una curva elíptica vamos a estudiar tanto la torsión como la parte libre.

En cuanto a la torsión, del estudio de las curvas elípticas sobre los cuerpos p-ádicos se obtiene el siguiente resultado:

Teorema 3.7 (Nagell-Lutz). *Sea C una curva elíptica racional en forma normal de Weierstrass*

$$y^2 = f(x) = x^3 + Ax - B \tag{3.36}$$

y $P = (x, y) \in C(\mathbb{Q})$ un punto de torsión. Entonces, $x, y \in \mathbb{Z}$. Además, o bien $y = 0$, si P es un punto de orden 2, o bien $y^2 | \Delta(f)$.

Este teorema nos da un algoritmo para el cálculo de la torsión en un número finito de pasos. Pero se puede decir aún más sobre la torsión. Una cuesión interesante es determinar qué ordenes pueden tener los puntos de torsión de una curva elíptica. Este problema se resolvió gracias al siguiente teorema [8].

Teorema 3.8 (Mazur). *Sea C una curva elíptica racional. Llamamos T a la torsión de $C(\mathbb{Q})$. Entonces T es isomorfo a uno de los siguientes grupos:*

1. *El grupo cíclico de orden N con $N \in \{1, \dots, 10, 12\}$.*
2. *El producto de un grupo cíclico de orden 2 y un grupo cíclico de orden $2N$ con $N \in \{1, 2, 3, 4\}$.*

Además todos estos casos se dan.

Con esto, tenemos bien clasificada la torsión de $C(\mathbb{Q})$. Pasamos ahora a hablar de la parte libre de $C(\mathbb{Q})$, que siempre es de la forma $\mathbb{Z}^r$. A r se le llama el rango de la curva elíptica y se denota por $\mathrm{rk}(C(\mathbb{Q}))$. El cálculo del rango de una curva elíptica es aún un problema abierto. De hecho, incluso la pregunta de si el rango de una curva elíptica está acotado es así mismo un problema abierto.

Uno de los principales objetivos del trabajo es explicar la conjetura de Birch y Swinnerton-Dyer, que nos da un método para calcular el rango de una curva elíptica usando herramientas del análisis complejo. Para dar la versión más completa de la conjetura, tenemos que construir el grupo de Tate-Shafarevich. A esta construcción dedicaremos el capítulo siguiente.

4 Construcción del grupo de Tate-Shafarevich

En este capítulo vamos a construir el grupo de Tate-Shafarevich, para ello vamos a comenzar dando ciertas nociones básicas de cohomología de Galois.

4.1 Cohomología de grupos

4.1.1 Cohomología de grupos finitos

En esta sección G será un grupo finito y M un grupo abeliano.

Definición 4.1. *A M se llama G-módulo si hay una aplicación producto exterior $G \times M \longrightarrow M$, que denotamos por σm, tal que cumple:*

1. $1m = m;\ \forall m \in M.$
2. $\sigma(\tau m) = (\sigma\tau)m;\ \forall m \in M,\ \forall \sigma, \tau \in G.$
3. $\sigma(m + m') = \sigma m + \sigma m';\ \forall \sigma \in G,\ \forall m, m' \in M.$

A dicha aplicación se llama acción de grupo y se dice que G actúa sobre M.

Definición 4.2. *Sean M y N G-módulos, un G-homomorfismo es un homomorfismo de $\phi : M \longrightarrow N$ de grupos abelianos que respetan la acción de G, esto es*

$$\phi(\sigma m) = \sigma\phi(m), \quad \forall m \in M,\ \forall \sigma \in G. \tag{4.1}$$

Habitualmente nos interesa saber sobre qué elementos de nuestro grupo abeliano la acción es trivial.

Definición 4.3. *El 0-grupo de cohomología del G-módulo M, denotado $H^0(G, M)$ o M^G, que se define como*

$$H^0(G, M) = \{m \in M \ : \ \sigma m = m, \ \forall \sigma \in G\}, \tag{4.2}$$

es el submódulo de M formado por todos los elementos G-invariantes.

La homología y la cohomología es un campo de estudio muy amplio que en general estudia la información que podemos obtener de ciertas estructuras a través de cadenas de morfismos entre dichas estructuras. Un tipo de cadenas interesante es el siguiente:

Definición 4.4. *Dada una sucesión de homomorfismos de G-módulos*

$$\cdots \longrightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \longrightarrow \ldots \tag{4.3}$$

se dice que es una sucesión exacta si $\mathrm{Img}(f_{n+1}) = \ker(f_n)$ *para todo* $n \in \mathbb{Z}$.

Comenzaremos nuestro estudio de la cohomología con el siguiente resultado general.

Proposición 4.1. Consideramos la siguiente sucesión exacta de G-módulos

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0. \tag{4.4}$$

Entonces, la siguiente sucesión, obtenida restringiendo las aplicaciones a los submódulos de G-invariantes, es exacta:

$$0 \longrightarrow P^G \xrightarrow{\phi^G} M^G \xrightarrow{\psi^G} N^G, \tag{4.5}$$

donde ϕ^G y ψ^G son las restricciones de ϕ a P^G y ψ a M^G respectivamente.

Demostración. Veamos primero que las restricciones están bien definidas. Sea $a \in P^G$ se tiene que $\sigma\phi(a) = \phi(\sigma a) = \phi(a)$ para todo $\sigma \in G$. Luego $\phi(a) \in M^G$. Análogamente, ψ^G también está bien definida.

De la exactitud de (4.4) se deduce que ϕ es inyectiva y ψ es sobreyectiva. Como ϕ es inyectiva cualquier restricción suya también lo es y, por tanto, $\ker(\phi^G) = \{0\}$.

De la exactitud de (4.4) se deduce $\psi \circ \phi$ es la aplicación nula. Como las restricciones están bien definidas $\mathrm{Img}(\phi^G) \subset \ker(\psi^G)$. Recíprocamente, sea $a \in \ker(\psi^G) \subset \ker(\psi) = \mathrm{Img}(\phi)$. Existe $b \in P$ tal que $\phi(b) = a$ por lo que basta ver que b está en P^G. En efecto, $\phi(b) = a = \sigma a = \sigma\phi(b) = \phi(\sigma b)$ y por la inyectividad de $\phi(b) = \sigma b$.

En esta proposición no podemos asegurar la sobreyectividad de la última aplicación. Para medir cuanto falta para que esta sea sobreyectiva construimos las siguientes definiciones.

Observación 4.1. En este contexto, aparecerán homomorfismos de grupos de la forma $\xi : G \longrightarrow M$. Trabajaremos con la siguiente notación, denotaremos la imagen de un elemento $\sigma \in G$ como ξ_σ y si $\tau \in G$ la acción de τ sobre ξ_σ la denotaremos por ξ_σ^τ, esto es:

$$\xi(\sigma) := \xi_\sigma \in M, \qquad \tau\xi(\sigma) := \xi_\sigma^\tau \in M.$$

Definición 4.5. *Sea M un G-módulo. El grupo de 1-cocadenas está definido por*

$$C^1(G, M) = \mathrm{Hom}(G, M) \tag{4.6}$$

esto es, es el conjunto de homomorfismos de grupos de G a M.

El grupo de 1-cociclos está dado por

$$Z^1(G, M) = \{\xi \in C^1(G, M) \mid \xi_{\tau\sigma} = \xi_\sigma^\tau + \xi_\tau,\ \forall \sigma, \tau \in G\}, \tag{4.7}$$

esto es, son los homomorfismos de G en M que verifican $\xi(\tau\sigma) = \tau\xi(\sigma) + \xi(\tau)$.

El grupo de los 1-cobordes está definido por

$$B^1(G, M) = \left\{\xi \in C^1(G, M) \mid \exists m \in M \text{ tal que } \xi_\sigma = m^\sigma - m,\ \forall \sigma \in G\right\}. \tag{4.8}$$

Es fácil comprobar que $B^1(G, M) \subset Z^1(G, M)$. De esta manera, definimos el primer grupo de cohomología, o 1-grupo de cohomología

$$H^1(G, M) = Z^1(G, M) \big/ B^1(G, M). \tag{4.9}$$

Sea $\phi : M \longrightarrow N$ un homomorfismo de G-módulos. Componiendo con ϕ es fácil comprobar que

$$\phi\left(Z^1(G, M)\right) \subset Z^1(G, N), \quad \phi\left(B^1(G, M)\right) \subset B^1(G, N),$$

por lo que ϕ induce una aplicación sobre los grupos de cohomología

$$\phi_* : H^1(G, M) \longrightarrow H^1(G, N).$$

Proposición 4.2. Sea

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0 \tag{4.10}$$

una sucesión exacta de G-módulos. Entonces, se tiene la siguiente sucesión exacta larga

$$0 \longrightarrow H^0(G,P) \longrightarrow H^0(G,M) \longrightarrow H^0(G,N) \xrightarrow{\delta} \\ \xrightarrow{\delta} H^1(G,P) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N),$$

donde δ está definida como sigue:

Sea $n \in H^0(G,N) = N^G$. Elegimos $m \in M$ tal que $\psi(m) = n$, y consideramos la cocadena $\xi \in C^1(G,M)$, que viene dada por,

$$\xi_\sigma = m^\sigma - m. \tag{4.11}$$

Como $n \in N^G$, es fácil comprobar que la imagen de ξ está en $\ker \psi$, que se puede identificar con P por exactitud. Así, se puede comprobar que $\xi \in Z^1(G,P)$ y, de esta manera, definimos $\delta(n)$ como la clase de cohomología en $H^1(G,P)$ del 1-cociclo ξ. Las demás aplicaciones vienen inducidas, de manera natural, por ϕ y ψ.

Demostración. A partir de δ y habida cuenta de la exactitud de la sucesión de la hipótesis, la conclusión es una mera comprobación. ∎

4.1.2 Cohomología de Galois

Sea K un cuerpo perfecto y sea $\overline{K}$ su clausura algebraIca. El grupo que actuará en este caso será $G_{\overline{K}/K}$, sin embargo este grupo no es finito en general. La diferencia fundamental con el caso finito es que a $G_{\overline{K}/K}$ se le da una topología de manera que la acción sea continua (dicha topología se conoce como topología profinita), dando a M la topología discreta. No desarrollaremos la topología de $G_{\overline{K}/K}$ sino que daremos una condición equivalente en términos algebráicos.

Definición 4.6. *Definimos un $G_{\overline{K}/K}$-módulo como un grupo abeliano M sobre el que actúa $G_{\overline{K}/K}$ y se cumple que para cada $m \in M$ existe $K \subset L$, una extensión de índice finito, tal que $m^\sigma = m$, para todo $\sigma \in G_{\overline{K}/L}$.*

Los grupos de cohomología se definen de manera completamente análoga al caso finito, salvo por alguna condición extra impuesta por la topología.

Definición 4.7. *El 0-grupo de cohomología del $G_{\overline{K}/K}$-módulo M, se define como*

$$M^G_{\overline{K}/K} = H^0\left(G_{\overline{K}/K}, M\right) = \left\{ m \in M \ : \ m^\sigma = m, \ \forall \sigma \in G_{\overline{K}/K} \right\}. \tag{4.12}$$

Definición 4.8. *Sea M un $G_{\overline{K}/K}$-módulo. Diremos que $\xi : G_{\overline{K}/K} \longrightarrow M$ es continua (para las topologías mencionadas al principio de la sección) si para cada $m \in M$, $\xi^{-1}(m)$ contiene un subgrupo de $G_{\overline{K}/K}$ de índice finito. Definimos el grupo de 1-cociclos continuos, denotado $Z^1_{cont}(G_{\overline{K}/K}, M)$ al grupo de aplicaciones continuas que cumplen la identidad*

$$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau. \tag{4.13}$$

Por su parte, los cobordes siempre son continuos, por lo que definimos el primer grupo de cohomología del $G_{\overline{K}/K}$-módulo M como;

$$H^1\left(G_{\overline{K}/K}\right) = Z^1_{cont}\left(G_{\overline{K}/K}, M\right) \Big/ B^1\left(G_{\overline{K}/K}, M\right). \tag{4.14}$$

El desarrollo hecho en la sección anterior sigue siendo cierto y las demostraciones son las mismas que en este caso salvo que hay que añadir la condición de continuidad de los cociclos. El resultado que más nos interesa de dicho desarrollo es el siguiente,

Proposición 4.3. Sea

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0 \tag{4.15}$$

una sucesión exacta de $G_{\overline{K}/K}$-módulos. Entonces, existe una sucesión exacta larga

$$0 \longrightarrow H^0\left(G_{\overline{K}/K}, P\right) \longrightarrow H^0\left(G_{\overline{K}/K}, M\right) \longrightarrow H^0\left(G_{\overline{K}/K}, N\right) \xrightarrow{\delta}$$
$$\xrightarrow{\delta} H^1\left(G_{\overline{K}/K}, P\right) \longrightarrow H^1\left(G_{\overline{K}/K}, M\right) \longrightarrow H^1\left(G_{\overline{K}/K}, N\right),$$

donde el homomorfismo δ se define como en el resultado del caso finito.

4.1.3 Cohomología no abeliana

Pasamos ahora a eliminar la condición de que M sea abeliano. De nuevo, empezamos con un grupo finito G y un grupo M sobre el que actúa G. Sin embargo, en este caso eliminaremos la hipótesis de que M sea abeliano. De nuevo definimos el 0-grupo de cohomología como

$$H^0(G, M) = M^G = \{m \in M \ : \ m^\sigma = m, \ \forall \sigma \in G\}. \tag{4.16}$$

Podemos definir tambien el conjunto de 1-cociclos de G en M como el conjunto de las aplicaciones $\xi : G \longrightarrow M$ que cumplen

$$\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau, \quad \forall \sigma, \tau \in G. \tag{4.17}$$

Notemos que, en general, por la no conmutatividad, los cociclos no forman un grupo. Decimos que dos 1-cociclos ξ y ζ son cohomólogos si existe un $m \in M$ tal que

$$m^{\sigma}\xi_{\sigma} = \zeta_{\sigma}m, \quad \forall \sigma \in G. \tag{4.18}$$

Es fácil ver que esto define una relación de equivalencia en el conjunto de los 1-cociclos. Definimos el primer conjunto de cohomología de M, denotado $H^1(G, M)$, es el conjunto de los 1-cociclos, módulo esta relación.

Siguiendo como en la sección anterior, diremos que el grupo de Galois $G_{\overline{K}/K}$ actúa discretamente sobre un grupo M (no abeliano en general) si el estabilizador de cualquier elemento de M es un subgrupo de índice finito en $G_{\overline{K}/K}$. De la misma manera podemos definir un 1-cociclo continuo de $G_{\overline{K}/K}$ a M como una aplicación $\xi : G_{\overline{K}/K} \longrightarrow M$ que cumple la condición de cociclo y es continua para la topología profinita sobre $G_{\overline{K}/K}$ y la discreta en M. Finalmente, decimos que dos cociclos ξ y ζ son cohomólogos si $m^{\sigma}\xi_{\sigma} = \zeta_{\sigma}m$.

Definimos entonces el 0-grupo de cohomología como:

$$H^0\left(G_{\overline{K}/K}, M\right) = M^{G_{\overline{K}/K}} = \{m \in M \ : \ m^{\sigma} = m, \ \forall \sigma \in G\} \tag{4.19}$$

y el primer conjunto de cohomología,

$$H^1\left(G_{\overline{K}/K}, M\right) = \frac{\{ \text{ conjunto de 1-cociclos continuos de } G_{\overline{K}/K} \text{ a } M \ \}}{\text{relación de equivalencia } \textit{ser cohomólogo}}. \tag{4.20}$$

Con esto tenemos suficiente teoría de cohomología para nuestro propósito, en las secciones siguientes se entenderá mejor la motivación de estos conceptos que hemos definido.

4.2 Cohomología de Galois en curvas elípticas

Sea C una curva elíptica definida sobre un cuerpo K, hay una acción natural de $G_{\overline{K}/K}$ en $C(K)$. Para cada $m \geq 2$, podemos construir una sucesión exacta. Para ello, necesitamos el siguiente lema.

Lema 4.1. Sea $P \in C(\overline{K})$, para cada $m \geq 2$ existe $Q \in C(\overline{K})$ tal que $P = mQ$.

Demostración. Basta notar que como $\overline{K}$ es algebraicamente cerrado. Luego $C(\overline{K})$ es una variedad proyectiva y la aplicación $P \mapsto nP$ es un morfismo entre curvas para todo $n \geq 1$. Todo morfismo entre curvas es sobreyectivo o constante. Como $\mathcal{O}$ va a $\mathcal{O}$ y no todos los puntos se anulan al sumarlos n veces, esta aplicación debe ser sobreyectiva, como queríamos demostrar. ∎

Si tomamos como cuerpo $K = \mathbb{Q}$, del lema se deduce que para cada $m \geq 2$ la siguiente sucesión de $G_{\overline{\mathbb{Q}}/\mathbb{Q}}$-módulos es exacta

$$0 \longrightarrow C(\overline{\mathbb{Q}})[m] \longrightarrow C(\overline{\mathbb{Q}}) \xrightarrow{[m]} C(\overline{\mathbb{Q}}) \longrightarrow 0 \tag{4.21}$$

donde $C(\overline{\mathbb{Q}})[m]$ representa el grupo de los puntos $P \in C(\overline{\mathbb{Q}})$ que verifican que $mP = \mathcal{O}$, esto es, los de orden un divisor de m.

Hemos visto en la sección anterior que esto implica que se tiene la siguiente sucesión exacta larga

$$\begin{aligned} 0 \longrightarrow C(\mathbb{Q})[m] \longrightarrow C(\mathbb{Q}) \xrightarrow{[m]} C(\mathbb{Q}) \xrightarrow{\delta} \\ \xrightarrow{\delta} H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]\right) \longrightarrow H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})\right) \xrightarrow{[m]} H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})\right). \end{aligned}$$

De esta sucesión podemos extraer otra tomando cociente en los extremos

$$0 \longrightarrow \frac{C(\mathbb{Q})}{mC(\mathbb{Q})} \xrightarrow{\delta} H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]\right) \longrightarrow H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})\right)[m] \longrightarrow 0. \tag{4.22}$$

El estudio de esta sucesión nos da mucha información sobre la estructura de $C(\mathbb{Q})$. Por ejemplo, el estudio del caso $m = 2$ nos da el teorema débil de la base. La prueba de este teorema se basa en encontrar un subconjunto finito de $H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]\right)$ que contenga a la imagen por δ de $C(\mathbb{Q})/mC(\mathbb{Q})$. Vamos a hacer un estudio similar, cambiando $\mathbb{Q}$ por $\mathbb{Q}_p$. Tenemos la misma sucesión exacta corta,

$$0 \longrightarrow \frac{C(\mathbb{Q}_p)}{mC(\mathbb{Q}_p)} \xrightarrow{\delta} H^1\left(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})[m]\right) \longrightarrow H^1\left(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})\right)[m] \longrightarrow 0. \tag{4.23}$$

Mediante las inclusiones $\mathbb{Q} \subset \mathbb{Q}_p$ y $G_{\overline{\mathbb{Q}}/\mathbb{Q}} \subset G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}$ obtenemos una restricción en los grupos de cohomología y, por tanto, el siguiente diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C(\mathbb{Q})/mC(\mathbb{Q}) & \longrightarrow & H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]\right) & \longrightarrow & H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})\right)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_p C(\mathbb{Q}_p)/mC(\mathbb{Q}_p) & \longrightarrow & \prod_p H^1\left(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})[m]\right) & \longrightarrow & \prod_p H^1\left(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})\right)[m] & \longrightarrow & 0 \end{array} \tag{4.24}$$

En virtud de este diagrama y buscando un grupo que contenga a la imagen de $C(\mathbb{Q})/mC(\mathbb{Q})$ tenemos las siguientes definiciones:

Definición 4.9. *Dada una curva elíptica C y un entero $m \geq 2$. Se define el m-ésimo grupo de Selmer como*

$$S^{(m)}(C/\mathbb{Q}) = \ker\left(H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]\right) \to \prod_p H^1\left(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})\right)\right). \tag{4.25}$$

De manera similar definimos el grupo de Tate-Shafarevich

$$Ш(E/\mathbb{Q}) = \ker\left(H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})\right) \to \prod_p H^1\left(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})\right)\right). \tag{4.26}$$

Notemos que por la conmutatividad del diagrama anterior y la exactitud de las filas la imagen de $C(\mathbb{Q})/mC(\mathbb{Q})$ está contenida en el m-ésimo grupo de Selmer. De hecho, se puede probar [10] (X.4.2) que la siguiente sucesión es exacta

$$0 \to C(\mathbb{Q})/mC(\mathbb{Q}) \to S^{(m)}(C/\mathbb{Q}) \to Ш(C/\mathbb{Q})[m] \to 0. \tag{4.27}$$

Se puede demostrar que todos los grupos de Selmer son finitos, aunque no lo haremos porque se sale de los propósitos del trabajo. En particular, esto demuestra el teorema de la base finita. Más aún, toda esta construcción se puede hacer para un cuerpo de números cualquiera y, de hecho, tanto el Teorema de Mordell como el teorema de la base finita son ciertos en ese caso.

Para dar un significado geométrico a estos grupos y su relación con la estructura de los puntos racionales, estudiaremos en las siguientes secciones los isomorfismos entre curvas y las curvas isomorfas a una dada, en particular nos interesarán los espacios principales homogéneos que son curvas que tendrán una estrecha relación con los grupos de cohomología y los grupos anteriores.

4.3 Twisting

En general, hemos visto que encontrar los puntos de una curva elíptica sobre $\mathbb{Q}$ es un problema difícil. Sin embargo, no hay tanto problema al estudiarlos sobre $\overline{\mathbb{Q}}$. Esta idea motiva esta sección, donde vamos a estudiar los isomorfismos, definidos sobre $\overline{\mathbb{Q}}$, entre curvas definidas sobre $\mathbb{Q}$.

Observación 4.2. Si C es una curva definida sobre $\mathbb{Q}$, denotaremos esto, como anteriormente, por $C/\mathbb{Q}$. Denotaremos al grupo de isomorfismos (definidos sobre $\overline{K}$) de C por $\mathrm{Isom}(C)$ y al subgrupo de isomorfismos definidos sobre K por $\mathrm{Isom}_K(C)$. En este contexto, habitualmente la composición $(\alpha\circ\beta)$ se denota por yuxtaposición $(\alpha\beta)$.

Definición 4.10. *Un twist de una curva $C/\mathbb{Q}$ es otra curva $C'/\mathbb{Q}$ que es isomorfa a C sobre $\overline{\mathbb{Q}}$. Identificaremos dos twists si son isomorfos sobre $\mathbb{Q}$. Al conjunto de los twists de $C/\mathbb{Q}$, módulo $\mathbb{Q}$-isomorfismo, se le denota* $\mathrm{Twist}(C/\mathbb{Q})$.

Sea ahora $C/\mathbb{Q}$ una curva elíptica y $C'/\mathbb{Q}$ un twist de C. Esto signigfica que existe $\phi : C' \longrightarrow C$ un isomorfismo definido sobre $\overline{\mathbb{Q}}$. Nos interesa saber *cuánto le falta* este isomorfismo para estar definido sobre $\mathbb{Q}$. Para medir esto consideramos la aplicación

$$\xi : G_{\overline{\mathbb{Q}}/\mathbb{Q}} \longrightarrow \mathrm{Isom}(C) \quad \xi(\sigma) = \xi_\sigma = \phi^\sigma\phi^{-1} \tag{4.28}$$

De esta manera podemos definir una acción de grupo de $G_{\overline{\mathbb{Q}}/\mathbb{Q}}$ sobre $\mathrm{Isom}(C)$ y podemos usar la maquinaria de cohomología no abeliana de la sección anterior. La relación entre los twists y la cohomología viene dada por el siguiente teorema.

Teorema 4.1. *Sea $C/\mathbb{Q}$ una curva elíptica. Para cada twist $C'/\mathbb{Q}$ de $C/\mathbb{Q}$, elegimos un isomorfismo $\phi : C' \longrightarrow C'$ y definimos la aplicación $\xi_\sigma = \phi^\sigma\phi^{-1}$. Entonces se tiene:*

1. *ξ es un 1-cociclo.*
2. *La clase de cohomología $[\xi]$ está determinada por la clase de equivalencia de C' como twist, i.e. $[\xi]$ no depende de la elección de ϕ. Luego tenemos la siguiente aplicación natural*

$$\mathrm{Twist}(C/\mathbb{Q}) \longrightarrow H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, \mathrm{Isom}(C)\right) \tag{4.29}$$

3. *La aplicación anterior es una biyección.*

Demostración. 1. El resultado se tiene ya que

$$\xi_{\sigma\tau} = \phi^{\sigma\tau}\phi^{-1} = (\phi^\sigma\phi^{-1})^\tau(\phi^\tau\phi^{-1}) = (\xi_\sigma)^\tau\xi_\tau.$$

2. Sea $C''/\mathbb{Q}$ otro twist de $C/\mathbb{Q}$, $\mathbb{Q}$-isomorfo a C'. Sea $\psi : C'' \longrightarrow C$ un $\overline{\mathbb{Q}}$-isomorfismo. Por hipótesis existe un $\mathbb{Q}$-isomorfismo $\theta : C'' \longrightarrow C'$. Consideramos el elemento $\alpha = \phi\theta\phi^{-1} \in \mathrm{Isom}(C)$. Por tanto,

$$\begin{aligned}\alpha^\sigma\left(\psi^\sigma\psi^{-1}\right) &= \left(\phi\theta\psi^{-1}\right)^\sigma\left(\psi^\sigma\psi^{-1}\right) = \phi^\sigma\theta^\sigma\psi^{-1}\\ &= \phi^\sigma\theta\psi^{-1} = \left(\phi^\sigma\phi^{-1}\right)\left(\phi\theta\psi^{-1}\right)\\ &= \left(\phi^\sigma\phi^{-1}\right)\alpha\end{aligned}$$

Esto prueba que $(\psi^\sigma\psi^{-1})$ y $(\phi^\sigma\phi^{-1})$ son cohomólogos.

3. Ver [10] (X.2.2).

4.4 Espacios homogéneos

Ya vimos en la sección 4.2 como aparecía el grupo $H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})\right)$ en nuestro estudio. En esta sección a cada elemento de este grupo le vamos a asociar un cierto twist de nuestra curva que llamaremos espacio homogéneo.

Definición 4.11. *Sea C/K una curva elíptica. Un espacio (principal) homogéneo de C/K es una curva no singular D/K equipada con una acción μ de C en D,*

$$\mu : D \times C \longrightarrow D, \tag{4.30}$$

un morfismo definido sobre $\mathbb{Q}$ que cumple las siguientes propiedades:

1. *$\mu(p, \mathcal{O}) = p$ para todo $p \in D$.*
2. *$\mu(\mu(p, P), Q) = \mu(p, P + Q)$ para todo $p \in D$ y $P, Q \in C$.*
3. *Dados $p, q \in D$ existe un único $P \in C$ que cumple $\mu(p, P) = q$.*

Observación 4.3. A menudo haremos el siguiente abuso de notación $\mu(p, P) = p + P$. Por ejemplo la propiedad (2) con esta notación es $(p + P) + Q = p + (P + Q)$.

Observación 4.4. Por la propiedad (3) podemos definir una *función resta* sobre D

$$\begin{aligned} \nu : D \times D &\longrightarrow C \\ (q, p) &\longmapsto \nu(q, p) = P \in E \text{ tal que } \mu(p, P) = q. \end{aligned}$$

Observemos que la función está, en efecto, bien definida,

Se verá más adelante que ν también es un morfismo definido sobre $\mathbb{Q}$. Análogamente, denotaremos $\nu(q, p) = q - p$. En el siguiente lema veremos que la suma y la resta tienen las propiedades habituales.

Lema 4.2. Sea $D/\mathbb{Q}$ un espacio homogéneo para $C/\mathbb{Q}$. Entonces, dados $p, q \in D$ y $P, Q \in C$ se cumplen los siguientes enunciados

1. $\nu(p, p) = \mathcal{O}$.

2. $\nu(\mu(p,P),p) = P$.
3. $\nu(\mu(q,Q),\mu(p,P)) = \nu(q,p) + Q - P$.

Demostración. 1. Por definición de espacio homogéneo $\mu(p,\mathcal{O}) = p$. Esto junto con la definición de $\nu(p,p)$ nos da la siguiente igualdad

$$\mu(p,\mathcal{O}) = p = \mu(p,\nu(p,p)). \tag{4.31}$$

Como $\nu(p,p)$ es único, $\nu(p,p) = \mathcal{O}$.

2. Por definición de la resta, $\mu(p,\nu(q,p)) = q$. Por lo que

$$\mu(p,\nu(\mu(p,P),p)) = \mu(p,P). \tag{4.32}$$

De nuevo, por la unicidad de la imagen de ν, se tiene que $\nu(\mu(p,P),p) = P$

3. De nuevo,empezamos con

$$q = \mu(p,\nu(q,p)) \tag{4.33}$$

Sumando Q tenemos

$$\begin{aligned}\mu(q,Q) &= \mu(p,\nu(q,p)+Q) = \mu(p,P+\nu(q,p)+Q-P)\\ &= \mu(\mu(p,P),\nu(q,p)+Q-P).\end{aligned}$$

Por la definición de ν esto implica que

$$\nu(\mu(q,Q),\mu(p,P)) = \nu(q,p) + Q - P. \tag{4.34}$$

Usando la otra notación escribimos más habitualmente

1. $p - p = \mathcal{O}$.
2. $(p+P) - p = P$.
3. $(q+Q) - (p+P) = (q-p) + Q - P$.

Para poder aplicar la teoría de la sección anterior vamos a probar que todo espacio homogéneo de $\mathcal{C}/\mathbb{Q}$ es un twist de $\mathcal{C}/\mathbb{Q}$. También vamos a caracterizar la suma y la resta en términos de $\overline{\mathbb{Q}}$- isomorfismos.

Proposición 4.4. Sea $\mathcal{C}/\mathbb{Q}$ una curva elíptica, y sea $\mathcal{D}/\mathbb{Q}$ un espacio homogéneo para $\mathcal{C}/\mathbb{Q}$. Fijado un punto $p_0 \in \mathcal{D}$, definimos la aplicación

$$\theta : \mathcal{C} \longrightarrow \mathcal{D} \qquad \theta(P) = p_0 + P \tag{4.35}$$

Entonces se tiene:

1. θ es un isomorfismo definido sobre $\mathbb{Q}(p_0)$. En particular $\mathcal{D}/\mathbb{Q}$ es un twist de $\mathcal{C}/\mathbb{Q}$.
2. Para todo $p \in \mathcal{D}$ y $P \in \mathcal{C}$,
$$p + P = \theta\left(\theta^{-1}(p) + P\right). \tag{4.36}$$
3. Dados $p, q \in \mathcal{D}$ se cumple,
$$q - p = \theta^{-1}(q) - \theta^{-1}(p). \tag{4.37}$$
4. La aplicación resta es un morfismo definido sobre $\mathbb{Q}$.

Demostración. 1. La acción de $\mathcal{C}$ sobre $\mathcal{D}$ está definida sobre $\mathbb{Q}$. Entonces, sea $\sigma \in G_{\overline{\mathbb{Q}}/\mathbb{Q}}$ tal que $p_0^\sigma = p_0$. Tenemos
$$\theta(P)^\sigma = (p_0 + P)^\sigma = p_0^\sigma + P^\sigma = p_0 + P^\sigma = \theta(P^\sigma). \tag{4.38}$$
Luego θ está definida sobre $\mathbb{Q}(p_0)$. Por la propiedad (3) de espacio principal homogéneo y por el lema anterior θ^* tiene grado 1. Como se vio en el capítulo de geometría algebraica, todo morfismo de grado 1 entre curvas regulares es un isomorfismo.

2. Se tiene que:
$$\theta(\theta^{-1}(p) + P) = p_0 + \theta^{-1}(p) + P = p + P \tag{4.39}$$
Notemos que en la última igualdad se ha usado la definición de θ^{-1}.

3. Se tiene que:
$$\theta^{-1}(q) - \theta^{-1}(p) = (p_0 + \theta^{-1}(q)) - (p_0 + \theta^{-1}(p)) = q - p. \tag{4.40}$$

4. Habida cuenta de que la resta dentro de una curva elíptica en un morfismo, ν es un morfismo por el apartado anterior. Veamos que ν está definido sobre $\mathbb{Q}$. Sea $\sigma \in G_{\overline{\mathbb{Q}}/\mathbb{Q}}$, usando el apartado anterior tenemos que
$$\begin{aligned}(q-p)^\sigma &= (\theta^{-1}(q) - \theta^{-1}(p))^\sigma = \theta^{-1}(q)^\sigma - \theta^{-1}(p)^\sigma \\ &= \left[p_0 + \theta^{-1}(q)\right]^\sigma - \left[p_0 + \theta^{-1}(p)\right]^\sigma = q^\sigma - p^\sigma.\end{aligned}$$
La segunda igualdad se deduce de que la resta sobre las curvas elípticas está definida sobre $\mathbb{Q}$ y la tercera igualdad se deduce de que la acción está definida sobre $\mathbb{Q}$.

Definición 4.12. *Diremos que dos espacios homogéneos $\mathcal{D}/\mathbb{Q}$ y $\mathcal{D}'/\mathbb{Q}$ para $\mathcal{C}/\mathbb{Q}$ son equivalentes si existe un isomorfismo $\theta : \mathcal{D} \longrightarrow \mathcal{D}'$ definido sobre $\mathbb{Q}$ tal que*

$$\theta(p+P) = \theta(p) + P, \qquad \forall p \in \mathcal{D},\ \forall P \in \mathcal{C}. \tag{4.41}$$

A la clase de equivalencia que contiene a $\mathcal{C}$, actuando sobre sí misma por traslaciones, la llamaremos la clase trivial. A la colección de todas las clases de equivalencia de espacios homogéneos para $\mathcal{C}/\mathbb{Q}$ la llamaremos el grupo de Weil-Châtelet de $\mathcal{C}/\mathbb{Q}$ y la denotaremos $\mathrm{WC}(\mathcal{C}/\mathbb{Q})$ *(se verá más adelante que, en efecto, es un grupo).*

Proposición 4.5. Sea $\mathcal{D}/\mathbb{Q}$ un espacio homogéneo de $\mathcal{C}/\mathbb{Q}$. Entonces, $\mathcal{D}/\mathbb{Q}$ está en la clase trivial si y solo si $\mathcal{D}(\mathbb{Q})$ es no vacío.

Demostración. Si $\mathcal{D}/\mathbb{Q}$ está en la clase trivial existe un $\mathbb{Q}$-isomorfismo $\theta : \mathcal{C} \longrightarrow \mathcal{D}$ y, por tanto, $\theta(\mathcal{O}) \in \mathcal{D}(\mathbb{Q})$.

Recíprocamente, supongamos que existe $p_0 \in \mathcal{D}(\mathbb{Q})$. Entonces, consideramos la aplicación

$$\theta : \mathcal{C} \longrightarrow \mathcal{D} \qquad \theta(P) = p_0 + P \tag{4.42}$$

que por la proposición anterior es un isomorfismo definido sobre $\mathbb{Q}(p_0) = \mathbb{Q}$. La compatibilidad del morfismo con la acción en este caso se traduce en

$$p_0 + (P+Q) = (p_0 + P) + Q, \tag{4.43}$$

que se tiene por la definición de espacio principal homogéneo. ∎

Observación 4.5. Esta última proposición nos da una condición equivalente en términos de espacios homogéneos al problema de la existencia de puntos racionales. Ahora vamos a relacionar el grupos de Weil-Châtelet con la cohomología.

Lema 4.3. Sea $\theta : \mathcal{D}/\mathbb{Q} \longrightarrow \mathcal{D}'/\mathbb{Q}$ una equivalencia de espacios homogéneos para $\mathcal{C}/\mathbb{Q}$. Entonces,

$$\theta(q) - \theta(p) = q - p, \qquad \forall p, q \in \mathcal{D}. \tag{4.44}$$

Demostración. Basta aplicar de manera conveniente las definiciones

$$\begin{aligned} \theta(q) - \theta(p) &= ([\theta(q) + (p-q)] - \theta(p)) + (q-p) \\ &= (\theta\,[q + (p-q)] - \theta(p)) + (q-p) = q - p. \end{aligned}$$

∎

Teorema 4.2. *Sea $\mathcal{C}/\mathbb{Q}$ una curva elíptica. Hay una biyección natural*

$$\mathrm{WC}(\mathcal{C}/\mathbb{Q}) \longrightarrow H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, \mathcal{C}(\mathbb{Q})\right) \tag{4.45}$$

definida como sigue:

Sea $\mathcal{D}/\mathbb{Q}$ un espacio homogéneo, y sea $p_0 \in \mathcal{D}$. Entonces,

$$\left[\mathcal{D}/\mathbb{Q}\right] \mapsto \left[\sigma \mapsto \left(p_0^\sigma - p_0\right)\right] \tag{4.46}$$

(Los corchetes $[\cdot]$ denotan clases de equivalencia.)

Demostración. Veamos primero que la aplicación está bien definida. La aplicación $\sigma \mapsto p_0^\sigma - p_0$ es claramente un cociclo:

$$p_0^{\sigma\tau} - P_0 = (p_0^{\sigma\tau} - p_0^\tau) + (p_0^\tau - p_0) = (p_0^\sigma - p_0)^\tau + (p_0^\tau - p_0). \tag{4.47}$$

Sean ahora $\mathcal{D}'/\mathbb{Q}$ un espacio homogéneo equivalente a $\mathcal{D}/\mathbb{Q}$. Sea $\theta : \mathcal{D} \longrightarrow \mathcal{D}'$ un $\mathbb{Q}$-isomorfismo que nos da la equivalencia, y sea $p_0' \in \mathcal{D}'$. Usamos ahora el lema anterior:

$$p_0^\sigma - p_0 = \theta(p_0^\sigma) - \theta(p_0) = \left((p_0')^\sigma - (p_0')\right) + \left((\theta(p_0) - p_0')^\sigma - (\theta(p_0) - p_0')\right). \tag{4.48}$$

De esta manera, los cociclos $p_0^\sigma - p_0$ y $(p_0')^\sigma - p_0'$ se diferencian en el coborde generado por el punto $\theta(p_0) - p_0' \in \mathcal{C}$. Luego $\left[p_0^\sigma - p_0\right] = \left[(p_0')^\sigma - p_0'\right] \in H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, \mathcal{C}\right)$.

Veamos la inyectividad, supongamos que los cociclos $p_0^\sigma - p_0$ y $(p_0')^\sigma - p_0'$ corespondientes a $\mathcal{D}$ y $\mathcal{D}'$ respectivamente son cohomólogos. Esto significa que existe $P_0 \in \mathcal{C}$ tal que

$$p_0^\sigma - p_0 = (p_0')^\sigma - p_0' + (P_0^\sigma - P_0,) \qquad \forall \sigma \in G_{\overline{\mathbb{Q}}/\mathbb{Q}}. \tag{4.49}$$

Consideramos la aplicación

$$\theta : \mathcal{D} \longrightarrow \mathcal{D}', \qquad \theta(p) = p_0' + (p - p_0) + P_0. \tag{4.50}$$

Entonces θ es un $\overline{\mathbb{Q}}$-isomorfismo que es compatible con las acciones de $\mathcal{C}$ sobre $\mathcal{D}$ y $\mathcal{D}'$. Veamos que θ está definido sobre $\mathbb{Q}$

$$\begin{aligned} \theta(p)^\sigma &= (p_0')^\sigma + (p^\sigma - p_0^\sigma) + P_0^\sigma \\ &= p_0' + \left(p^\sigma - p_0\right) + P_0 + \left((p_0')^\sigma - p_0' + P_0^\sigma - P_0 - (p_0^\sigma - p_0)\right) = \theta(p^\sigma). \end{aligned}$$

Luego $\mathcal{D}$ y $\mathcal{D}$' son equivalentes.

Falta probar la sobreyectividad. Sea $\xi : G_{\overline{\mathbb{Q}}/\mathbb{Q}} \longrightarrow \mathcal{C}$ un cociclo representante de su clase en $H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\mathbb{Q})\right)$. Incrustamos $\mathcal{C}$ en Isom($\mathcal{C}$) (el grupo de los isomorfismos

de C) mandando $P \in C$ a la traslación $\tau_P \in \mathrm{Isom}(C)$. De esta manera, podemos ver ξ en el conjunto de cohomología $H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, \mathrm{Isom}(C)\right)$. Por la biyección que construimos en la sección anterior, existe una curva $D/\mathbb{Q}$ y un $\overline{\mathbb{Q}}$-isomorfismo $\phi : D \longrightarrow C$ tal que para todo $\sigma \in G_{\overline{\mathbb{Q}}/\mathbb{Q}}$

$$\phi^\sigma \circ \phi^{-1} = (\text{traslación por -}\xi_\sigma) \tag{4.51}$$

(usaremos -ξ en vez de ξ para hacer más sencilla la prueba). Definimos una aplicación

$$\mu : D \times C \longrightarrow D \qquad \mu(p, P) = \phi^{-1}(\phi(p) + P). \tag{4.52}$$

Veamos que μ le da a $D/\mathbb{Q}$ estructura de espacio homogéneo sobre $C/\mathbb{Q}$. Las dos primeras propiedades de espacio homogéneo se verifican fácilmente. Sean $p, q \in D$, por definición tenemos que

$$\mu(p, P) = q \iff \phi^{-1}\left(\phi(p) + P\right) = q, \tag{4.53}$$

y, por tanto, $P = \phi(q) - \phi(p)$ está unívocamente determinado. Falta verificar que μ está definido sobre $\mathbb{Q}$. Sea $\sigma \in G_{\overline{\mathbb{Q}}/\mathbb{Q}}$, tenemos que

$$\mu(p, P)^\sigma = (\phi^{-1})^\sigma(\phi^\sigma(p^\sigma) + P^\sigma) = \phi^{-1}\left((\phi(p^\sigma) - \xi_\sigma + P^\sigma) + \xi_\sigma\right) = \mu(p^\sigma, P^\sigma).$$

Luego, en efecto $D/\mathbb{Q}$ es un espacio homogéneo para $C/\mathbb{Q}$. Por último vamos a calcular la clase de cohomología asociada a $D/\mathbb{Q}$. Tomamos como $p_0 \in D$ el punto $\phi^{-1}(\mathcal{O})$, de esta manera,

$$p_0^\sigma - p_0 = (\phi^\sigma)^{-1}(\mathcal{O}) - \phi^{-1}(\mathcal{O}) = \phi^{-1}(\mathcal{O} + \xi_\sigma) - \phi^{-1}(\mathcal{O}) = \xi_\sigma. \tag{4.54}$$

La segunda igualdad se deduce de (4.53) y la tercera del apartado (3) de la proposición 4.4. Con esto concluye la prueba.

4.5 Reflexiones finales

Estamos ahora en posición de entender mejor los grupos de Selmer y Tate-Shafarevich. Recordemos que usando los resultados de cohomología del principio del capítulo habíamos construido el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C(\mathbb{Q})/mC(\mathbb{Q}) & \longrightarrow & H^1(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]) & \longrightarrow & H^1(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}_p}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_p^\infty C(\mathbb{Q}_p)/mC(\mathbb{Q}_p) & \longrightarrow & \prod_p^\infty H^1(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p})[m]) & \longrightarrow & \prod_p^\infty H^1(G_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}, C(\overline{\mathbb{Q}_p}))[m] & \longrightarrow & 0 \end{array} \tag{4.55}$$

Gracias a la relación entre el primer grupo de cohomología y los espacios homogéneos vista en la sección anterior podemos identificar $H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}_p})\right)$ con el grupo de Weil-Châtalet. La motivación principal de estudiar los grupos de Selmer es para probar que $C(\mathbb{Q})/mC(\mathbb{Q})$ es finito. Intentar probar esto directamente es tremendamente complicado. $C(\mathbb{Q})/mC(\mathbb{Q})$ se puede identificar con

$$\ker\left[H^1\left(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, C(\overline{\mathbb{Q}})[m]\right) \to \mathrm{WC}(C/\mathbb{Q}_p)\right]$$

por la exactitud del diagrama anterior. Hemos visto en la sección anterior que saber si un elemento del grupo de Weil-Châtelet es trivial es equivalente a saber si unas curvas (de género 1) tienen puntos racionales. Este problema es extremadamente difícil y hace que sea inarbordable el cálculo de estos núcleos. Por esta razón es razonable mayorar estos núcleos por un grupo un poco más grande. De hecho, gracias a un resultado de análisis p-ádico en el que no ahondaremos los grupos de Selmer se pueden computar fácilmente.

Por su parte, el grupo de Tate-Shafarevich con esta nueva identificanción es

$$Ш(C/\mathbb{Q}) = \ker\left(\mathrm{WC}\left(C/\mathbb{Q}\right) \to \prod_p^\infty \mathrm{WC}\left(C/\mathbb{Q}_p\right)\right). \tag{4.56}$$

De nuevo, por el resultado que nos caracteriza los elementos triviales del grupo de Weil-Châtelet, podemos ver $Ш(C/\mathbb{Q})$ como los espacios homogéneos de $C/\mathbb{Q}$ que son no vacíos en todos los cuerpos p-ádicos y en $\mathbb{R}$. En cierta forma esta es una manera de medir por cuánto falla el principio de Hasse para una curva elíptica dada. Como ya hemos mencionado antes los grupos de Selmer son finitos, sin embargo no se sabe si el grupo de Tate-Shafarevich lo es. De hecho, a este problema se le conoce como la conjetura de Tate-Shafarevich. Este problema está muy relacionado con uno de los problemas del milenio la conjetura de Birch y Swinnerton-Dyer. Para una mejor comprensión de la conjetura, antes de enunciarla vamos a dar una breve explicación de la relación que hay entre el estudio de las curvas elípticas en los cuerpos $\mathbb{Q}_p$ y $\mathbb{F}_p$.

Sea p un primo y consideremos el espacio proyectivo $\mathbb{P}^2(\mathbb{Q}_p)$. Sea, $[x, y, z] \in \mathbb{P}^2(\mathbb{Q}_p)$ un punto, notemos que multiplicando por un escalar adecuado siempre podemos suponer que

$$\text{máx}\left\{|x|_p, |y|_p, |z|_p\right\} = 1,$$

o, equivalentemente, que $x, y, z \in \mathbb{Z}_p$. Recordemos que todo entero p-ádico se podía escribir como una serie de potencias en p con coeficientes en $\{0, \cdots, p-1\}$. Podemos ahora definir un homomorfismo de reducción,

$$\begin{aligned} \text{red} : \mathbb{Z}_p &\longrightarrow \mathbb{F}_p \\ \sum_{n=0}^{\infty} a_n p^n &\longmapsto a_0. \end{aligned}$$

Si $x \in \mathbb{Z}_p$ denotaremos su reducción como $\overline{x}$. De esta manera, tenemos la siguiente aplicación natural,

$$\text{red} : \mathbb{P}^2(\mathbb{Q}_p) \longrightarrow \mathbb{P}^2(\mathbb{F}_p),$$

que manda el punto $[x, y, z]$, con $\text{máx}\left\{|x|_p, |y|_p, |z|_p\right\} = 1$, al punto $\left[\overline{x}, \overline{y}, \overline{z}\right]$. Naturalmente, esta aplicación está bien definida. Pasamos ahora a explicar la conjetura.

Dada una curva elíptica definida sobre los racionales,

$$C : y^2 = x^3 + ax + b,$$

podemos suponer que $a, b \in \mathbb{Z}$. En caso contrario, si p es un primo que divide al denominador de a o de b, basta hacer el cambio de variable $x = x'/p^2$ e $y = y'/p^3$ para obtener otra ecuación en forma normal en las que p no divide al denominador de los coeficientes de la ecuación. Fijamos ahora un primo p, podemos ver la ecuación de la curva como una ecuación en el cuerpo $\mathbb{F}_p$. Definimos las siguientes cantidades,

$$N_p := \#\left\{(x, y) \in \mathbb{F}_p^2 \ : \ y^2 \equiv x^3 + ax + b \mod p\right\}, \tag{4.57}$$

$$a_p := p - N_p. \tag{4.58}$$

Gracias a estas cantidades podemos asociar una función holomorfa a cada curva elíptica, esta se puede definir como el siguiente producto infinito,

$$L(C, s) = \prod_{p \nmid 2\Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1},$$

donde Δ es el discriminante de la curva. Esta función es un producto de Euler, y por los resultados de convergencia de este tipo de productos, la función converge

en $\mathcal{R}(s) > 3/2$. Estos resultados de convergencia se han visto en las asignaturas de Teoría Analítica de Números y Variable Compleja. A esta función se la suele llamar la L-serie incompleta (ya que faltan los términos en los que $p|\Delta$) asociada a la curva C. El nombre de serie viene porque la función también tiene una representación como serie de Dirichlet. Se puede probar que esta función tiene una prolongación analítica a todo el plano complejo. Ya estamos en condiciones de enunciar la primera versión de la conjetura, que fue la que originalmente plantearon Birch y Swinnerton-Dyer.

Conjetura 4.1. *Sea C una curva elíptica. El desarrollo de Taylor de $L(C, s)$ en $s = 1$ tiene la forma,*

$$L(C, s) = c(s-1)^r + \textit{(términos de orden superior)}$$

con $c \neq 0$ y $r = \mathrm{rk}(C(\mathbb{Q}))$.

En la versión más refinada de la conjetura se añaden a la L-serie un factor por cada primo que divide a Δ. Denotaremos a esta nueva función por L^*. Esta versión, nos da además el coeficiente de Taylor de la L-serie.

Conjetura 4.2. *Sea C una curva elíptica. El desarrollo de Taylor de $L^*(C, s)$ en $s = 1$ tiene la forma,*

$$L^*(C, s) = c^*(s-1)^r + \left\{ \textit{términos de orden superior} \right\},$$

con $r = \mathrm{rk}(C(\mathbb{Q}))$ y

$$c^* = \frac{2^r \Omega \cdot |Ш(C/\mathbb{Q})| \cdot R(C/\mathbb{Q}) \cdot \prod_p c_p}{|C_T(\mathbb{Q})|^2}, \tag{4.59}$$

donde:

1. $\Omega = \int_{C(\mathbb{R})} |\omega|$ *donde ω es la forma diferencial $dx/2y$.*
2. $C_T(\mathbb{Q})$ *es la torsión del grupo $C(\mathbb{Q})$.*
3. $Ш(C/\mathbb{Q})$ *es el grupo de Tate-Shafarevich, al que hemos dedicado este capítulo. Como hemos dicho antes, la finitud del grupo de Tate-Safarevich no está probada a día de hoy, por lo que una prueba de esta conjetura requeriría también una prueba de que el grupo de Tate-Shafarevich es finito.*
4. c_p *se define como el orden del grupo $C(\mathbb{Q}_p)/C_0(\mathbb{Q}_p)$, donde $C_0(\mathbb{Q}_p)$ es el conjunto de los puntos de $C(\mathbb{Q}_p)$ tales que su reducción módulo p es un punto no singular de la curva C, entendida como el conjunto de puntos que son solución de la ecuación de $C/\mathbb{F}_p$ módulo p. Se puede probar que es un grupo y que $|C(\mathbb{Q}_p)/C_0(\mathbb{Q}_p)|$ es finito.*

5. *$R(C/\mathbb{Q})$ se denomina el regulador de la curva. En el capítulo 3, hicimos un esbozo de la prueba del Teorema de Mordell en la que usamos una función llamada altura. Las funciones altura son una familia de funciones con propiedades similares a las que le pedimos a nuestra función en el capítulo 3. Hay una manera canónica de definir la función altura de una curva elíptica. A esta función la denotaremos $\overline{h}$. Podemos definir la forma bilineal,*

$$\langle \cdot, \cdot \rangle : C(\overline{\mathbb{Q}}) \times C(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R},$$

dada por,

$$\langle P, Q \rangle = \overline{h}(P + Q) - \overline{h}(P) - \overline{h}(Q).$$

Dados $P_1, \ldots, P_r \in C(\mathbb{Q})/C_T(\mathbb{Q})$ genradores de dicho grupo, definimos el regulador de C sobre $\mathbb{Q}$ como

$$R(C/\mathbb{Q}) = \det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}.$$

De ser cierta la conjetura, dispondríamos de un método para calcular el rango de cualquier curva elíptica. Esto unido a los teoremas que tenemos sobre la torsión nos permitiría clasificar el grupo de cualquier curva elíptica. En particular, esto nos daría un criterio para saber si una curva elíptica tiene puntos racionales o no.

Con esto finalizamos el propósito del trabajo, construir el grupo de Tate-Shafarevich y entender la conjetura de Birch y Swinnerton-Dyer.

Bibliografía

[1] Michael F. Atiyah; Ian G. Mcdonald , 'Introducción al Álgebra Conmutativa'. *Ed. Reverté* (1978).

[2] J. W. S. Cassels, 'Lectures on Elliptic Curves'. *Cambridge, London Mathematical Society Student Texts*.

[3] Alberto Castaño; Luís Narváez, Notas de Teoría de Álgebra Conmutativa y Geometría Algebraica. Curso 2021/22.

[4] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73** (1983) 349–366.

[5] William Fulton, 'Algebraic curves'. Edición original en Benjamin, versión actualizada accesible libremente en https://dept.math.lsa.umich.edu/ wfulton/

[6] Robin Harstshorne, 'Algebraic Geometry'. *Springer, Graduate Text in Mathematics* (1977).

[7] Frances Kirwan, 'Complex algebraic curves'. *Cambridge, London Mathematical Society Student Texts* (1992).

[8] Barry Mazur, *Rational isogenies of prime degree*. Invent. Math. **44** (1978) 129–162.

[9] J.P. Serre, 'A course in Arithmetic'. *Springer-Verlag, Graduate Text in Mathematics* (1996).

[10] Joseph H. Silverman, 'The Arithmetic of Elliptic Curves'. *Springer* 2nd Edition (1986).

[11] John Tate; Joseph H. Silverman, 'Rational Points on Elliptic Curves'. *Springer*.

[12] Oscar Zariski; Pierre Samuel, 'Commutative Algebra'. *Springer, Graduate Text in Mathematics* (1960).