UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

DIVISION DE ESTUDIOS DE POSGRADO

CURVAS ELIPTICAS DE RANGO MAYOR

T E S I S

PARA OBTENER EL GRADO ACADEMICO DE

MAESTRIA EN CIENCIAS (MATEMATICAS)

P R E S E N T A :

MAT. ARMANDO PAULINO PRECIADO BABB

DIRECTOR: DR. RODOLFO SAN AGUSTIN CHI.

MEXICO, D. F. 2000

Agradecimientos

Durante los estudios de la maestría he convivido con campañeros y profesores, a los cuales quiero agradecer por el simple hecho de haber compartido con ellos el tiempo de estudio. Me refiero a compañeros como Dino, los Gemelos, Mito, Mica, Larisa, Andrés y Barbas; y a profesores como Emilio, Javier, Cristoff Paco y Víctor. Además de agradecer a otros compañeros que por falta de memoria omito en esta lista.

Agradezco al personal del instituto de matemáticas de Cuernavaca en el que figuran personas como Gaby, Margaretta, José Luis y Nora por ser tan agradables compañeros. Y a Jorge Luis en particular quien me dio recomendaciones para los primeros capítulos de este trabajo. Además quiero agradecer a profesores como José Luis Cisneros, Pepe Seade, Araceli y por supuesto a Alberto Verjovsky por su ayuda tanto en esta tesis como en otras ocasiones en las que he recibido apoyo de su parte. También quiero agradecer la ayuda que he recibido de Paty, Mary y Lizbeth (secretarias del instituto). Y más aún de agradecer por las revisiones a este trabajo y por la ayuda que he recibido de su parte en distintos momentos, me permito proponer a Emigdio Martinez (Mito) como sinodal no oficial de esta tesis.

Otras personas que han sido de gran ayuda para mi desarrollo académico son mi familia, de quien también me siento muy agradecido: mi madre por supuesto, Ulises, Juan Carlos por la ayuda desde lejos, a Katty y a Jup.

Me siento sumamente agradecido con CONACYT por el apoyo que recibí durante los estudios con la beca correspondiente y que sin ésta me hubiera sido muy difícil, si no es que imposible, hacer la maestría.

Para concluir quiero agradecer también a Granny, a quien dedico con cariño esta tesis.

Índice General

Introducción

Dada una ecuación definida por un polinomio con coeficientes enteros, nos podemos preguntar por las soluciones dentro de los números racionales de esta ecuación. Este es un problema bastante antiguo y se cataloga dentro de la teoría de ecuaciones Diofantinas. En particular nos interesarán ecuaciones con dos incógnitas. El caso más simple es cuando se tiene una función lineal, en el cual tenemos una infinidad de soluciones (todos los puntos racionales de una recta). Si tomamos ecuaciones de grado dos (cónicas), entonces también tenemos el problema resuelto. En este caso si existe un punto cuyas coordenadas sean dos números racionales, entonces cada recta definida con coeficientes racionales que pase por este punto cortará a la curva en un segundo punto también con coordenadas racionales (puede ser el mismo punto y en este caso la recta es la tangente a la curva). Un clásico ejemplo es la caracterización de todas las ternas pitagóricas de números enteros, es decir las ternas de enteros a, b, c, con $c \neq 0$, tales que:

$$a^2 + b^2 = c^2.$$

Cada terna pitagórica (a, b, c) representa una solución racional $(\frac{a}{c}, \frac{b}{c})$ de la ecuación

$$x^2 + y^2 = 1,$$

por lo que podemos reducir el problema a encotrar las soluciones racionales de esta última ecuación. El punto $(0, 1)$ es solución de esta ecuación y a partir de éste podemos construir todas las demás soluciones usando las rectas definidas por ecuaciones con coeficientes racionales ya que estas cortarán en puntos Q que también tienen coordenadas racionales (ver figura 1).

El siguiente caso son las curvas definidas por polinomios de grado tres. Este tipo de curvas tienen a lo más un punto singular, además si dicha curva puede ser definida por un polinomio con coeficientes racionales, entonces su punto singular también tiene coeficientes racionales. En este caso cualquier recta definida sobre los racionales que pase por este punto cortará a la curva en otro punto con coordenadas racionales, por lo que todos puntos racionales quedan determinados de esta forma. Así, pasamos al problema de curvas suaves definidas por polinomios de grado tres.

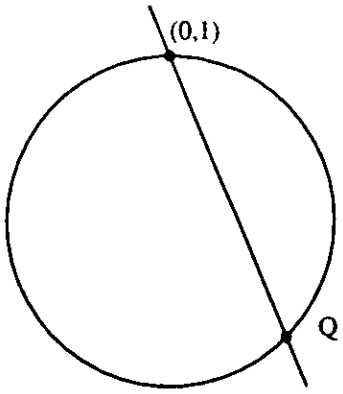

Figura 1: Puntos racionales en la circunferencia unitaria

Una curva elíptica es una curva suave de género igual a uno. Se sabe que estas curvas se pueden representar por polinomios de grado tres, así es que son el siguiente paso en el estudio de puntos racionales de curvas planas.

Usando las propiedades de que una recta corta a una curva definida por un polinomio de grado tres en tres puntos, contando multiplicidades; y que si corta en dos entonces corta en un tercero, es posible definir una operación de suma de los puntos racionales de las curvas elípticas, escogiendo primero un punto como el neutro de dicha operación. El conjunto de puntos racionales de una curva de este tipo resulta ser un grupo conmutativo conocido como el grupo de Mordell-Weil. Este grupo es finitamente generado, por lo que basta con conocer un conjunto de generadores para tener determinados todos los puntos racionales de dicha curva. Tenemos entonces que el grupo de puntos racionales de una curva elíptica es de la forma

$$Tor \times \mathbb{Z}^r,$$

donde r se le conoce como el rango de la curva. Curiosamente la parte de torsión de dicho grupo es fácil de calcular, pero el rango es bastante difícil. Se conjetura que existen curvas elípticas de rango arbitrario, pero sólo se han encontrado curvas con al menos 23 generadores, no se sabe si estas curvas tienen ese número como rango pero al menos es una cota inferior.

Existe el problema similar de buscar curvas de este tipo definidas sobre campos finitos, tales que tengan el mayor número de puntos posible. Estos dos problemas están relacionados entre sí como se verá durante esta tesis.

Este problema tiene aplicaciones a otras áreas como a la criptografía (ver [Len87] y [Kob87]) y a la física (ver [Wal90]). El problema por sí sólo tiene aspectos interesantes en la matemática pura.

Esta tesis tiene como primer objetivo dar una introducción al estudio de curvas elípticas desde el punto de vista de la aritmética, enfocado al estudio del grupo de Mordell-Weil de dichas curvas. Se presentan los principales resultados

al respecto además de las herramientas con las que se ha atacado el problema. También se da una amplia referencia de trabajos publicados (libros, revistas y páginas electrónicas) al respecto. El segundo objetivo de esta tesis es estudiar la forma en la que se han encontrado recientemente curvas elípticas de rango grande. En 1991 J-P Mestre publica un artículo en el que genera familias de curvas con rango al menos once. De ahí en adelante todos los avances han sido usando la misma técnica o de forma muy similar. En algunas ocasiones se han hecho búsquedas exhaustivas en las familias de curvas que Mestre dió con el fin de encontrar curvas de rango más grande.

La información que se presenta en este trabajo esta organizada de la siguiente forma: En los primeros dos capítulos se presentan aspectos generales de la geometría algebraica y de las curvas elípticas. En el tercer capítulo se estudian las curvas elípticas desde el punto de vista del análisis complejo y la teoría de formas modulares; también se da una introducción a la teoría de superficies elípticas como herramienta para estudiar las curvas elípticas. Después, en el capítulo cuatro, se analiza el grupo de Mordell-Weil para curvas elípticas definidas sobre campos perfectos (en particular campos finitos, locales y numéricos). En el capítulo cinco se da una introducción a la teoría de alturas, la cual resulta ser una herramienta de gran utilidad para determinar cuándo un conjunto de puntos de una curva elíptica es independiente, es decir, que podrían ser generadores de la parte libre del grupo; aquí se presenta la demostración del teorema de Mordell-Weil usando el algoritmo de descenso, el cual nos permite también estudiar la parte de torsión del grupo. El capítulo seis muestra herramientas para estudiar el grupo de Mordell-Weil a partir de una ecuación de Weierstrass que define la curva de donde se está tomando el grupo. Por último, en el capítulo siete se describe como Mestre genera familias de curvas elípticas de rango al menos once y también se presentan los resultados obtenidos posteriormente y que se basan en la construcción de Mestre.

La siguiente tabla resume el avance en la búsqueda de curvas elípticas, donde r es el rango de el grupo de puntos racionales de dicha curva.

1992	J. -P. Mestre	$r \geq 15$	[Mes92]
1992	K. Nagao	$r \geq 17$	[Nag92]
1992	S. Fermigier	$r \geq 19$	[Fer92]
1993	K. Nagao	$r \geq 20$	[Nag93]
1994	K. Nagao, T. Couya	$r \geq 21$	[Nag94]

Existen resultados que aún no se han publicado, sin embargo pueden encontrarse en páginas electrónicas.

1996	S. Fermigier	$r \geqslant 22$
1998	R. Martin, W. McMillen	$r \geqslant 23$

Capítulo 1

Contexto Geométrico

Antes de empezar a trabajar con las curvas elípticas es necesario repasar algunas definiciones y resultados de la geometría algebraica en general, así como también definir la notación en el contexto en el que estaremos trabajando. Existen diferencias entre algunas de las definiciones que aquí se usan y las que se pueden encontrar en varios libros de geometría. La notación que se usará es la misma que maneja Silverman en sus libros [Sil86] y [Sil96].

En la primera sección de este capítulo se revisa la teoría de valuación discreta sobre anillos. Las demás secciones tratan aspectos de la geometría algebraica y las demostraciones de los resultados expuestos se pueden encontrar en [Sil86].

1.1 Valuación Discreta

Para trabajar con anillos de valuación discreta es conveniente dar un breve repaso de la teoría de campos que ésta involucra.

1.1.1 Extensiones de Campos

Esta sección presenta las definiciones básicas de los tipos de extensiones de campos que se ocuparán más adelante. Una buena referencia donde se puede encontrar más acerca de esto es [Mor96].

Sea $K : F$ una extensión algebraica de campos, $f \in F[x]$ un polinomio mónico irreducible y S un subconjunto de polinomios no constantes de $F[x]$ Diremos entonces que:

1. f se *descompone* en K si todas sus raíces están en K.
2. Fijémonos en el conjunto de raíces en K de los polinomios dentro de S,

$$X_S = \{\alpha \in K | f(\alpha) = 0 \text{ para algún } f \in S\}.$$

Entonces K es un *campo de descomposición* de S sobre F si K contiene todos los elementos de X_S, es decir, $K = F(X_S)$ y además cada polinomio $f \in S$ se descompone en K.

3. K es *normal* sobre F si K es un campo de descomposición de algún subconjunto de polinomios no constantes $S \subseteq F[x]$.

4. f es *separable* sobre F si no tiene raíces repetidas en algún campo de descomposición.

5. Un elemento $\alpha \in K$ es *separable* en F si su polinomio mínimo es separable sobre F.

6. K es *separable* sobre F si todo elemento $\alpha \in K$ es separable sobre F.

7. F es un *campo perfecto* si toda extensión algebraica de F es separable.

El siguiente resultado es de gran utilidad en el estudio de curvas definidas sobre campos finitos y su demostración puede ser encontrada en cualquier libro de teoría de campos (ver [Mor96] o [Lan86]).

1.1. Teorema. *Si la característica de un campo F ($char(F)$) es cero, entonces F es perfecto. Si $char(F) = p \neq 0$, entonces F es perfecto si y sólo si $F^p = F$.*

Sea $K : F$ una extensión algebraica. Un elemento $\alpha \in K$ es *puramente inseparable* si su polinomio mínimo tiene una sola raíz en cualquier extensión. K es *puramente inseparable* sobre F si todo elemento de K es puramente inseparable en F.

Sea $K : F$ una extensión algebraica. Los conjuntos que a continuación se definen resultan ser campos, por lo que podemos hablar del grado de su extensión.

1. La *cerradura separable* de F en K es el conjunto

$$S = \{a \in K | a \text{ es separable sobre } F\}.$$

El *grado separable de esta extensión* es $[F : S]$.

2. La *cerradura puramente inseparable* de F en K es el conjunto

$$I = \{a \in K | a \text{ es puramente inseparable sobre } F\}.$$

Definimos el *grado inseparable de la extensión* como $[F : I]$.

Denotarémos por $\overline{K}$ a la cerradura algebraica del campo K.

1.1.2 Anillos de Valuación Discreta

Cuando nos refiramos en general a un *anillo* estaremos pensando en un anillo conmutativo con identidad. Se revisará a continuación un poco de teoría de anillos locales. Las demostraciones de los resultados que se presentan pueden ser encontradas en [Ser76], [Eis96] o [Lan86].

Un dominio entero A es un *anillo de valuación discreta* si es un anillo noetheriano de ideales principales con un único ideal primo m_A. Como este ideal es

maximal, se tiene que A/m_A es un campo. Los elementos invertibles de un anillo A se les llama comúnmente unidades. Estas unidades forman un grupo multiplicativo. Si A es un anillo de valuación discreta, entonces definimos su *campo de residuos* como el cociente A/m_A.

En un anillo de valuación discreta A, su ideal maximal m_A es generado por un sólo elemento. Este elemento se conoce como *elemento primo, parámetro uniformizador* o bien solo como *uniformizador* de A. Si π es un uniformizador de A, entonces todos los demás ideales de A son de la forma $\pi^n A$. De esto se tiene que si $x \in A$ es distinto de cero, entonces podemos escribir $x = u\pi^n$, donde u es una unidad en A y $n \in \mathbb{Z}$. Usando lo anterior podemos definir la *valuación de* x como

$$v(x) = \begin{cases} n & \text{si } x = u\pi^n \neq 0 \\ \infty & \text{si } x = 0 \end{cases}$$

1.2. Nota. Esta valuación no depende de la elección del uniformizador π.

Si K es el campo de cocientes de un anillo de valuación discreta A, es decir,

$$K = \{a/b | a, b \in A \text{ y } b \neq 0\},$$

entonces podemos extender la valuación a este campo con $v(a/b) = v(a) - v(b)$. Tenemos entonces una función $v : K^* \to \mathbb{Z}$ que :

1. es un homomorfismo del grupo multiplicativo K^* en el grupo aditivo $\mathbb{Z}$.
2. $v(x + y) \geq \min(v(x), v(y))$.

Una función como la anterior definida sobre un campo K se llama una *valuación discreta sobre* K.

Si partimos de un campo K con una valuación discreta, podemos reconstruir su anillo de valuación discreta

$$A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}.$$

Sea v una valuación discreta sobre un campo K, entonces definimos el conjunto

$$R_K = \{x \in K \mid v(x) > 0\}$$

como el *anillo de enteros* de K respecto a v.

Dado un campo K con una valuación discreta v y $a \in \mathbb{R}$ tal que $0 < a < 1$, denotamos el *valor absoluto* como

$$\|x\|_v = \begin{cases} a^{v(x)} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

Es fácil verificar las siguientes propiedades.

$$\begin{aligned} \|x\|_v &= 0 \Leftrightarrow x = 0, \\ \|xy\|_v &= \|x\|_v \cdot \|y\|_v, \\ \|x + y\|_v &\leq \|x\|_v + \|y\|_v. \end{aligned}$$

Cualquier función $\| \| : K \to \mathbb{R}$ que satisfaga las propiedades anteriores se llamará también valor absoluto. Se dice que un valor absoluto es *no arquimediano* si además de satisfacer la última de las condiciones anteriores satisface

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

Estos valores absolutos se les suele llamar ultramétricas. Reciprocamente, toda ultramétrica es de la forma $||x|| = a^{v(x)}$ para alguna valuación real $v : K \to \mathbb{R}$.

1.3. Ejemplo. Sea $x \in \mathbb{Q}$ de la forma $x = p^r m/n$ con p, m, n primos relativos y p primo.

1. Si definimos $v(x) = r$ y $a = \frac{1}{p}$, entonces obtenemos el *valor absoluto p-ádico* $|| \, ||_p$ de la forma $||x||_p = ||p^r m/n||_p = \frac{1}{p^r}$.

2. El *valor absoluto arquimediano* $|| \, ||_\infty$ igual a

$$||x||_\infty = \max\{x, -x\}$$

Completación de Campos con Valuación Discreta

Dada una métrica como la anterior es posible dotar a K de la topología definida por los abiertos básicos de la forma

$$B_\varepsilon = \{x \in K \mid ||x|| \leq \varepsilon\}.$$

Sea $\{a_n\}$ una sucesión de Cauchy de elementos de un campo K, es decir, que para todo $\varepsilon > 0$, existe $N \in \mathbb{N}$ tal que si $m, n > N$, entonces $||a_m - a_n|| \leq \varepsilon$. Nos podemos fijar en el conjunto de sucesiones de Cauchy bajo la relación de equivalencia dada por: $\{a_n\} \sim \{b_n\}$ si $\{a_n - b_n\}$ converge a cero. Llamamos a este conjunto la completación de K respecto a $\| \|$ y lo denotamos por $\widehat{K}$. Esta completación resulta también ser un campo.

Sea ahora K una extensión de $\mathbb{Q}$. Diremos que dos valores absolutos son equivalentes si al completar respecto a éstos obtenemos campos isomorfos (o equivalentemente que definan la misma topología). Esta relación entre valores absolutos resulta ser de equivalencia, por lo que cuando nos refiramos a un valor absoluto realmente estaremos pensando en un representante de cada clase de equivalencia. Denotamos por $M_\mathbb{Q}$ al conjunto de las clases de equivalencia de valores absolutos para $\mathbb{Q}$ y por M_K al conjunto de clases de equivalencia de valores absolutos definidos en K tales que al restringirse a $\mathbb{Q}$ son elementos de $M_\mathbb{Q}$.

1.4. Ejemplo. Si usamos el valor absoluto arquimediano en $\mathbb{Q}$, entonces al completar obtenemos $\mathbb{R}$.

1.5. Ejemplo. Si usamos el valor absoluto p-ádico en $\mathbb{Q}$, entonces la completación será el campo de los números p-ádicos, denotado por $\mathbb{Q}_p$.

1.2 Variedades Algebraicas

Cuando se trabaja en algún espacio afín o proyectivo es importante especificar el campo en el que se está definiendo éste. También es importante saber cómo son algunas variedades en diferentes extensiones algebraicas del campo base. Por este motivo siempre que se esté hablando de un espacio se pensará a éste como el conjunto de puntos dentro del espacio definido por la cerradura algebraica del campo en el que estemos trabajando. De esta forma se tiene que el *espacio afín* de dimensión n sobre un campo K es el conjunto de n-adas de elementos de $\overline{K}$, es decir,

$$\mathbb{A}^n = \{(x_1, ..., x_n) \mid x_i \in \overline{K}\}.$$

El conjunto de puntos con coordenadas en algún subcampo F de $\overline{K}$ es el subconjunto de puntos *F-racionales* de $\mathbb{A}^n$ y lo denotamos como

$$\mathbf{A}^n(F) = \{(x_1 \quad ., x_n) \mid x_i \in F\}.$$

De la misma forma podemos definir también el *espacio proyectivo* de dimensión n sobre el campo K como el conjunto de subespacios de dimensión uno de $\mathbb{A}^{n+1}$, dicho de otro modo.

$$\mathbb{P}^n = \{(x_0, ..., x_n) \neq \bar{0} \mid x_i \in \overline{K}\}/\sim.$$

en el cual $(a_0, ..., a_n) \sim (b_0, ..., b_n)$ si existe $\gamma \in \overline{K}^*$ tal que $a_i = \gamma b_i$. Como es usual, se denotará con $[a_0, \ldots a_n]$ a la clase de equivalencia de $(a_0, \ldots, a_n)$. Podemos entonces hablar también de los puntos F-racionales de $\mathbb{P}^n$ donde F es un subcampo de $\overline{K}$, como las clases de equivalencia bajo la relación anterior pero en $\mathbb{A}(K)^{n+1}$,

$$\mathbb{P}^n(F) = \{(x_0 \quad ., x_n) \neq \bar{0} \mid x_i \in F\} \sim$$

1.2.1 Conjuntos Algebraicos y Variedades

Denotamos por $K[X]$ (en lugar de $K[x_1, ..., x_n]$ o de $K[x_0, \ldots, x_n]$) al conjunto de polinomios en n ó $n+1$ variables, según estemos trabajando en el espacio afín o proyectivo de dimensión n, respectivamente. Si no se especifica la dimensión, entonces estaremos pensando en que ésta puede ser arbitraria.

Un *conjunto algebraico* es un subconjunto de puntos de algún espacio, afín o proyectivo, cuyas coordenadas anulan a todo polinomio dentro de un subconjunto de $\overline{K}[X]$. Si el espacio es proyectivo, entonces estos polinomios deben de ser homogéneos.

El conjunto de todos los polinomios (homogeneos en el caso de espacios proyectivos) que se anulan en un conjunto algebraico genera un ideal. Por el teorema de las bases de Hilbert el ideal anterior es finitamente generado, más aún, si el ideal es generado por polinomios homogéneos, entonces éste es

finitamente generado por polinomios homogéneos (ver [Eis96]). Si V es un conjunto algebraico en un espacio afín, denotaremos entonces este ideal por

$$I(V) =< f \in K[X] \mid P \in V \Rightarrow f(P) = 0 > .$$

Es importante indicar cuándo un conjunto algebraico está definido por polinomios con coeficientes en cierto subcampo F de $\overline{K}$, así como también los puntos F-racionales de dicho conjunto. Por lo que se denotará por V/F a un conjunto algebraico V que se pueda definir con polinomios en $F[X]$. Para los puntos F-racionales de este conjunto se usará

$$V(F) = \{P \in V \mid P \text{ es punto } F - \text{racional}\}.$$

También es conveniente especificar el ideal generado por los polinomios dentro de $F[X]$ que se anulan en $V(F)$, el cual lo denotamos por

$$I(V/F) = \{f \in F[X] \mid P \in V/F \Rightarrow f(P) = 0\}.$$

Una *variedad algebraica* (o *variedad* simplemente) V es un conjunto algebraico en el que el ideal generado por los polinomios que se anulan en este conjunto, $I(V)$, es primo. Hay que recordar que este último ideal está en $\overline{K}[X]$.

1.6. Ejemplo. El polinomio $x^2 + 1$ genera un ideal primo dentro de $\mathbb{R}[x]$, pero el ideal que genera dentro de $\mathbb{C}[x]$ no lo es, por lo que el conjunto algebraico definido por este polinomio no es una variedad.

Cuando se haga referencia a una variedad algebraica sin especificar si es afín o proyectiva, se entenderá que puede ser cualquiera de estas dos.

1.2.2 Dimensión

Caso Afín

En una variedad algebraica afín V/K se define el *anillo de coordenadas* de dicha variedad como el cociente

$$K[V] = \frac{K[X]}{I(V/K)}.$$

Como $I(V/K)$ es un ideal primo, entonces este anillo de coordenadas resulta ser un dominio entero. Por tal motivo es posible completar el anillo a un campo agregando los cocientes de los elementos del anillo. Este campo se conoce como el *campo de fracciones* de la variedad V/K, el cual denotaremos por

$$K(V/K) = \{a/b \mid a, b \in K[V],\ b \neq 0\}.$$

Las variables x_i son elementos trascendentes de $K[X]$, pero al hacer el cociente con algún ideal primo y después tomar su campo de fracciones, estas variables pueden dejar de ser elementos trascendentes en $K(V/K)$. Esto último nos conduce a definir la *dimensión* de una variedad como el grado de trascendencia de la extensión del campo $\overline{K}$ en el campo $\overline{K}(V)$,

$$\dim V = \text{grado de trascendencia de } \overline{K}(V) : \overline{K}.$$

Caso Proyectivo

Cada punto $P = [a_0, ..., a_n]$ de un espacio proyectivo $\mathbb{P}^n$ puede ser pensado como un punto de un espacio afín $\mathbb{A}^n$ contenido en este espacio proyectivo. Para ver esto basta tomar alguna $a_i \neq 0$ de un representante $(a_0, ..., a_n)$ de P y fijarse en $(a_0/a_i, ...a_{i-1}/a_i, 1, a_{i+1}/a_i, a_n/a_i)$. El conjunto de puntos de la forma $(x_0, ..., x_{i-1}, 1, x_{i+1}, ..., x_n)$ es un espacio afín de dimensión n.

La función $\rho_i : \mathbb{A}^n \to \mathbb{P}^n$ definida por

$$\rho_i(a_1, ..., a_n) = [a_1, ..., a_{i-1}, 1, a_{i+1}, ..., a_n]$$

es una inyección en la que la imagen inversa de una variedad proyectiva $V(K)$ es una variedad afín $U(K)$.

Sea P un punto de una variedad proyectiva V Como se mencionó anteriormente, existe una variedad afín U que contiene a P. Definimos la dimensión y el campo de cocientes de V como la dimensión y el campo de cocientes de U, es decir,

$$K(V) = K(U) \qquad \text{y} \qquad \dim V = \dim U.$$

1.7. Nota. Es importante indicar que esta definición no depende de la elección del punto P ni del abierto U.

1.8. Nota. En muchas ocasiones es conveniente ver al campo de cocientes de una variedad proyectiva V como el campo

$K(V) = \{f/g | f \text{ y } g \text{ son polinomios homogéneos del mismo grado dentro de } K[V]\}$

1.2.3 Aplicaciones entre Variedades Algebraicas

Si V_1 y V_2 son dos variedades proyectivas, diremos que una *aplicación racional* de V_1 en V_2 es una aplicación de la forma

$$\begin{aligned} \phi &: V_1 \to V_2 \\ \phi(P) &= [f_0(P), ..., f_n(P)], \end{aligned}$$

donde $f_0, ..., f_n \in \overline{K}(V_1)$ satisfacen que para todo punto P, en donde estas funciones estén bien definidas, se tiene $\phi(P) \in V_2$. Una aplicación racional no es necesariamente una función, ya que puede suceder que el denominador de una función racional f_i se anule en algún punto dentro de la variedad V_1. En ocasiones se puede escoger un polinomio $g \in \overline{K}[V_1]$ tal que

$$\phi(P) = [g(P)f_0(P), ..., g(P)f_n(P)]$$

esté bien definido en P (no se ha cambiado la aplicación ϕ ya que estamos trabajando en el espacio proyectivo y los puntos son clases de equivalencia). Cuando esto suceda diremos que ϕ es una *aplicación regular* en el punto P y si ϕ es regular en todo punto de V_1, entonces diremos que es un *morfismo* (o *aplicación regular*) de V_1 en V_2.

1.9. Ejemplo. Sea V_1 la variedad definida por el ideal $< x >$ dentro de $\mathbb{P}^2$ y $V_2 = \mathbb{P}^2$.

1. Sea $\phi : V_1 \to V_2$ dada por $[x, y, z] \mapsto [\frac{x}{z}, \frac{y}{z}, \frac{z}{y}]$. ϕ es una aplicación regular.
2. Sea $\phi : V_1 \to V_2$ dada por $[x, y, z] \mapsto [\frac{x}{z}, 1, 1]$. En este caso ϕ no es una aplicación regular.

Sea $\phi : V_1 \longrightarrow V_2$ un morfismo de variedades definidas sobre el campo K. Éste induce un morfismo de campos

$$\begin{aligned} \phi^* : \quad K(V_2) &\longrightarrow K(V_1) \\ f &\longmapsto f \circ \phi \end{aligned}$$

Definición. En la notación anterior definimos el grado de ϕ como:

$$grad(\phi) = \begin{cases} 0 & \text{si } \phi \text{ es constante} \\ [K(V_1) : \phi^* K(V_2)] & \text{si } \phi \text{ no es constante} \end{cases}$$

Diremos que ϕ es *separable* si la extensión de campos $K(V_1)/\phi^* K(V_2)$ es separable.

1.2.4 Puntos Singulares

Sea V una variedad algebraica definida por los polinomios $f_1, f_2, ..., f_m \in \overline{K}[X]$ y P un punto de esta variedad, entonces diremos que V ***no es singular*** en P si la matriz cuyas entradas son las derivadas parciales de los polinomios anteriores,

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

tiene rango igual a $n - \dim V$, y diremos que es ***singular*** si su rango es menor. Diremos en general que una variedad V ***no es singular,*** *o* que es ***suave*** si ésta no es singular para todo $P \in V$.

1.10. Ejemplo. Considerando las variedades

$$\begin{aligned} V_1 &: Y^2 = X^3 + X \\ V_2 &: Y^2 = X^3 + X^2, \end{aligned}$$

es fácil comprobar que la primera no es singular mientras que la segunda tiene una singularidad en el origen y que ambas tienen dimensión igual a uno.

1.2.5 Localización

Existe una forma algebraica de caracterizar las singularidades de las variedades. Si P es un punto de la variedad V, entonces denotemos al ideal que contiene a todos los polinomios que se anulan en punto por

$$M_P = \{f \in \overline{K}[V] | f(P) = 0\}.$$

Este ideal es maximal y el cociente de ideales M_P/M_P^2 es un espacio vectorial sobre $\overline{K}$.

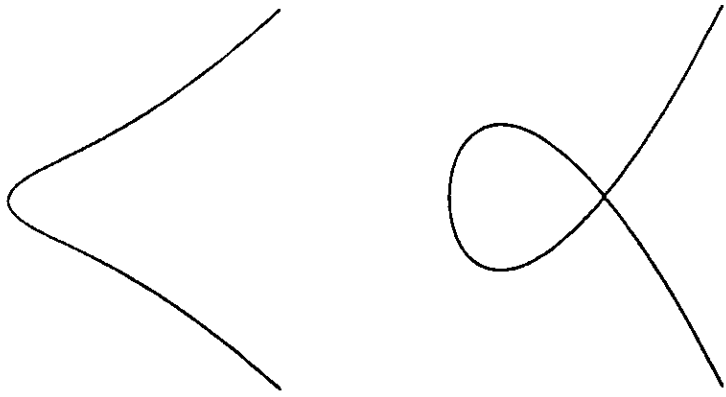

Figura 1.1: Curvas V_1 y V_2

1.11. Proposición. *Sea V una variedad. Un punto $P \in V$ no es singular si y sólo si*

$$\dim_{\overline{K}} M_P/M_P^2 = \dim V.$$

En el ejemplo 1.10 el punto $P = (0,0)$ pertenece a ambas variedades y en los dos casos el ideal M_P es el generado por los polinomios X y Y; y M_P^2 está generado por X^2, XY y Y^2. Pero en el anillo de coordenadas de la primera, $\overline{K}[V_1]$, se tiene

$$X = Y^2 - X^3 \equiv 0 \ mod M_P^2$$

por lo que M_P/M_P^2 se puede generar con la variable Y como espacio vectorial sobre $\overline{K}$, es decir, $\dim M_P/M_P^2 = 1$. Y en la variedad V_2 las variables X y Y no tienen una relación lineal que las involucre con los demás elementos de M_P^2, por lo que se necesitan las dos variables para generar M_P/M_P^2 como espacio vectorial sobre $\overline{K}$, por lo tanto $\dim M_P/M_P^2 = 2$. Así, tenemos que V_1 no es una variedad singular en el origen mientras que V_2 si lo es.

Los cocientes de polinomios dentro de $\overline{K}(V)$ no están definidos como funciones en los puntos donde el denominador se anula. Para centrar nuestra atención en las funciones racionales que estén bien definidas en algún punto P dentro de una variedad V, definimos el *anillo local* en P como el conjunto de elementos del campo de cocientes de V que están bien definidos para P, el cual denotamos por

$$\overline{K}[V]_P = \{f/g \in \overline{K}(V) \mid g(P) \neq 0\}.$$

1.3 Curvas Algebraicas

A continuación nos enfocaremos a la teoría de curvas algebraicas así como también se enunciarán algunas características de éstas. En esta sección se estará tra-

bajando con campos perfectos. Las demostraciones de los resultados que aquí se presentan pueden ser encontradas en [Har77] y [Sil86].

Por una *curva algebraica* entenderemos una variedad algebraica de dimensión uno. Para abreviar nos referiremos a las curvas algebraicas como curvas simplemente.

1.3.1 Valuación en Curvas

Los anillos locales son de gran importancia y a través de estos podemos dar lo que se conoce como orden en el campo de funciones de una curva.

1.12. Proposición. *Si C es una curva y P un punto no singular de ésta, entonces la localización de su anillo de coordenadas en P, $\overline{K}[C]_P$, es un anillo de valuación discreta.*

Sea C una curva, P un punto no singular de C y $f \in \overline{K}[C]_P$. Definimos el *orden* de f en el punto P como la valuación

$$\begin{aligned} ord_p &: \overline{K}[C] \to \{0,1,2,3,...\} \cup \{\infty\} \\ ord_P(f) &= \max\{d \mid f \in M_P^d\}, \end{aligned}$$

donde M_P es el ideal maximal de $\overline{K}[C]_P$. Podemos extenderla a todo $\overline{K}(C)$ usando $ord_P(f/g) = ord_P(f) - ord_P(g)$.

Si $ord_P(f) > 0$ diremos que f *tiene un cero* en P, si $ord_P(f) < 0$, diremos entonces que f *tiene un polo* en P.

1.13. Proposición. *Sea C una curva suave y $f \in \overline{K}(C)$. Entonces existe un número finito de puntos P para los cuales $f(P)$ tiene un cero o un polo. Y si además f no tiene polos, entonces $f \in \overline{K}$.*

1.14. Ejemplo. Consideremos las curvas descritas en el ejemplo 1.10. Donde V_1 es suave en el origen mientras que V_2 no lo es. Si P es el origen, se tiene entonces que en V_1

$$ord_P(Y) = 1 \qquad ord_P(X) = 2$$

La siguiente proposición será útil cuando estemos trabajando con curvas definidas sobre campos de característica mayor que cero.

1.15. Proposición. *Sea C/K una curva algebraica donde $charK > 0$ y sea $t \in K(C)$ un uniformizador en algún punto $P \in C$ no singular. Entonces $K(C)$ es una extensión separable finita de $K(t)$.*

1.3.2 Aplicaciones entre Curvas

En esta sección se presenta una serie de resultados que tienen que ver con aplicaciones entre variedades algebraicas enfocando nuestra atención al caso de curvas.

Sea $\phi = [f_0, ..., f_n] : V_1 \to V_2$ una aplicación racional, es decir, un morfismo. Si V_1 y V_2 están definidas sobre el campo K, entonces el grupo de Galois $G_{\overline{K}/K}$ actúa en ϕ de forma obvia:

$$\phi^\sigma(P) = [f_0(P)^\sigma, ..., f_n(P)^\sigma].$$

Diremos que dos variedades V_1 y V_2 son *isomorfas (o birracionalmente equivalentes)* si existen morfismos $\phi : V_1 \to V_2$ y $\psi : V_2 \to V_1$ tales que $\psi \circ \phi$ y $\phi \circ \psi$ son la identidad en V_1 y V_2 respectivamente. También diremos que son *isomorfas sobre el campo* K si tanto las variedades V_1 y V_2 como estos morfismos φ y ψ están definidos sobre K.

1.16. Teorema. *Sea $\phi : C_1 \to C_2$ un morfismo entre curvas proyectivas. Entonces ϕ es constante o suprayectiva.*

Supogamos ahora que C_1/K y C_2/K son curvas y que $\phi : C_1 \to C_2$ es una función racional no constante entre estas curvas definida sobre K. Se puede ver que la composición con ϕ induce la siguiente inyección, que fija a K :

$$\begin{aligned} \phi^* &: K(C_2) \to K(C_1), \\ \phi^*(f) &= f \circ \phi. \end{aligned}$$

1.17. Teorema. *Sean C_1/K y C_2/K curvas.*

1. *Si $\phi : C_1 \to C_2$ es un morfismo no constante definido sobre K, entonces $K(C_1)$ es una extensión finita de $\phi^*(K(C_2))$.*
2. *Si $i : K(C_2) \to K(C_1)$ es una inyección que fija K, entonces existe una única función no constante $\phi : C_1 \to C_2$ definida sobre K tal que $\phi^* = i$.*
3. *Sea $\mathbb{K}$ un subcampo de $K(C_1)$ de índice finito que contenga a K. Entonces existe una curva suave C'/K, única salvo $K-$isomorfismo, y una función no constante $\phi : C \to C'$ definida sobre K, tal que $\phi^*(K(C')) = \mathbb{K}$.*

1.4 Divisores

En esta sección revisaremos los conceptos concernientes a divisores en curvas. Las demostraciones de los resultados que se presentan pueden ser encontradas en [Sil86] y en [Har77].

Sea C una curva. El *grupo de divisores* de C, denotado por $Div(C)$, es el grupo libre aditivo generado por los puntos de C. De esta forma cada elemento D de $Div(C)$ se escribe

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

donde $n_P \in \mathbb{Z}$, (P) es el divisor correspondiente al punto P y n_P es cero para todos excepto un número finito de puntos $P \in C$. El *grado* del divisor D es la suma de los valores de n_P.

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

El conjunto de divisores de grado cero forma un subgrupo de $Div(C)$ que se denotará $Div^0(C)$.

Si la curva C está definida sobre K, entonces el grupo de Galois $G_{\overline{K}/K}$ actúa en $Div(C)$ de forma obvia.

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

Decimos que D está definido sobre K si $D^\sigma = D$ para todo $\sigma \in G_{\overline{K}/K}$.

1.18. Ejemplo. Si tomamos los puntos $P_1 = [1, \sqrt{2}]$ y $P_2 = [1, -\sqrt{2}]$ dentro de $\mathbb{P}^1(\bar{\mathbb{Q}})$, entonces el divisor $D = (P_1) + (P_2)$ está definido sobre $\mathbb{Q}$, ya que cualquier $\sigma \in G_{\bar{\mathbf{Q}}/\mathbf{Q}}$ deja fijo a $\sqrt{2}$ o bien lo manda a $-\sqrt{2}$.

Si C es una curva suave y $f \in \overline{K}(C)^*$, entonces podemos asociar a f el divisor

$$Div(f) = \sum_{P \in C} ord_P(f)(P)$$

(la proposición 1.13 justifica que es efectivamente un divisor)

Un divisor $D \in Div(C)$ es *principal* si es el divisor de alguna función $f \in \overline{K}(C)^*$. Dos divisores son *linealmente equivalentes* si su diferencia está en $Div^0(C)$. Para el caso de curvas podemos definir el *grupo de Picard* (o de clase de divisores) $Pic(C)$ como el cociente de $Div(C)$ entre el grupo de sus divisores principales. La siguiente proposición es válida sólo para el caso de curvas.

1.19. Proposición. *Si C es una curva suave y $f \in \overline{K}(C)^*$, entonces:*

1. $Div(f) = 0$ *si y sólo si* $f \in \overline{K}^*$.
2. $grad(Div(f)) = 0$.

1.20. Ejemplo. Si nos fijamos de nuevo en la curva C definida por la ecuación

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

y en la función $x \in K(C)$ (ó $\frac{x}{z}$ si se piensa como cociente de polinomios homogéneos del mismo grado), podemos calcular el divisor de esta función (ver ejemplo 1.14). Ésta tiene como ceros a $P_1 = [0, 0, 1]$ y $P_2 = [0, 1, 0]$ (el punto al infinito), con ordenes

$$ord_{P_1}(x) = 2, \qquad ord_{P_2}(x) = 1.$$

Y tiene un único polo en P_2 de orden 3, es decir, $ord_{P_2}(z) = 3$. Así podemos calcular su divisor

$$Div(x) = 2(P_1) - 2(P_2),$$

donde la función x representa la recta que se ve en la figura 1.2.

1.4.1 Diferenciales

Una de las condiciones que deberá tener una curva para ser elíptica es no tener singularidades. Para esto es útil el uso de las diferenciales. Sea C una curva. El espacio de *formas diferenciales meromorfas* sobre C, denotado por Ω_C, es el espacio vectorial sobre $\overline{K}(C)$ generado por los símbolos de la forma dx para cada $x \in \overline{K}(C)$ sujetos a las siguientes relaciones:

1. $d(x+y) = dx + dy$ para $x, y \in \overline{K}(C)$.
2. $d(xy) = xdy + ydx$ para $x, y \in \overline{K}(C)$.
3. $da = 0$ para $a \in \overline{K}$.

1.21. Proposición. *Sean P un punto de una curva C y $t \in \overline{K}(C)$ un uniformizador en P.*

1. *Para toda forma diferencial meromorfa $\omega \in \Omega_C$, existe una función g dentro de $\overline{K}(C)$ tal que*

$$\omega = gdt.$$

   Denotaremos a g por ω/dt.

2. *El valor de $ord_P(g)$ depende sólo de P y de ω, no depende de la elección del uniformizador t.*

De acuerdo a está última proposición, definimos el orden de ω como

$$ord_P(\omega) = ord_P(g).$$

Así, a cada forma diferencial meromorfa $\omega \in \Omega_C$ se le puede asociar un divisor

$$Div(\omega) = \sum_{P \in C} ord(\omega)_P(P) \in Div(C).$$

Una forma diferencial meromorfa $\omega \in \Omega_C$ es una *forma regular* (u *holomorfa*) si

$$ord_P(\omega) \geqslant 0$$

y se dice que *no se desvanece* si

$$ord_P(\omega) \leqslant 0.$$

Un *divisor canónico* es la imagen de un divisor $Div(\omega)$ dentro de $Pic(C)$ para algún $\omega \in \Omega_C$.

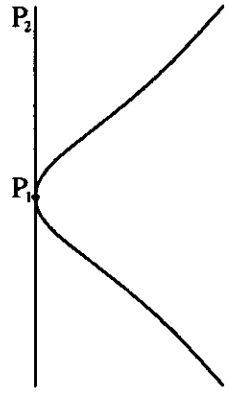

Figura 1.2: Orden de la función x en los puntos P_1 y P_2

Capítulo 2

Curvas Elípticas

Recordemos que por una curva estamos pensado en una variedad algebraica de dimensión uno. Ahora nos interesarán las curvas suaves de género uno, conocidas también como curvas elípticas (para el caso de curvas el género algebraico, aritmético y topológico coinciden). Además siempre estaremos considerando un punto distinguido de esta curva. Así, una curva elíptica será una pareja (E, O) donde E es una curva suave de género uno y O es un punto distinguido de E. También será importante estudiar los morfismos entre curvas elípticas, los cuales deberán ser de la forma

$$\varphi : (E, O) \to (E', O'),$$

donde φ es morfismo de las varidades algebraicas E y E', con la condición extra de que $\varphi(O) = O'$. Las demostraciones de los resultados que se presentan en este capítulo pueden ser encontradas en [Sil86], o bien, ahí se da la referencia correspondiente.

2.1 Género de una Curva Algebraica

En esta sección se enuncia la versión del teorema de Riemann-Roch para curvas suaves definidas sobre cualquier campo, el cual nos permite definir el género de éstas. Si tenemos una curva suave definida sobre el campo de los números complejos, entonces su género algebraico coincide con el género topológico, de este modo las curvas no singulares de género uno son topológicamente los toros.

2.1.1 Teorema de Riemann-Roch

Sea C una curva plana. Diremos que un divisor

$$D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$$

es *positivo* (o efectivo), denotado por

$$D \geqslant 0,$$

si $n_P \geq 0$ para todo $P \in C$. Definiremos un orden parcial, $\leq$, en el grupo de divisores de esta curva de la siguiente forma: Si D' es otro divisor, usaremos

$$D \geqslant D'$$

para indicar que $D - D'$ es positivo.

Ahora, el conjunto

$$\mathfrak{L}(D) = \{f \in \overline{K}(C)^* | \mathrm{Div}(f) \geqslant -D\} \cup \{0\}.$$

es un espacio vectorial de dimensión finita sobre el campo $\overline{K}$. Denotaremos por $l(D)$ a la dimensión de este espacio vectorial.

2.1. Ejemplo. Consideremos la curva C definida por la ecuación $y^2 = x^3 + x$ y el divisor $6P_\infty \in \mathbb{C}(C)$ (ver ejemplo 1.20). En este caso tenemos las funciones 1, x, y ,x^2, y^2, xy y x^3 dentro de $\mathfrak{L}(6P_\infty)$, pero usando la ecuación que define a C, estas funciones son linealmente dependientes, por lo que se puede generar $\mathfrak{L}(6P_\infty)$ usando seis de estas funciones:

$$\mathfrak{L}(6P_\infty) = < 1, x, y, xy, x^2, y^2 > \qquad \text{y} \qquad l(6P_\infty) = 6.$$

2.2. Teorema (Riemann-Roch). *Sea C una curva suave y K_C un divisor canónico sobre C. Existe un entero $g \geqslant 0$, llamado el género algebraico de C, tal que para todo divisor $D \in Div(C)$, se cumple la igualdad*

$$l(D) - l(K_C - D) = grad(D) - g + 1.$$

2.3. Ejemplo. En el ejemplo 2.1 la curva C es una curva de genero uno.

Si C/K es una curva de genero igual a uno y $P \in C$ un punto de C, entonces tenemos $l(nP) = n$. Por lo que existen $x, y \in K(C)$ tales que:

$$\begin{aligned} \mathfrak{L}(P) &= < 1 > \\ \mathfrak{L}(2P) &= < 1, x > \\ \mathfrak{L}(3P) &= < 1, x, y > . \end{aligned}$$

donde $< x_1, x_2, \ldots x_n >$ representa el subespacio vectorial generado por $x_1, \ldots, x_n$. Se puede ver de la misma forma que el conjunto $\{1, x, y, x^2, y^2, xy, x^3\}$ es linealmente dependiente dentro de $\mathfrak{L}(6P)$, por lo que existe una combinación lineal igual a cero.

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0,$$

con $A_1, \ldots, A_7 \in K(C)$. En esta última ecuación es posible ver que $A_6 A_7 \neq 0$, por lo que podemos hacer el cambio de variables

$$(x, y) = (-A_6 A_7 x, A_6 A_7^2 y)$$

y dividir toda la ecuación entre $A_6^3 A_7^4$, lo cual da como resultado una ecuación de Weierstrass. Lo anterior prueba una parte de la siguiente porposición.

2.4. Proposición. *Sea E una curva suave de género uno definida sobre un campo K y O un punto distinguido de ésta. Entonces existen funciones $x, y \in K(E)$ tales que la función*

$$\phi(E) \to \mathbb{P}^2$$
$$\phi = [x, y, 1]$$

es un isomorfismo de E/K en una curva dada por una ecuación de la siguiente forma (Forma de Weierstrass):

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

con $a_1, \ldots, a_6 \in K$; y tal que $\phi(O) = [0, 1, 0]$.

Una curva elíptica se puede definir como una curva C no singular de género igual a uno. El objetivo de este trabajo es estudiar el conjunto de puntos $\mathbb{Q}$–racionales de esta curva, $C(\mathbb{Q})$. Cuando tomamos un punto distinguido $O \in C(\mathbb{Q})$ es posible dar estructura de grupo al conjunto $C(\mathbb{Q})$, lo cual se verá a continuación. Si cambiamos el punto distinguido, entonces el grupo que se forma no es necesariamente el mismo.

Definición. Una curva *elíptica* es una curva E no singular de género igual a uno junto con un punto distinguido O de E.

2.1.2 Puntos Racionales en Cúbicas

Sea C una curva plana definida por un polinomio f de grado tres. Si escogemos un punto O no singular de C, podemos dar estructura de grupo a los puntos no singulares de C. Definimos primero a O como el neutro del grupo. Ahora, dado un punto $P \in C$, definimos su inverso, $-P$, como el tercer punto de intersección de la recta que pasa por P y por O, es decir, P, $-P$ y O son coolineales. Para determinar la suma de dos puntos, $R = P + Q$, definimos $-R$ como el tercer punto de intersección de la recta que pasa por P y Q con C, de modo que los puntos R, $-R$ y O son coolineales. Es relativamente fácil comprobar que esta operación es conmutativa y que cada elemento tiene inverso. Para la asociatividad es necesario usar el teorema de Bezout. Para este fín basta con saber que si una curva de grado tres pasa por ocho de los puntos de intersección de otras dos cúbicas, entonces pasa por el punto restante de intesección de estas últimas dos curvas.

2.5. Nota. Si F es un subcampo de K y $O \in C(F)$, entonces la operación que se definió anteriormente da estructura de grupo a los puntos F-racionales no singulares de C.

2.2 Ecuación de Weierstrass

Trabajaremos con curvas definidas por una ecuaciones de la forma

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

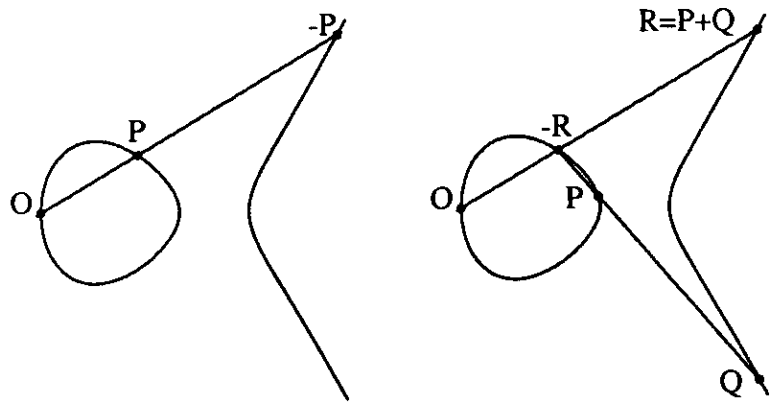

Figura 2.1: Operación del grupo de Mordell-Weil en una curva elíptica

con a_1, a_2, a_3, a_4 y a_6 dentro de K. Este tipo de ecuaciones se les conoce como ecuaciones de Weierstrass.

Si analizamos las curvas definidas de esta forma, se puede ver que éstas cortan a la recta al infinito en un sólo punto $P_\infty = [0, 1, 0]$. En cualquier curva definida con una ecuación de Weierstrass, por ser ésta una ecuación de tercer grado, es posible hablar del grupo de los puntos K-racionales no singulares de dicha curva (tal como se menciona en la sección anterior).

Supongamos en lo que resta del capítulo que E es una curva definida por una ecuación de Weierstrass como se hizo anteriormente. Supondremos también que el campo donde estamos definiendo E es de característica distinta de dos o tres (posteriormente se dará el tratamiento para estos campos). Si sustituimos y por

$$\frac{y - a_1x - a_3}{2},$$

entonces podemos reescribir la ecuación anterior de la forma

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.1}$$

donde

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

También será conveniente definir los siguientes valores:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24 b_4 \\ c_6 &= b_2^3 + 36 b_2 b_4 - 216 b_6 \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6 \\ j &= \frac{c_4^2}{\Delta}. \end{aligned}$$

Estos valores cumplen las siguientes relaciones:

$$\begin{aligned} 4b_8 &= b_2 b_6 - b_4^2 \\ 1738\Delta &= c_4^2 - c_6^2. \end{aligned}$$

Sustituyendo ahora (x, y) por

$$\left(\frac{x - 3b_2}{36}, \frac{y}{216}\right)$$

podemos reescribir de nuevo la ecuación 2.1 de una forma más simple

$$E : y^2 = x^3 - 27 c_4 x - 54 c_6.$$

Así, la curva queda determinada por los valores de c_4 y c_6.

2.2.1 Curvas Hiperelípticas

Por un momento fijemonos en las curvas definidas por ecuaciones de la forma

$$y^2 = f(x),$$

donde $f(x)$ es un polinomio que no tiene un cero doble para $x = 0$. Este tipo de curvas son llamadas *hiperelípticas* y se sabe que si el grado de f es d, entonces estas curvas son no singulares y su género está dado por el único entero g tal que $d - 1 < 2g \leq d$ (ver [Sil92, II]).

2.3 Invariantes en Ecuaciones de Weierstrass

Cuando estamos trabajando con una curva E definida por una ecuación de Weierstrass, los valores Δ, c_4 y c_6 nos permitirán saber si la curva que ésta define tiene singularidades y de que tipo de singularidad son. Diremos que un punto de una curva es un *nodo* si es singular y es un punto donde la curva se autointerseca; y diremos que es una *cúspide* si es singular pero E no se autointerseca en este punto.

2.6. Proposición. *Sea E una curva definida por una ecuación de Weierstrass.*

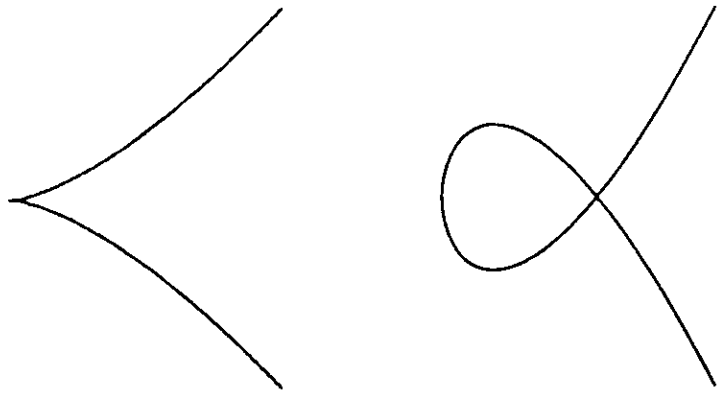

Figura 2.2: Tipos de singularidad en cúbicas (cúspide y nodo)

1. $\Delta \neq 0$ *si, y sólo si* E *es no singular.*
2. $\Delta = 0$ *y* $c_4 \neq 0$ *si, y sólo si* E *tiene un punto nodal.*
3. $\Delta = 0$ *y* $c_4 = 0$ *si, y sólo si* E *tiene un punto cuspidal.*

Además, si E *es singular, entonces sólo tiene un punto singular.*

Ya que se han clasificado las curvas de acuerdo a las ecuaciones de Weierstrass que las definen, pasaremos ahora a ver en qué condiciones podemos decir que dos de estas curvas son isomorfas. En lo que resta del capítulo E y E' serán curvas definidas por una ecuación de Weierstrass.

2.7. Proposición. *Sean* j *y* j' *los* $j-$*invariantes de las curvas* E *y* E'.

1. E *y* E' *son isomorfas (sobre* $\overline{K}$*) si, y sólo si* $j = j'$.
2. *Para todo* $j_0 \in K$ *existe una curva elíptica con* $j-$*invariante igual a* j_0.

Las curvas elípticas se pueden escribir con ecuaciones de Weierstrass, y viceversa, cualquier ecuación de Weierstrass que no tenga puntos singulares determina una curva elíptica.

2.8. Proposición. *Para cualquier curva elíptica* E *existen* $\lambda \in K - \{0,1\}$ *y una curva elíptica* E_λ *definida por* $y^2 = x(x-1)(x-\lambda)$ *tales que:*

1. E *y* E_λ *son isomorfas.*
2. *El* $j-$*invariante de la curva* E *está dado por*

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

3. *La función que a cada* λ *le asigna* $j(E_\lambda)$ *es seis a uno si* $0 \neq j \neq 1728$; *dos a uno si* $j = 0$; *y es tres a uno si* $j = 1728$.

De esta forma es posible parametrizar las curvas elípticas. A esta forma de determinar las curvas se le conoce como La Forma de Legendre. En lo sucesivo y de acuerdo a estos últimos resultados, cuando nos refiramos a una curva elíptica estaremos pensando a ésta como el conjunto de puntos con la estructura de grupo definida en 2.1.2 con el punto al infinito como origen, $O = P_\infty$ (este grupo se conoce como el Grupo de Mordell-Weil). Si E es un curva definida por una ecuación de Weierstrass, denotaremos entonces por E_{ns} a el conjunto de puntos donde la curva no es singular.

2.9. Proposición. *Sea E una curva definida por una ecuación de Weierstrass tal que $\Delta = 0$.*

1. *Si $c_4 \neq 0$, entonces $E_{ns} = K^*$.*
2. *Si $c_4 = 0$, entonces $E_{ns} = K^+$.*

Donde K^* representa al grupo multiplicativo de $K - \{0\}$ y K^+ al grupo aditivo de K.

2.3.1 Isogenias

Cuando estamos pensando en variedades en las que sus puntos tienen una estructura de grupo, como lo son las curvas elípticas, nos interesa trabajar con los morfismos que respeten esta estructura, es decir, que también son homomorfismos de grupo.

Definición. Sean E_1 y E_2 dos curvas elípticas con neutros O_1 y O_2 respectivamente. Una isogenia entre estas dos curvas es un morfismo de variedades $\varphi : E_1 \longrightarrow E_2$ que satisface $\varphi(O_1) = O_2$. Si además $\varphi(E_1) \neq \{O_2\}$, diremos que E_1 y E_2 son isógeneas

Una isogenia $\varphi : E_1 \longrightarrow E_2$ determina una función entre los campos de funciones de las curvas, que denotaremos por $\varphi^* : K(E_2) \longrightarrow K(E_1)$. Dadas dos isogenias φ y ψ, podemos definir la función $\varphi + \psi : E_1 \longrightarrow E_2$ de la forma $(\varphi+\psi)(P) = \varphi(P)+\psi(P)$, la cual resulta ser otra isogenia, por lo cual podemos dar estructura de grupo al conjunto de isogenias de E_1 en E_2. En este contexto nos referiremos a $Hom(E_1, E_2)$ como el grupo anterior y del mismo modo y de manera usual podemos definir $End(E)$ como el grupo de endomorfismos y $Aut(E)$ como el grupo de automorfismos. Si además agregamos la composición de isogenias como multiplicación, podemos dotar a $End(E)$ una estructura de anillo.

2.10. Proposición. *Sean E_1 y E_2 curvas elípticas y m un entero no negativo.*

1. *El morfismo $[m] : E_1 \longrightarrow E_1$, dado por $[m](P) = P + ... + P$ (m veces) es una isogenia.*
2. *$Hom(E_1, E_2)$ es un $\mathbf{Z}-$módulo libre de torsión.*

2.11. Ejemplo. Sea E una curva elíptica y O su punto distinguido. La función $[0] : E \to E$ tal que $[0](P) = P$ para todo $P \in E$ es una isogenia.

Hay que recordar que las isogenias tienen que respetar la estructura de grupo de las curvas donde se define, como lo indica el siguiente teorema.

2.12. Teorema. *Toda isogenea es un homomorfismo de grupos de las curvas en donde se define.*

2.13. Corolario. *Si* $\varphi : E_1 \longrightarrow E_2$ *es una isogenia distinta de* $[0] : E_1 \longrightarrow E_2$, *entonces* $\ker(\varphi)$ *es un subgrupo finito de* E_1.

Una observación interesante es que toda curva elíptica puede ser vista como un $\mathbb{Z}-$ módulo bajo la operación $mP = [m](P)$, para $m \in \mathbb{Z}$ y $P \in E$.

Sea $m \in \mathbb{Z}$. El $m-$subgrupo de torsión de una curva elíptica E es el subgrupo

$$E[m] = \{P \in E | [m](P) = O\}.$$

El subgrupo de torsión E_{Tor} de E es la unión de todos los $m-$subgrupos de torsión de E.

Isogenias Duales

Si bien las funciones $[m]$ son isogenias, no toda isogenia es de esta forma, sin embargo es posible relacionar cada isogenia con una de éstas.

2.14. Teorema. *Sea* $\varphi : E_1 \longrightarrow E_2$ *una isogenia. Existe una isogenia*

$$\overline{\varphi} : E_2 \longrightarrow E_1$$

y un entero m *tal que*

$$\overline{\varphi} \circ \varphi = [m].$$

Definimos esta isogenia como la *isogenia dual* de φ.

2.15. Teorema. *Sean* $\varphi, \psi : E_1 \longrightarrow E_2$ *y* $\lambda : E_1 \longrightarrow E_2$ *isogenias entre curvas elípticas.*

1. *Si* $m = \deg(\varphi)$, *entonces*

$$\overline{\varphi} \circ \varphi = [m] \in End(E_1);$$
$$\varphi \circ \overline{\varphi} = [m] \in End(E_2).$$

2. $\overline{\lambda \circ \varphi} = \overline{\varphi} \circ \overline{\lambda}$.
3. $\overline{\varphi + \psi} = \overline{\varphi} + \overline{\psi}$.
4. $\overline{[m]} = [m]$ *y* $\deg([m]) = m^2$.
5. $\deg(\overline{\varphi}) = \deg(\varphi)$.
6. $\overline{\overline{\varphi}} = \varphi$.

Con estas propiedades se puede observar que la función que determina el grado de una isogenia $\deg : Hom(E_1, E_2) \longrightarrow \mathbb{Z}$ es una forma cuadrática positivamente definida.

2.16. Corolario. *Sea E una curva elíptica y $m \in \mathbb{Z}$. Sea también $p = char(K)$.*

1. *Si $p \neq 0$ y p y m son primos relativos, o si $p = 0$, entonces*

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

2. *Si e es un entero positivo, entonces*

$$E[p^e] \simeq 0 \qquad \acute{o} \qquad E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}.$$

Capítulo 3

Curvas Elípticas Sobre $\mathbb{C}$ y Superficies Elípticas

En este capítulo se estudian las curvas elípticas definidas sobre el campo de los números complejos. También se estudiarán curvas elípticas sobre el campo de funciones de una curva, $k(C)$. Este último campo nos conduce al estudio de las superficies elípticas, a través de las cuales se generan familias de curvas elípticas. Se combinan la geometría algebraica y el análisis complejo para el estudio de este tipo de curvas. Los resultados que en este capítulo se presentan pueden ser encontrados en [Sil96] y [Ahl79].

3.1 Funciones Elípticas

En esta sección se define el concepto de retícula dentro de $\mathbb{C}$, en el capítulo 5 se da una definición más general de este concepto.

Definición. 1. Una *retícula* Λ es un subgrupo aditivo discreto de $\mathbb{C}$ que contiene una base de $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$.

2. Una *función elíptica* (relativa a una retícula Λ) es una función meromorfa $f : \mathbb{C} \to \mathbb{C}$, que satisface

$$f(x + \omega) = f(x)$$

para cualquier $\omega \in \Lambda$. Se denotará por $\mathbb{C}(\Lambda)$ al conjunto de todas las funciones elípticas relativas a Λ.

3. Si $\{\omega_1, \omega_2\}$ es una base de Λ, entonces una *región fundamental* de Λ es un conjunto de la forma

$$\{a + t_1\omega_1 + t_2\omega_2 | 0 \leq t_1, t_2 < 1\},$$

donde $a \in \mathbb{C}$. Cuando nos refiramos a cualquier región fundamental escribiremos $\mathbb{C}/\Lambda$.

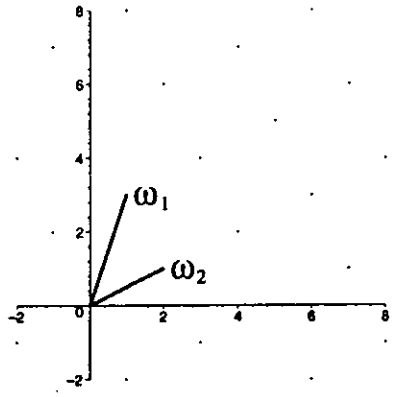

Figura 3.1: Retícula

Tenemos algunas propiedades resumidas en el siguiente teorema.

3.1. Teorema. *Sea* $f \in \mathbb{C}(\Lambda)$.

1. *Si* f *no tiene polos, entonces es constante.*
2. $\sum_{\omega \in C/\Lambda} res_\omega(f) = 0.$
3. $\sum_{\omega \in C/\Lambda} ord_\omega(f) = 0.$
4. $\sum_{\omega \in C/\Lambda} res_\omega(f)\omega \in \Lambda.$

El *orden* de una función elíptica es el número de polos, contados con multiplicidad, de la función en una región fundamental.

El *grupo de divisores* $Div(\mathbb{C}/\Lambda)$ de Λ, es el grupo libre generado por los elementos de $\mathbb{C}/\Lambda$. El *grado* de un divisor $D = \sum n_\omega(\omega)$ es $\sum n_\omega$ y lo denotaremos por $grad(D)$. Por último se denotará $Div^0(\mathbb{C}/\Lambda)$ al subgrupo

$$\{D \in Div(\mathbb{C}/\Lambda) | grad(D) = 0\}.$$

3.1.1 Construcción de Curvas Elípticas

Sea Λ una retícula. La *función* φ *de Weierstrass* (relativa a Λ) está definida por la serie

$$\varphi(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

La *serie de Eisenstein* de altura $2k$ (respecto a Λ) es la serie

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \omega^{-2k}.$$

3.2. Teorema. *Sea* Λ *una retícula.*

1. *La serie de Eisenstein G_{2k} de Λ es absolutamente convergente para toda k mayor que uno.*
2. *La serie que define la función φ de Weierstrass converge absoluta y uniformemente en todo subconjunto compacto de $\mathbb{C} - \Lambda$. Ésta define una función meromorfa en $\mathbb{C}$ que tiene polos dobles con residuos cero en cada punto de la retícula, sin más polos que éstos.*
3. *La función φ de Weierstrass es una función elíptica par.*

Es fácil ver que el conjunto de funciones elípticas relativas a una retícula Λ es un campo.

3.3. Teorema. *Sea Λ una retícula. Entonces $\mathbb{C}(\Lambda) = \mathbb{C}(\varphi(z), \varphi'(z))$. Es decir, que el conjunto de funciones elípticas relativas a Λ es un cociente de polinomios con $\varphi(z), \varphi'(z)$ como variables.*

Existe una relación algebraica entre $\varphi(z)$ y $\varphi'(z)$ que posteriormente nos permitirá establecer una conexión entre las funciones elípticas y la curvas elípticas.

3.4. Teorema. 1. *La serie de Laurent de $\varphi(z)$ en $z = 0$ está dada por*

$$\varphi(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1)(G_{2k+2} z^{2k}).$$

2. *Para toda $z \in \mathbb{C} - \Lambda$ se tiene*

$$\varphi'(z)^2 = 4\varphi(z)^3 - 60G_4\varphi(z) - 140G_6.$$

Como es comúnmente usado definimos los siguientes valores asociados a una retícula:

$$\begin{aligned} g_2 &= 60G_4, \\ g_3 &= 140G_6. \end{aligned}$$

También definimos el discriminante de la retícula como

$$\Delta(\Lambda) = g_2^3 - 27g_3^2.$$

La siguiente proposición es la que permite construir curvas elípticas a partir de una retícula, además de dotar de estructura de superficie de Riemann a esta curva.

3.5. Proposición. *Sean g_2, g_3 los valores asociados a una retícula Λ.*

1. *El polinomio $f(x) = 4x^3 - g_2 x - g_3$ no tiene raíces repetidas y su discriminante, $\Delta(\Lambda)$, es distinto de cero.*
2. *Si E es la curva elíptica definida por $y^2 = f(x)$. Entonces la función*

$$\phi : \mathbb{C}(\Lambda) \to E \qquad z \mapsto [\varphi(z), \varphi'(z), 1]$$

es un isomorfismo de superficies de Riemann que es también un homomorfismo de los grupos de $\mathbb{C}/\Lambda$ en $\mathbb{C}(E)$.

3.1.2 Retículas homotéticas

Si Λ_1 y Λ_2 son dos retículas tales que $\alpha\Lambda_1 = \Lambda_2$ con $\alpha \in \mathbb{C}^*$, diremos entonces que estas retículas son *homotéticas*. Tenemos que la función

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \qquad \phi_\alpha(z) = \alpha z \ mod(\Lambda_2)$$

es holomorfa y es un homomorfismo.

3.6. Teorema. *1. La asociación*

$$\{\alpha \in \mathbb{C} | \alpha\Lambda_1 \subset \Lambda_2\} \to \{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 | \phi(0) = 0\}$$

$$\alpha \mapsto \phi_\alpha$$

es una biyección.

2. *Sean E_1 y E_2 las curva elípticas correspondientes a Λ_1 y Λ_2. Entonces la inclusión natural de las isogenias de E_1 a E_2 a las funciones holomorfas de $\mathbb{C}/\Lambda_1$ en $\mathbb{C}/\Lambda_2$ es una biyección.*

3.7. Corolario. *Sean $E_1/\mathbb{C}$ y $E_2/\mathbb{C}$ las curvas elípticas correspondientes a las retículas Λ_1 y Λ_2. Entonces E_1 y E_2 son isomorfas si, y sólo si Λ_1 y Λ_2 son homotéticas.*

A continuación se relacionan tres categorías que resultan ser equivalentes

3.8. Teorema. *Sean $A, B \in \mathbb{C}$ tales que $A^3 - 27B^2 \neq 0$. Entonces existe una única retícula Λ tal que $g_2(\Lambda) = A$ y $g_3(\Lambda) = B$.*

3.9. Corolario. *Sea $E/\mathbb{C}$ una curva elíptica. Entonces existe una única retícula Λ, salvo homotecia, y un isomorfismo complejo analítico*

$$\phi : E/\mathbb{C} \to E(\mathbb{C}) \qquad \phi(z) = [\varphi(z;\Lambda), \varphi'(z;\Lambda), 1]$$

de grupos de Lie complejos.

3.10. Teorema. *Las siguientes categorías son equivalentes*

1. *Objetos: Curvas elípticas sobre $\mathbb{C}$. Morfismos: Isogenias.*
2. *Objetos: Curvas elípticas sobre $\mathbb{C}$. Morfismos: Funciones complejas analíticas que dejen fijo O.*
3. *Objetos: Retículas Λ, salvo homotopía. Morfismos: $\{\alpha \in \mathbb{C} | \alpha\Lambda_1 \subset \Lambda_2\}$.*

3.11. Proposición. *Sea $E/\mathbb{C}$ una curva elíptica y m un entero mayor que cero. Entonces se cumple:*

1. *$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*
2. *La isogenia $[m] : E \to E$ tiene grado m^2.*

Sea k un campo numérico. Un *orden* R de k es un subanillo de k que es finitamente generado como $\mathbb{Z}$-módulo y tal que $R \otimes k = k$.

3.12. Teorema. *Sea $E(\mathbb{C})$ una curva elíptica, y sean ω_1, ω_2 generadores de la retícula Λ asociada a E. Entonces $End(E) = \mathbb{Z}$; ó $\mathbb{Q}(\omega_1/\omega_2)$ es una extensión cuadrática imaginaria de $\mathbb{Q}$ y $End(E)$ es isomorfo a un order en $\mathbb{Q}(\omega_1/\omega_2)$.*

3.2 El Grupo Modular

Sea $\Lambda \subset \mathbb{C}$ una retícula. Entonces ésta se puede escribir como la suma $\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$, donde $\{\omega_1,\omega_2\}$ genera a Λ y que el ángulo entre ω_1 y ω_2 sea positivo de modo que $Im(\omega_1/\omega_2) > 0$. Si tenemos una base de esta forma, diremos entonces que ésta está orientada. Así nos basta con considerar el semiplano superior complejo,

$$H = \{\tau \in \mathbb{C} \mid Im\tau > 0\}.$$

Fijémonos en el conjunto de retículas bajo la relación de equivalencia por homotopía. Podemos escribir

$$\frac{1}{\omega_2}\Lambda = \mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}.$$

De este modo se puede asignar a cada elemento τ de H una retícula

$$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}.$$

Sea

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{M}_{2\times 2}(\mathbb{Z}) \middle| \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1 \right\}$$

el conjunto de matrices invertibles de dos por dos en el anillo de los números enteros.

Tenemos las siguientes propiedades

3.13. Lema. *1. Sea Λ una retícula, y sean $\{\omega_1,\omega_2\}$ y $\{\omega_1',\omega_2'\}$ dos bases orientadas de Λ. Entonces existe una matriz $M \in \mathrm{SL}_2(\mathbb{Z})$ tal que*

$$(\omega_1,\omega_2)M = (\omega_1',\omega_2').$$

2. Sean $\tau_1,\tau_2 \in H$. Entonces Λ_1 es homotética a Λ_2 si, y sólo si existe una matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \qquad \text{tal que} \qquad \tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}.$$

3. Para toda retícula Λ existe un $\tau \in H$ tal que Λ es homotética a

$$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}.$$

Se puede ver fácilmente que la matriz

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

es la única matriz no trivial de $\mathrm{SL}_2(\mathbb{Z})$ que deja fijos a todos los elementos de H.

El *grupo modular*, denotado por $\Gamma(1)$ es el cociente de grupos

$$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{I,-I\}.$$

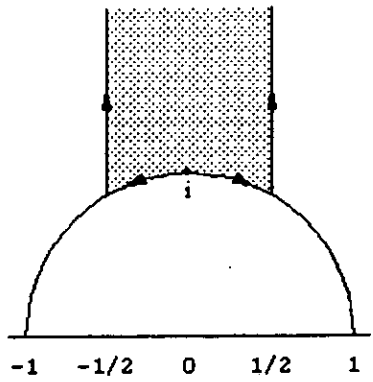

Figura 3.2: Región Fundamental

3.14. Proposición. *El grupo modular* $\Gamma(1)$ *esta generado por los elementos*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad y \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

De esto se tiene que el grupo modular actúa en el semiplano H.

3.15. Proposición. *El conjunto*

$$F = \{\tau \in H \mid |\tau| \geq 1,\ |Re(\tau)| \leq \frac{1}{2}\}$$

es una región fundamental de la acción de $\mathrm{SL}_2(\mathbf{Z})$ *en* H.

De este modo es posible ver que el espacio cociente $\Gamma(1) \setminus H$ como la dos esfera de Riemann.

El *plano superior extendido* H^* es la unión de los conjuntos

$$H^* = H \cup \mathbb{P}^1(\mathbb{Q}).$$

Los puntos de $\mathbb{P}^1(\mathbb{Q})$ se llaman *cúspides* de H^*.

Se puede extender la acción de $\Gamma(1)$ a H^* bajo la acción

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}.$$

3.2.1 La Curva Modular $X(1)$

Se definen ahora

$$Y(1) = \Gamma(1) \setminus H \qquad \text{y} \qquad X(1) = \Gamma(1) \setminus H^*.$$

Podemos formar una topología en H^* si tomamos como base a las vecindades usuales de los puntos en H; los conjuntos

$$\{\tau \in H \ : \ Im(\tau) > k\} \cup \{\infty\}$$

como vecindades de ∞; y los conjuntos de la forma

$$\{ \text{ interior de un circulo tangente al eje real } \} \cup \{\tau\}$$

como vecindades los demás puntos de $\mathbb{P}^1(\mathbb{Q})$.

De este modo podemos dotar a $X(1) = \Gamma(1) \setminus H^*$ de la topología débil obtenida de la inclusión $\phi : H \to X(1)$.

3.16. Proposición. *Es espacio topológico antes definido en $X(1)$ es Hausdorff.*

3.3 Uniformización en Curvas Elípticas

Las curvas elípticas definidas sobre el campo de los número complejos pueden ser parametrizadas por funciones elípticas. Definimos el invariante $j-$modular $j(\tau)$ como la función

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)}.$$

De modo que $j(\tau)$ es el invariante j de la curva elíptica

$$E_{\Lambda_\tau} : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

y $E_{\Lambda_\tau}(\mathbb{C})$ se puede parametrizar usando la función φ de Weierstrass

$$\begin{array}{rcl} C/\Lambda_\tau & \longrightarrow & E_{\Lambda_\tau}(\mathbb{C}) \\ z & \longrightarrow & (\varphi(z,\Lambda_\tau), \varphi'(z,\Lambda_\tau)). \end{array}$$

El siguiente resultado nos permite ver cómo se parametrizan las curvas elípticas a través de las funciones de Weierstrass.

3.17. Teorema. *La función $j(\tau)$ induce un isomorfismo de variedades analíticas complejas*

$$j : X(1) \backsimeq \mathbb{P}^1(\mathbb{C}).$$

De lo anterior tenemos los siguientes resultados

3.18. Corolario. *Sea f una función modular de altura 0.*

1. *La función f es una función racional de j, es decir, $f \in \mathbb{C}(j)$.*
2. *Si además f es holomorfa en H, entonces f es una función polinomial de j, es decir, $f \in \mathbb{C}[j]$.*

Y también como corolario tenemos el teorema de uniformización para curvas elípticas sobre $\mathbb{C}$.

3.19. Corolario. *Sean $A, B \in \mathbb{C}$ tales que $4A^3 + 27B^2 \neq 0$. Entonces existe una única retícula $\Lambda \subset \mathbb{C}$ tal que*

$$g_2(\Lambda) = 60G_4(\Lambda) = -4A \qquad y \qquad g_3(\Lambda) = 140G_6(\Lambda) = -4B.$$

Además la correspondencia

$$\begin{aligned} C/\Lambda &\longrightarrow E : y^2 = x^3 + Ax + B, \\ z &\longrightarrow \left(\wp(z,\Lambda), \frac{1}{2}\wp'(z,\Lambda)\right) \end{aligned}$$

es un isomorfismo de variedades analíticas complejas.

En resumen podemos decir que hay una correspondencia uno a uno entre el conjunto de curvas elípticas bajo isomorfismo en $\mathbb{C}$ y el conjunto de retículas bajo equivalencia homotética.

$$\frac{\{\text{curvas elípticas sobre } \mathbb{C}\}}{\mathbb{C}-\text{isomorfismo}} \simeq \frac{\{\text{retículas}\}}{\text{homotecia}}.$$

3.4 Familias de Curvas Elípticas

En ocasiones nos interesará trabajar con familias de curvas en lugar de considerar una en particular. Una forma de hacer esto es fijarnos en el campo de funciones de una curva C y definir una curva elíptica sobre este campo, $E/k(C)$. Cuando valuamos una función $f \in k(C)$ en algún punto $P \in C$, que no sea un polo de f, lo que obtenemos es un valor del campo k. De esta forma podemos definir una curva E_P/k para casi todo punto $P \in C$. Por supuesto que lo que nos interesa es que estas curvas E_P sean elípticas. En esta sección se da una introducción a esta forma de parametrizar curvas elípticas y se enuncia el teorema de Mordell-Weil para este caso. Los resultados que aquí se presentan pueden ser encontrados en [Sil96].

3.20. Ejemplo. 1. Consideremos la curva

$$E : y^2 = x^3 + A(T)x + B(T)$$

con las funciones racionales $A(T), B(T) \in \mathbb{Q}(T)$ tales que

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

sea distinto de cero. Lo que tenemos entonces es una curva definida sobre $\mathbb{Q}(T)$, que además representa una familia de curvas

$$E_t : y^2 = x^3 + A(t)x + B(t)$$

parametrizada por los valores $t \in \mathbb{Q}$.

2. De forma más general se puede considerar una curva proyectiva C/k sin singularidades y definir

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

con $A, B \in k(C)$ tales que $\Delta = 4A^3 + 27B^2 \neq 0$. Entonces para casi todo punto $P \in C(\bar{k})$ podemos evaluar A y B en P para obtener una curva

$$E_t : y^2 = x^3 + A(P)x + B(P)$$

que es elíptica siempre y cuando $\Delta(P) \neq 0$.

Una curva $E/k(C)$ tiene por definición dimensión igual a uno. Pero Si C es una curva, entonces el grado de trascendencia de $k(C) : k$ es uno. Por lo que cada elemento de $k(C)$ se puede pensar como un elemento de $\overline{k(T)}$, es decir, que si agregamos a T como variable, entonces E se puede pensar como una superficie (variedad algebraica de grado dos) definida sobre el campo k. Por ejemplo la curva definida anteriormente (ejemplo 3.20).

3.4.1 Superficies Elípticas

En el ejemplo 3.20 se puede pensar a la curva E como el conjunto

$$\varepsilon = \left\{([X, Y, Z], t) \in \mathbb{P}^2 \times C \mid Y^2Z = X^3 + A(t)XZ^2 + B(t)Z^3\right\}.$$

Este último conjunto resulta ser una subvariedad de $\mathbb{P}^2 \times C$ formada por una familia de curvas elípticas. Podemos entonces definir el morfismo

$$\pi : \varepsilon \longrightarrow C, \qquad ([X, Y, Z], t) \longmapsto t.$$

Para casi todo $t \in C$, la *fibra*

$$\varepsilon_t = \pi^{-1}(t) = \{P \in \varepsilon \mid \pi(P) = t\}$$

es una curva E_t. Asumiendo que

$$\Delta = -16(4A^3 + 27B^2) \neq 0 \text{ en } k(C),$$

basta con usar $t \in C$ tal que $A(t) \neq \infty$, $B(t) \neq \infty$ y $\Delta(t) \neq 0$ para obtener curvas elípticas.

En realidad todavía no hemos definido una familia de curvas elípticas ya que no se ha mencionado nada acerca del punto distinguido O que sirve como neutro en el grupo de puntos de la curva. Para definir estos puntos distinguidos usamos

$$O_t = ([0, 1, 0], t) \in \varepsilon_t \subset \mathbb{P}^2 \times C.$$

Esta propiedad se puede describir de otra forma. Como cada fibra ε_t es una curva elíptica con un elemento distinguido O_t, tenemos la función

$$\begin{aligned} \sigma_0 &: C \longrightarrow \varepsilon, \\ &: t \longmapsto O_t. \end{aligned}$$

Es posible ver a los puntos O_t como una familia algebraica de puntos, o de forma equivalente, a σ_0 como una aplicación racional entre variedades.

Podemos ahora definir formalmente lo que es una superficie elíptica.

Definición. Sea C una curva proyectiva suave. Una ***superficie elíptica sobre*** C consiste de los siguientes datos:

1. una superficie ε, es decir, una variedad proyectiva de dimensión igual a dos,
2. un morfismo
$$\pi : \varepsilon \longrightarrow C$$
tal que, salvo un núumero finito de puntos, la fibra
$$\varepsilon_t = \pi^{-1}(t)$$
es una curva suave de género igual a uno,
3. un morfismo
$$\sigma_0 : C \longrightarrow \varepsilon$$
tal que $\sigma_0(t) \in \varepsilon_t$.

Sean $\pi : \varepsilon \to C$ y $\pi' : \varepsilon' \to C$ dos superficies elípticas definidas sobre la misma curva C. Una *aplicacón racional de* ε *en* ε' *sobre* C es una aplicación racional $\phi : \varepsilon \to \varepsilon'$ que conmuta con las proyecciones, es deçir, $\pi' \circ \phi = \pi$. Si tal aplicación $\phi : \varepsilon \to \varepsilon'$ existe y además es un isomorfismo diremos entonces que ε y ε' son *birracionalmente equivalentes*. Si esta aplicación y estas superficies están definidas sobre el campo k, entonces diremos que ε y ε' son *$k-$birracionalmente equivalentes sobre* C.

Ahora enunciaremos un resultado que ralaciona las curvas elípticas definidas en el campo $k(C)$ con las superficies elípticas $\pi : \varepsilon \to C$ definidas enel campo k.

3.21. Proposición. *1. Sea $E/k(C)$ una curva elíptica. Si a cada ecuación de Weierstrass de E*
$$E : y^2 = x^3 + Ax + B, \qquad A, B \in k(C),$$
le asociamos la superficie elíptica
$$\varepsilon(A,B) = \left\{([X,Y,Z],t) \in P^2 \times C \mid Y^2Z = X^3 + A(t)XZ^2 + B(t)Z^3\right\}$$
descrita anteriormente, entonces todas estas curvas $\varepsilon(A,B)$ son k-birracionalmente equivalentes sobre C.

2. Para cada superficie elíptica sobre C definida en k existe una curva elíptica
$$E : y^2 = x^3 + Ax + B, \qquad A, B \in k(C)$$
(única salvo isomorfismos sobre $k(C)$) tal que ε y la superficie $\varepsilon(A,B)$ asociada a E son k-birracionalmente equivalentes.

De esta forma podemos asociar a cada superficie elíptica $\varepsilon \to C$ definida en k una curva elíptica $E/k(C)$. A esta curva le llamaremos *fibra genérica*.

3.4.2 Grupo de Secciones de una Superficie Elíptica

Sea $\pi : V \to W$ un morfismo entre variedades algebraicas. Una *sección para* π es un morfismo $\sigma : W \to V$ tal que la composición $\pi \circ \sigma : W \to W$ es la aplicación identidad.

3.22. Ejemplo. En el caso particular de una superficie elíptica $\pi : \varepsilon \to C$ la función que nos determina quién es el cero para cada curva elíptica $\varepsilon_t = \pi^{-1}(t)$ es la sección $\sigma_0 : C \to \varepsilon$, donde $O_t = \sigma_0(t)$.

Daremos una estructura de grupo a las secciones de una superficie elíptica $\varepsilon \to C$. Si σ_1 y σ_2 son dos secciones de ε, entonces para los valores $t \in C$ donde estas dos secciones estén definidas tenemos $\sigma_1(t),_2(t) \in \varepsilon_t$. Así, definimos

$$(\sigma_1 + \sigma_2)(t) = \sigma_1(t) + \sigma_2(t), \qquad (-\sigma_1)(t) = -\sigma_1(t).$$

Denotaremos por $\varepsilon(C/k)$ al conjunto de secciones de ε definidas en el campo k.

3.23. Proposición. *Sea $\varepsilon \to C$ una superficie elíptica definida en k y σ_1, σ_2 dos secciones de esta curva definidas también en k. Tenemos entonces que:*

1. *Las funciones $(\sigma_1 + \sigma_2)$ y $(-\sigma_1)$ definidas anteriormente están en $\varepsilon(C/k)$, lo cual da estructura de grupo a $\varepsilon(C/k)$.*
2. *Si $E/k(C)$ es la fibra genérica de ε, entonces existe un isomorfismos de grupos*

$$\begin{aligned} E(C/k) &\longrightarrow \varepsilon(C/k), \\ P = (x_P, y_P) &\longmapsto (\sigma_P : t \mapsto (x_P(t), y_P(t), t)). \end{aligned}$$

De esta forma se pueden pensar los puntos de una curva elíptica $E(k(C))$ como las secciones de la superficie elíptica $\varepsilon(A, B)$ asociada a alguna ecuación de Weierstrass

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

como en el ejemplo 3.20.

Capítulo 4

El Grupo de Mordell-Weil

Como ya se mencionó anteriormente el conjunto de puntos $K-$racionales de una curva elíptica forma un grupo. En particular nos interesará el estudio de los puntos $\mathbb{Q}-$racionales de curvas elípticas definidas sobre $\mathbb{Q}$. En este capítulo se estudia este grupo para diversos campos, incluidos los campos finitos para los cuales se cuenta con fórmulas explícitas para calcular la cantidad de puntos las curvas elípticas con coordenadas en estos campos (Ver [Sil86]).

4.1 Descripción del Grupo de Puntos Racionales en Cúbicas

Siempre que tenemos una cúbica C y un punto O no sigular ésta, podemos dar estructura de grupo a sus puntos K-racionales, $K(C)$ (ver 2.1.2). También será importante conocer la estructura que tienen las cúbicas singulares, lo cual se verá en esta sección.

4.1.1 Formas Mínimas

Clasificaremos las curvas definidas por ecuaciones de Weierstrass bajo isomorfismos. Cuando estamos trabajando en un campo algebraicamente cerrado basta con fijarnos en el $j-$invariante (página 28). Pero aún cuando dos curvas sean isomorfas dentro de un campo K, no necesariamente lo son dentro de un subcampo F de K. De la misma forma, dos curvas que sean isomorfas en $\mathbb{C}$, no lo son necesariamente dentro de $\mathbb{Q}$. Para estudiar este tipo de ismorfismos será necesario usar lo que se conoce como forma mínima de la ecuación de Weierstrass.

Sea K un campo local completo respecto a una valuación v, y R_K el anillo de enteros de K (ver 1.1.2). Es posible reducir toda ecuación de Weierstrass de forma que sus coeficientes a_1, a_2, a_3, a_4 y a_6 pertenezcan a R_K.

Sea E/K una curva elíptica. Diremos que la ecuación de Weierstrass que la define es *mínima* si $v(\Delta) \in R_K$, y además $v(\Delta)$ es el mínimo valor para el cual $a_1, a_2, a_3, a_4, a_6 \in R_K$.

4.1. Proposición. *1. Toda curva elíptica E/K tiene una ecuación mínima de Weierstrass.*

2. Toda ecuación mínima de Weierstrass es única salvo un cambio de coordenadas de la forma

$$x = u^2x + r, \qquad y = u^3y + u^2sx + t$$

donde $u \in R_K^*$ y $s, t \in R_K$.

3. Conversamente, si se tiene una ecuación de Weierstras con coeficientes en R_K, entonces todo cambio de coordenadas

$$x = u^2x + r, \qquad y = u^3y + u^2sx + t$$

que sirva para llegar a una ecuación mínima de Weierstrass satisface que $u, r, t \in R_K$.

De acuerdo con la definición de Δ, al reesecribir una ecuación de Weierstrass en nuevos términos como se menciona en la proposición anterior, se obtiene un discriminante nuevo de la forma $\Delta' = u^{12}\Delta$. De lo anterior podemos concluir que una ecuación de Weierstrass es mínima si, y sólo si $v(\Delta) < 12$. Es fácil ver que esto último se cumple también cuando $v(c_4) < 4$ ó $v(c_6) < 6$.

4.2 Reducción Módulo π

Cuando se tiene un anillo local R, podemos hablar de un generador de su único ideal maximal. Sea π uno de estos generadores del ideal maximal πR de R. Tenemos entonces el morfismo natural

$$\begin{array}{rccc} \Gamma & : & R & \longrightarrow R/\pi R \\ t & \longmapsto & \widetilde{t}. & \end{array}$$

Denotaremos con k al campo cociente del anillo entre su ideal maximal

$$k = R/\pi R.$$

Si tomamos una ecuación mínima de Weierstrass para definir E/K, podemos entonces reducir esta módulo π a una nueva curva

$$\widetilde{E} : y^2 + \widetilde{a}_1xy + \widetilde{a}_3y = x^3 + \widetilde{a}_2x^2 + \widetilde{a}_4x + \widetilde{a}_6.$$

Esta última curva $\widetilde{E}/k$ es la *reducción módulo el uniformizador* π de la curva original E/K. Dicha curva se define por una ecuación de Weierstrass, pero no es necesariamente una curva elíptica, sin embargo el conjunto de puntos no singulares de esta curva es también un grupo.

4.2. Proposición. *Sea E/K un curva elíptica y $m \geq 1$ un entero primo relativo con la característica del campo k.*

1. *El núcleo* $\ker(\Gamma)$ *de la reducción carece de puntos no triviales de* $m-$*torsión.*
2. *Si la curva* $\tilde{E}/k$ *es elíptica, entonces la función restricción*

$$E(K)[m] \longrightarrow \tilde{E}(k)$$

es inyectiva. Aquí. $E(K)[m]$ *son los puntos de* $m-$*torsión de* $E(K)$.

Definición. Sea $\tilde{E}$ la reducción de una curva elíptica E definida por una ecuación de Weierstrass. Diremos que:

1. E tiene una buena reducción si $\tilde{\Delta} \neq 0$, es decir, $\tilde{E}$ es una curva no singular.
2. E tiene una reducción multiplicativia si $\tilde{E}$ es nodal.
3. E tiene una reducción aditiva si $\tilde{E}$ es cuspidal.

En los últimos dos casos diremos que E tiene mala reducción.

Podemos ahora clasificar las curvas elípticas según el tipo de reducción.

4.3. Proposición. *Sea* E/K *una curva elíptica definida por una ecuación mínima de Weierstrass.*

1. E *tiene buena reducción si, y sólo si* $v(\Delta) = 0$, *es decir que* $\Delta \in R^*$;
2. E *tiene reducción multiplicativa si, y sólo si* $v(\Delta) > 0$ *y* $v(c_4) = 0$;
3. E *tiene reducción aditiva si, y sólo si* $v(\Delta) > 0$ *y* $v(c_4) > 0$.

El tipo de reducción nos permite analizar el grupo de torsión de una curva elíptica, como se establece a continuación.

4.4. Proposición. *Sea* E/K *una curva elíptica y* $m \geq 1$ *un entero primo relativo con la característica del campo* k.

1. *El núcleo del homomorfismo natural*

$$\ker(\Gamma : R \longrightarrow R/\pi R)$$

no tiene puntos de torsión distintos de O.

2. *Si* E *tiene buena reducción, entonces la función*

$$E(K)[m] \longrightarrow \tilde{E}(k)$$

es inyectiva.

De esta forma podemos estudiar la parte de torsión de curvas elípticas a partir de sus reducciones que son campos de característica distinta de cero.

4.3 Curvas Elípticas Sobre Campos Finitos

Todos los resultados referentes a las ecuaciones de Weierstrass que se han dado anteriormente son válidos para campos de característica distinta de dos o tres. Primero presentaremos los resultados equivalentes a lo dados en 2.2 para estos campos. Después se hará el análisis general de las curvas definidas sobre campos finitos.

4.3.1 Curvas Elípticas Sobre Campos con Característica Igual a Dos y Tres.

Supondremos en este párrafo que se esta trabajando en un campo K con característica igual a dos o tres.

4.5. Proposición. *Sea E/K una curva definida por una ecuación de Weierstrass. Existen $u \in K^*$ y $r, s, t \in K$ tales que las substituciones*

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

nos conducen a las ecuaciones dadas según se indica en los siguientes casos.

1. *Si $\mathrm{char}K = 3$ y $j(E) \neq 0$, entonces*

$$y^2 = x^3 + a_2x^2 + a_6 \qquad \Delta = -a_2^3a_6 \qquad j = -a_2^3/a_6.$$

2. *Si $\mathrm{char}K = 3$ y $j(E) = 0$, entonces*

$$y^2 = x^3 + a_4x + a_6 \qquad \Delta = -a_4^3 \qquad j = 0.$$

3. *Si $\mathrm{char}K = 2$ y $j(E) \neq 0$, entonces*

$$y^2 + xy = x^3 + a_2x^2 + a_6 \qquad \Delta = a_6 \qquad j = 1/a_6.$$

4. *Si $\mathrm{char}K = 2$ y $j(E) = 0$, entonces*

$$y^2 + a_3y = x^3 + a_4x + a_6 \qquad \Delta = a_3^4 \qquad j = 0.$$

Cuando se tiene una campo con característica dos, se puede escribir algo equivalente a la forma de Legendre definida en página 25.

4.6. Proposición. *Sea E/K una curva elíptica, con $\mathrm{char}(K) \neq 3$. Entonces E tiene una ecuación de Weierstrass sobre $\overline{K}$ de la forma*

$$E_\alpha : y^3 + \alpha xy + y = x^3 \qquad \alpha \in \overline{K},\ \alpha \neq 27.$$

Esta ecuación tiene discriminante y $j-$invariante dados por

$$\Delta = \alpha^3 - 27 \qquad j = \alpha^3(\alpha^3 - 24)^3/(\alpha^3 - 27)^3 = 0.$$

4.3.2 Cantidad de Puntos en Curvas Elípticas

En esta sección supondremos que K es un campo con q elementos y de característica p distinta de cero. Para cada entero no negativo n, denotaremos por K_n a la extensión de K de grado n. Usaremos $\#V(E/K_n)$ para indicar la cantidad de puntos K_n-racionales de la variedad V/K.

Definición. Sea V/K una variedad. Definimos la función zeta como

$$Z(V/K, t) = \exp\left(\sum \#V(E/K_n)\frac{t^n}{n}\right).$$

En el caso particular de curvas de género igual a uno tenemos el siguiente resultado.

4.7. Teorema (Weil). *Si E/K es una curva elíptica. Entonces existe $a \in \mathbb{Z}$ tal que*

$$Z(V/K,t) = \frac{1 - at + qt^2}{(1-t)(1-qt)}.$$

4.3.3 El Invariante de Hasse

Ahora supondremos que K es una campo perfecto, finito y de característica $p \neq 0$.

4.8. Teorema. *Sea E/K una curva elíptica. Para cada entero no negativo r, sean*

$$\begin{array}{rcl} \phi_r & : & E \longrightarrow E^{(p^r)} \\ a & \longmapsto & a^{(p^r)} \\ & & y \\ \widehat{\phi} & : & E^{(p^r)} \longrightarrow E \end{array}$$

el p^r – automorfismo de Frobenius y su automorfismo dual respectivamente.

1. *Las siguientes afirmaciones son equivalentes.*
   (a) *$E[p^r] = 0$ para algún $r \geq 0$.*
   (b) *ϕ_r es puramente inseparable para algún $r \geq 0$.*
   (c) *La función $[p] : E \longrightarrow E$ es puramente inseparable y $j(E) \in \mathbb{F}_p$.*
2. *Si no se cumple lo anterior, entonces $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ para todo entero no negativo r y el grupo formal $\widehat{E}/K$ tiene altura igual a uno*

Si una curva cumple las condiciones de la primera parte del teorema anterior diremos entonces que la curva E es *supersingular*. El siguiente teorema da un criterio para saber cuándo una curva es supersingular.

4.9. Teorema. *Sea K un campo de característica mayor a dos.*

1. *Sea E/K una curva elíptica definida por una ecuación*

$$E : y^2 = f(x)$$

   donde $f(x) \in K[x]$ es de grado tres con raíces distintas en $\overline{K}$. Entonces E es supersingular si, y sólo si el coeficiente de x^{p-1} en $f(x)^{(p-1)/2}$ es cero.
2. *Sea $m = (p-1)/2$. Definimos el polinomio*

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

Si $\lambda \in \overline{K}$ es distinto de cero o uno, entonces la curva elíptica

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

es supersingular si, y sólo si $H_p(\lambda) = 0$.

3. *El polinomio $H_p(t)$ tiene raíces distintas en $\overline{K}$. Y salvo isomorfismo, existen exactamente*

$$\left[\frac{p}{12}\right] + \epsilon_p$$

curvas elípticas supersingulares en característica p, donde $\epsilon_3 = 1$, y para $p \geq 5$,

$$\epsilon_p = 0, 1, 1, 2 \qquad si \qquad p \equiv 1, 5, 7, 11 mod 12 \qquad respectivamente.$$

4.10. Proposición. *Sea $E/\mathbb{F}_p$ una curva elíptica y $\phi : E \longrightarrow E$ el $q-$endomorfismo de Frobenius.*

1. *E es supersingular si, y sólo si $tr(\phi) \equiv 0 mod p$. (tr es el grado de trascendencia)*
2. *Si $p = q$, entonces E es supersingular si, y sólo si $\#E(\mathbb{F}_p) = p + 1$.*

4.4 Curvas Elípticas Sobre Campos Numéricos

Ahora trabajaremos con una campo numérico K, es decir, una extensión finita de $\mathbb{Q}$. Enunciaremos los resultados referentes al grupo de Mordell-Weil de los campos numéricos. Cabe mencionar que en la demostración de este teorema se usa una versión débil del mismo.

4.11. Teorema. (Mordell-Weil versión débil) *Sea K una campo numérico y m un entero mayor que uno. Si E/K es una curva elíptica, entonces $E(K)/Im([m])$ es un grupo finito.*

4.12. Teorema (Mordell-Weil). *En el contexto anterior, $E(K)$ es finitamente generado.*

De acuerdo con la teoría de grupos, tenemos que $E(K)$ es un grupo de la forma $E_{tor} \times \mathbb{Z}^r$, donde E_{tor} es el subgrupo de torsión de $E(K)$ y r es el *rango* de la curva. El problema de determinar todos los puntos $K-$racionales de una curva elíptica se reduce entonces a encontrar generadores de este grupo.

La parte de torsión del grupo de puntos $\mathbb{Q}-$racionales de una curva esta completamente determinada.

4.13. Teorema. *Sea $E/\mathbb{Q}$ una curva elíptica. El subgrupo de torsión $E(\mathbb{Q})_{tor}$ de $E(\mathbb{Q})$ es de alguna de las siguientes formas:*

1. $\mathbb{Z}/N\mathbb{Z}$ *para* $0 < N < 11$ *ó* $N = 12$;
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *con* $0 < N < 5$.

Para campos numéricos arbitrarios se tiene:

4.14. Teorema. *Sea $K/\mathbb{Q}$ un campo numérico y p un número primo. Entonces existe una constante N que depende sólo de K y de p tal que para toda curva elíptica E/K, el orden de la componente $p-$primaria de $E(K)$ es divisible por p^N.*

El Rango de Curvas Elípticas

La parte más difícil de determinar del grupo de puntos $K-$racionales de una curva elíptica es la parte libre. Para el caso de curvas sobre los números racionales se tiene la siguiente conjetura.

Para cada entero no negativo r, existe una curva elíptica definida sobre $\mathbb{Q}$, tale que el rango de $E(\mathbb{Q})$ es mayor o igual a r.

La parte central de esta tesis consiste en estudiar los algoritmos que se han empleado para encontrar curvas elípticas de rago mayor. No se ha podido calcular exactamente el rango de todas estas curvas, pero se da una cota mínima de este. La curva de rango más grande que se ha encontrado en curvas elípticas hasta el momento lo tiene mayor o igual a 23.

Capítulo 5

Funciones de Altura en $E(K)$

En este capítulo se prueba el teorema de Mordell-Weil para el grupo de puntos $\mathbb{Q}$–racionales de una curva elíptica $E/\mathbb{Q}$. Esta demostración se divide en dos partes, la primera tiene que ver con funciones de altura. La segunda parte es la versión débil, que en su demostración presenta a $E(K)/mE(K)$ como un subgrupo de $Hom(G_{L/K}, E[m])$ para una extensión finita de campos L/K, que resulta ser un grupo finito. Esto nos permite estudiar el grupo a través de $Hom(G_{L/K}, E[m])$. También se muestra esta teoría en el caso de superficies elípticas. Los resultados que aquí se presentan se pueden encontrar en [Sil86] [Sil96] y [Shi90].

5.1 Teoría de Alturas

Las funciones de altura se usan en general para estudiar puntos en variedades que son a su vez grupos. Estas variedades se conocen como variedades abelianas. Las curvas elípticas son un caso particular de estas veriedades y en este capítulo se revisará la teoría de alturas que se ocupará más adelante. Existe un programaa de computo para calcular el determinante de la matriz de alturas canónicas en curvas elípticas (PARI), con en cual podemos determinar si un conjunto de puntos de una curva elíptica es independiente.

5.1.1 Alturas en Curvas Elípticas

Definición. Sea G un grupo abeliano y $h : G \longrightarrow \mathbb{R}$ una función. Decimos que h es una función de altura si:

1. Para cualquier elemento $Q \in G$ existe una constante $C_1 \in \mathbb{R}$ que satisface

$$h(P+Q) - 2h(P) \leq C_1$$

para todo $P \in G$.

2. Existe un entero $m \geq 2$ y una constante C_2 tal que

$$m^2 h(P) - h(mP) \leq C_2$$

para todo $P \in G$.

3. Para todo número real C_3 y cualquier elemento P de G

$$|\{P \in G |\ h(P) \leq C_3\}| < \infty.$$

Existen distintas formas de definir funciones de altura. La siguiente proposición nos muestra un algoritmo importante en el cálculo del grupo de Mordell-Weil y es una parte crucial para demostrar que éste es finitamente generado.

5.1. Teorema. *Sea G un grupo abeliano, con una función de altura h y m el entero de la condición (2) de la definición anterior. Si $|G/mG| < \infty$, entonces G es finitamente generado.*

Demostración. Sean $Q_1, ..., Q_r$ representantes de los elementos de G/mG. Tenemos que cada $P \in G$ pertenece a alguna clase de equivalencia, es decir, $P - Q_{i_1} = mP_1$ para algún $P_1 \in G$. De esta forma podemos construir recursivamente

$$\begin{aligned} P &= mP_1 + Q_{i_1} \\ P_1 &= mP_2 + Q_{i_2} \\ &\cdots\cdots \\ P_{n-1} &= mP_n + Q_{i_n}. \end{aligned}$$

De donde se deduce

$$P = m^n P_n + \sum m^{j-1} Q_{i_j}.$$

Si ocupamos la condición (2) de la definición de altura, tenemos entonces la siguiente desigualdad

$$h(P_j) \leq \frac{1}{m^2}(h(mP_j) + C_2)$$

Usando que $P_{j-1} = mP_n + Q_{i_j}$ y (1) de la definición podemos escribir

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2) \\ h(P_{i_j}) &\leq \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2). \end{aligned}$$

En esta última desigualdad C_1' depende de Q_{i_j}. Tomemos C_1 como el máximo de todos estos valores para cada Q_i. De esta forma podemos usar esta desigualdad reiteradamente hasta llegar a

$$h(P_n) \leq (\frac{2}{m^2})^n h(P) + (C_1 + C_2)(\frac{1}{m^2} + \frac{2}{m^4} + ... + \frac{2^{n-1}}{m^{2n}}).$$

Podemos observar que

$$\frac{1}{m^2}\sum_{i=0}^{n-1}\frac{2^i}{m^{2i}} = \frac{(1-(\frac{2}{m^2})^n)}{(m^2-2)}$$

para llegar a la desigualdad

$$h(P_n) < (\frac{2}{m^2})^n h(P) + \frac{C_1+C_2}{m^2-2},$$

y para n suficientemente grande se tiene

$$h(P_n) < 1 + \frac{C_1+C_2}{2}.$$

Usando ahora el inciso (3) de la definición de altura se puede ver que P se genera con

$$\{Q_1,...,Q_r\} \cup \{Q \in G | h(Q) < 1 + \frac{C_1+C_2}{2}\}$$

que es finito, por lo tanto G es finitamente generado. □

5.1.2 Altura Simple

Definiremos una función de altura para el caso de los números racionales, la cual sirve para probar el teorema de Mordell-Weil.

Definición. Sea $p/q \in \mathbb{Q}$ con $(p,q) = 1$, definimos

$$H(p/q) = \max\{|p|,|q|\}.$$

La altura simple (o de Weill) sobre una curva elíptica es

$$h(x,y) = \begin{cases} \log H(x) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

Esta última función resulta ser efectivamente de altura, con lo que se prueba Mordell-Weill en el caso de $\mathbb{Q}$. Con esto basta probar la versión débil del teorema, lo cual haremos después de dar otras definiciones de función de altura que también pueden ser usadas en esta demostración y que además se ocuparan para verificar si algún conjunto de puntos en una curva elíptica es independiente.

5.1.3 Alturas en el Plano Proyectivo

Sea $P = [x_1, x_2, x_3] \in \mathbb{P}_2(\mathbb{Q})$. Siempre podemos tomar un representante de este punto de forma que x_1, x_2, x_3 sean enteros y primos relativos entre si. Podemos definir $H(P) = \max\{|x_1|,|x_2|,|x_3|\}$ y $h(P) = \log\ H(P)$. Esta última función resulta ser también de altura.

Para extender esta definición a campos numéricos es necesario tomar en cuenta los valores absolutos definidos en el campo.

Definición. Sea $P = [x_1, x_2, x_3]$ un punto de $\mathbb{P}_2(K)$, donde K es un campo numérico. Sea también

$$H(P) = \prod_{v \in M_K} \max\{|x_1|_v, |x_2|_v, |3|_v\}^{n_v}$$

donde M_K es el conjunto de valores absolutos no equivalentes de K y $n_v = [K_v : \mathbb{Q}_v]$ (ver 1.1.2. Definimos la *altura logarítmica* como la función $h : K \longrightarrow$ dada por

$$h(P) = \log\ H(P).$$

Esta última función resulta ser efectivamente de altura. Esta definición se puede extender a cualquier espacio proyectivo sobre K.

Siempre que tenemos una función $f \in \overline{K}(E)$ se puede pensar a ésta como una función $f : E \longrightarrow \mathbb{P}_1$, donde $f(P) = [f(P), 1]$ si $f(P) < \infty$ ó $[0, 1]$ si P es un polo de f.

Definición. Sea $f \in \overline{K}(E)$, donde E/K es una curva elíptica. Definimos la *altura (relativa a f)* en E como

$$h_f(P) = h(f(P)).$$

5.1.4 Altura Canónica

Una de las alturas más importantes que se usan para calcular el grupo de Mordell-Weill es la canónica. Esta altura permite saber cuándo un conjunto de elementos del grupo es independiente, lo cual nos sirve para establecer cotas del rango de curvas.

5.2. Teorema. *Sea E/K una curva elíptica y $f \in K(E)$ una función par no constante. Si $P \in E(\overline{K})$, entonces el límite*

$$\lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

existe y no depende de f.

Definición. Definimo la altura canónica (de Néron Tate) $\widehat{h} : E(K) \longrightarrow \mathbb{R}$ como

$$\widehat{h}(P) = \frac{1}{grad\ (f)} \lim_{N \to \infty} 4^{-N} h_f([2^N]P).$$

5.3. Teorema. *Sea E/K una curva elíptica.*

1. *Si $P, Q \in E(\overline{K})$, entonces*

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

2. *Para $P \in E(\bar{K})$ y $m \in \mathbb{Z}$ se tiene*

$$\hat{h}([m]P) = m^2 \hat{h}(P).$$

3. *La forma* $< P, Q >= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ *es bilineal.*

4. *Para cualquier* $P \in E(\overline{K})$, $\hat{h}(P) \geq 0$ *y se tiene que* $\hat{h}(P) = 0$ *si, y sólo si* $P \in E_{tor}$.

5. *Si* $f \in \bar{K}(E)$ *es par, entonces* $(grad f)\hat{h} = h_f +$ *términos lineales.*

5.4. Proposición. *Sean* V *un espacio vectorial sobre* $\mathbb{R}$ *de dimensión finita y* $\Lambda \subset V$ *una retícula. Si* $q : V \longrightarrow \mathbb{R}$ *es una forma cuadrática que cumple:*

1. *Si* $P \in \Lambda$, *entonces* $q(P) = 0$ *si, y sólo si* $P = 0$.

2. *Para cualquier constante* C, *el conjunto*

$$\{P \in \Lambda | q(P) \leq C\}$$

es finito. Entonces q *es positiva definida en* V.

5.5. Corolario. *La altura de Néron-Tate es una forma cuadrática positivamente definida.*

Definición. La forma bilineal $<,>$ antes definida se conoce como el *apareamiento de Néron-Tate* . Sean $P_1, ..., P_r \in E(K)$ representantes de cada clase en $E(K)/E_{tor}(K)$. El *regulador elíptico* $R_{E/K}$ de una curva elíptica E/K es el determinante de la matriz $(< P_i, P_j >) \in M_{r,r}(R)$. (Definimos por conveniencia $R_{E/K} = 1$ cuando $r = 0$).

5.6. Corolario. *El regulador elíptico de un conjunto de puntos es no negativo. Y es igual a cero si, y sólo si el conjunto de puntos es independiente.*

5.1.5 Apareamientos de Weil, y de Kummer

Sea E/K una curva elíptica definida sobre un campo K y $m \geq 2$ un entero primo relativo con la característica de K, si ésta es distinta de cero. Sea $T \in E[m]$, entonces existe $f \in \overline{K}(E)$ tal que se cumple la siguiente propiedad para divisores:

$$div(f) = m(T) - m(O).$$

También existe una función $g \in \bar{K}(E)$ tal que $f \circ [m] = g^m$.

Si suponemos además que $S \in E[m]$ es otro punto de m-torsión, entonces se tiene para cualquier punto $X \in E$,

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

De lo anterior podemos deducir que

$$\frac{g(X+S)}{g(X)}$$

es una raíz m-ésima de la unidad en K y esta no depende de la elección de X.

Definición. La función $e_m : E[m] \times E[m]$ (donde μ_m es el conjunto de raíces m-ésimas de la unidad) definida por:

$$e_m(S,T) = \frac{g(X+S)}{g(x)}$$

es el *apareamiento de Weil.*

5.7. Proposición. *El apareamiento de Weil Cumple las siguientes propiedades:*

1. $e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T)$ *y* $e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$;
2. $e_m(S,T) = e_m(T,S)^{-1}$;
3. *Si* $e_m(S,T) = 1$ *para toda* $S \in E[m]$, *entonces* $T = O$;
4. *Para todo* $\sigma \in G_{\overline{K}/K}$,

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma);$$

5. *Si* $S \in E[mm']$ *y* $T \in E[m]$, *entonces*

$$e_{mm'}(S,T) = e_m([m']S,T).$$

Estas propiedades básicas del apareamiento de Weil tienen un resultado que se ocupará más adelante.

5.8. Corolario. *Existen puntos* $S,T \in E[m]$ *tales que* $e_m(S,T)$ *es una raíz* m*-ésima primitiva de la unidad. Se tiene en particular que* $E[m] \subset E(K)$ *implica* $\mu_m \subset K^*$.

Tomando en cuenta este último resultado supondremos que $E[m] \subset E(K)$ para la siguiente definición (si esto no sucede podemos usar que $E[m]$ es finito y tomar una extensión finita de K).

Definición. Definimos el apareamiento de Kummer

$$k : E(K) \times G_{\overline{K}/K} \longrightarrow E[m]$$

de la siguiente forma. Si $P \in E(K)$, entonces escogemos $Q \in E(K)$ tal que $[m]Q = P$ y escribimos

$$\kappa(P,\sigma) = Q^\sigma - Q.$$

5.9. Proposición. *De acuerdo a la definición anterior:*

1. κ *esta bien definido.*
2. κ *es bilineal.*
3. $\ker(\kappa) = mE(K) \times G_{\overline{K}/L}$, *donde*

$$L = K([m]^{-1}E(K)).$$

De esta proposición podemos deducir lo siguiente.

5.10. Corolario. *El apareamiento de Kummer induce un apareamiento perfecto*

$$E(K)/mE(K) \times G_{L/K} \to E[m],$$

donde L es el mismo campo de la proposición anterior.

5.11. Corolario. *$E(K)/mE(K) \times G_{L/K}$ es un subgrupo del grupo de homomorfismos de $G_{L/K)}$ en $E[m]$ (denotado por $Hom(G_{L/K}, E[m])$).*

5.2 Aluras en Superficies Elípticas

Como se ha visto antes el uso de superficies elípticas es conveniente en el estudio de las curvas elípticas (ver 3.4), y también es posible definir funciones de altura en éstas.

A continuación se enuncia la versión débil del teorema de Mordell-Weil para curvas elípticas definidas sobre el campo de funciones de una curva.

5.12. Teorema. *Sea k un campo algebraicamente cerrado de característica igual a cero, sea $K = k(C)$ el campo de funciones de una curva, y sea E/K una curva elíptica. Entonces el grupo cociente $E(K)/2E(K)$ es finito.*

La demostración de este teorema es similar a la de la versión de curvas elípticas sobre campos numéricos.

5.2.1 Alturas en Curvas Elípticas Definidas Sobe Campos de Funciones

Sea E/K una curva elíptica sobre un campo de funciones. Ya se mencionó que el grupo $E(K)/2E(K)$ es finito (teorema 5.12). Para probar el teorema de Mordell-Weil en este caso es necesario definir funciones de altura como se hizo en el caso de campos numéricos.

Definición. Sea $K = k(C)$ un campo de funciones de una curva algebraica suave C/k. La *altura* de un elemento $f \in K$ se define como el grado de f vista como una función de C en $\mathbb{P}^1$

$$h(F) = grad(f : C \longrightarrow \mathbb{P}^1).$$

En particular, si $f \in k$, entonces tenemos $h(f) = 0$. Sea E/K una curva elíptica dada por la ecuación de Weierstrass

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

Definición. La *altura* de un punto $P \in E(K)$ está definida por

$$h(x) = \begin{cases} 0, & \text{si } P = O \\ h(x) & \text{si } P = (x, y) \end{cases}.$$

Hay que observar que efectivamente esta función de altura coincide con la de la definición y que $h(P)$ depende de la ecuación de Weierstrass con que se definió la curva.

Esta definición de altura tiene ciertas propiedades geométricas que se describen a continuación.

5.13. Teorema. *Sea E/K una curva elíptica definida sobre un campo de funciones.*

1. $h(2P) = 4h(P) + O(1)$ *para todo* $P \in E(K)$.
2. $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1)$.

Aquí, el valor de $O(1)$ depende sólo de la curva E.

Altura Canónica

Igual que se hace para curvas elípticas definidas sobre campos numéricos, es posible construir una altura canónica que resulta ser una forma cuadrática en el grupo $E(K)$.

5.14. Proposición. *Sea E/K una curva elíptica definida sobre el campo de funciones $K = k(C)$. Para cada punto $P \in E(K)$, el límite*

$$\lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$$

existe.

Definición. De acuerdo a la proposición anterior, definimos la altura canónica (o altura de Nerón-Tate) de un punto $P \in E(K)$ como el límite

$$\widehat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h(2^n P).$$

5.15. Teorema. *Sea E/K una curva elíptica definida sobre el campo de funciones $K = k(C)$.*

1. *La altura canónica cumple las siguientes propiedades:*
   (a) $\widehat{h}(P) = \frac{1}{2}h(P) + O(1)$ *para todo punto* $P \in E(K)$.
   (b) $\widehat{h}(mP) = m^2\widehat{h}(P)$ *para todo* $P \in E(K)$ *y* $m \in \mathbb{Z}$.
   (c) $\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$ *para todos* $P, Q \in E(K)$.
2. *La altura canónica es una forma cuadrática en $E(K)$, es decir, $\widehat{h}(-P) = \widehat{h}(P)$ y el apareamiento*

$$\begin{aligned} \langle \cdot, \cdot \rangle &: E(K) \times E(K) \longrightarrow \mathbb{R} \\ \langle P, Q \rangle &= \widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q) \end{aligned}$$

es bilineal.

Para poder enunciar en este caso el teorema de Mordell-Weil es necesario hacer cierta consideración. Diremos que una superficie elíptica $\varepsilon \longrightarrow C$ *se descompone sobre* k si existe una curva elíptica E_0/k y un isomorfismo birracional

$$i : \varepsilon \longrightarrow E_0 \times C$$

tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \varepsilon & \xrightarrow{i} & E_0 \times C \\ \pi \searrow & & \swarrow p_2 \\ & C & \end{array}$$

5.16. Proposición. *Sea $\varepsilon \longrightarrow C$ una curva elíptica sobre el campo k y E/K una curva elíptica, donde $K = k(C)$. Las siguientes afirmaciones son equivalentes:*

1. *$\varepsilon \longrightarrow C$ se descompone en k.*
2. *Existe una curva elíptica E_0/k isomorfa a E sobre K.*

Podemos ahora enunciar el teorema.

5.17. Teorema (Mordell-Weil). *Sea $\varepsilon \longrightarrow C$ una curva elíptica definida sobre una campo k, y E/K la correspondiente curva elíptica definida sobre el campo de funciones $K = k(C)$. Si $\varepsilon \longrightarrow C$ no se descompone, entonces $E(K)$ es finitamente generado.*

La idea de la demostración de este teorema es muy similar a la del caso de curvas elípticas definidas sobre campos numéricos, pero requiere un especial cuidado en el hecho de que $\varepsilon \longrightarrow C$ no se descomponga.

5.2.2 Retículas de Mordell-Weil

Una herramienta importante para saber cuándo un conjunto de puntos de una curva elíptica E/K es independiente es definir una forma bilineal simétria positivamente definida. Ésto se ha hecho usando la altura canónica, pero podemos definir de otra manera esta forma bilineal, la cuál será de gran utilidad ya que hay fórmulas explicitas con las que puede ser calculada. Los resultados que aquí se presentan se encuentran en [Shi90]. Aquí no se pretende definir ni demostrar todos los términos y resultados que se presentan, sino dar una idea de cómo se define esta otra forma bilineal y mostrar las fórmulas que nos permiten calcularla.

Cuando nos refiramos a una *retícula* estaremos pensando en un $\mathbb{Z}$-módulo libre de rango finito L, junto con una forma bilineal simétrica no degenerada

$$\langle , \rangle : L \times L \to \mathbb{Q}.$$

Si los valores de esta forma bilineal cáen dentro de $\mathbb{Z}$, diremos entonces que L es una retícula entera.

Sea $\pi : S \to C$ una superficie elíptica. Existe un equivalencia entre los divisores de esta superficie llamada *equivalencia algebraica* . En [Har77] se encuentra la definición y algunos resultados de este término. De momento lo único que nos interesa es saber que podemos hablar del grupo de divisores de S módulo equivalencia algebraica. A este grupo se le llama "Grupo de Néron-Severi" de S y se denota por $NS(S)$.

5.18. Teorema. *Sea E/K la fibra genériaca de la superficies elíptica*

$$\pi : S \to C.$$

Existe una única forma bilineal

$$Div(S) \times Div(S) \to Z \qquad (D_1, D_2) \to D_1 \cdot D_2$$

con las siguientes propiedades:

1. *Si T_1 y T_2 son curvas irreducibles en S que se intersecan en un cunjunto de puntos con multiplicidad igual a uno cada uno de ellos (intersección transversal). Entonces $T_1 \cdot T_2 = \#(T_1 \cup T_2)$.*
2. *Si D, D_1 y D_2 son divisores de S tales que $D \sim D_1$ y $D \sim D_2$, entonces $D \cdot D_1 = D \cdot D_2$.*
3. *Esta forma es independiente también de equivalencia algebraica.*

La demostración del resulatado anterior se encuentra en [Sil96] para los dos primeros incisos y en [Shi90] para el último. Además, usando bilineallidad podemos extender esta forma bilineal a $NS(S)_{\mathbb{Q}} = NS(S) \otimes \mathbb{Q}$ con el propósito de dar una forma bilideal a E/K.

5.19. Proposición. *Existe un homomorfismo de grupos $\varphi : E(K) \to NS(S)_{\mathbb{Q}}$ tal que:*

1. $\ker(\varphi) = E(K)_{tor}$.
2. *Sean $P, Q \in E(K)$, el apareamiento*

$$\langle P, Q \rangle = -\varphi(P) \cdot \varphi(Q)$$

define una forma bililneal simétrica positivamente definida no degenerada en $E(K)$ que induce una estructura de retícula positivamente definida en $E(K)/E(K)_{tor}$.

Así, tenemos ya definida una forma bilideal positivamente definida. La parte interesante de todo esto es que en el caso particular de que $\pi : S \to C$ sea una superficie elíptica sin fibras $\pi^{-1}(t)$ que sean curvas no irreducibles, hay fórmulas muy simples para calcular esta última forma bilineal, con lo cual es posible calcular el regulador de un conjunto de puntos (secciones en el caso de superficies elípticas). El siguiente teorema se prueba en [Shi90].

5.20. Teorema. *Sea $\pi : S \to C$ una superficie elíptica sin firbras no irreducibles, entonces*

1. $\langle P, Q \rangle = \chi + P \cdot O + Q \cdot O - P \cdot Q$.
2. $\langle P, P \rangle = 2\chi + 2P \cdot O$.

Donde χ es un valor que sólo depende de S y es conocido como su género aritmético.

Capítulo 6

Cálculo del Grupo de Mordell-Weil

En este capítulo se muestran herramientas que permiten estudiar en ciertos casos el grupo de Mordell-Weil de una curva elíptica. La existencia de puntos racionales en una curva elíptica está relacionada con la existencia de puntos racionales en ciertas curvas auxiliares llamadas espacios homogéneos. Después nos enfocaremos a describir los grupos de la forma $E(K)/mE(K)$, donde E es una curva elíptica y $mE(K)$ es la imagen de la isogenia

$$[m] : E(K) \to E(K).$$

Estos últimos también son de gran utilidad para calcular el grupo de Mordell-Weil de las curvas elípticas. Sabemos que $E[m]$ es finito, así que para una extensión finita $K/\mathbb{Q}$ podemos suponer que $E[m] \subseteq E(K)$, lo cual haremos durante este capítulo.

6.1 Espacios Homogéneos

En ocasiones será conveniente usar curvas auxiliares para atacar nuestro problema de calcular el grupo de Mordell-Weill. Primero estudiaremos un poco las clases de curvas isomorfas bajo cierto campo.

6.1.1 Clases de Isomorfismo de Curvas

Definición. Sea C/K una curva proyectiva no singular. Denotamos por $Isom(C)$ al grupo de isomorfismos de C en sí misma definidos sobre $\overline{K}$. Denotaremos por $Isom_K(C)$ al subgrupo de $Isom(C)$ que consiste en los isomorfismos definidos sobre K.

Cabe recordar que en el caso de una curva elíptica E/K, no es lo mismo $Isom(E)$ que $Aut(E)$ ya que tenemos tomar en cuenta la diferencia entre isogenia e isomorfismo.

Definición. Un *doblez* de una curva no singular C/K es otra curva C'/K isomorfa a la primera sobre $\overline{K}$. Denotamos con $Twist(C/K)$ al conjunto de curvas isomorfas a C/K sobre K.

6.1.2 Espacios Homogéneos de Curvas Elípticas

Los espacios homogéneos de una curva elíptica E/K son curvas sobre las cuales el grupo de Mordell-Weill actúa.

Definición. Sea E/K una curva elíptica. Un *espacio homogéneo* para E es una curva suave C/K con una acción transitiva del grupo E en esta curva, es decir, existe un morfismo

$$\mu : C \times E \longrightarrow C$$

definido sobre K con las siguientes propiedades:

1. $\mu(p, O) = p$ para todo $p \in C$.
2. $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ para todos $p \in C$ y $P, Q \in E$.
3. Para cuales quiera $p, q \in C$ existe un único $P \in E$ tal que $\mu(p, P) = q$.

Podemos usar una notación más cómoda si escribimos $p + P$ en lugar de $\mu(p, P)$ y además usando el inciso (3) de la definición anterior denotamos por $p - q$ al único punto $P \in E$ tal que $\mu(p, P) = q$.

6.1. Lema. *Sea C/K un espacio homogéneo para una curva elíptica E/K. Entonces para todos los pares de puntos $p, q \in C$ y $P, Q \in E$ se cumplen:*

1. $p + O = p \;\; y \;\; p - p = O$.
2. $p + (q - p) = q \;\; y \;\; (p + P) - p = P$.
3. $(q + Q) - (p + P) = (q - p) + (Q - P)$.

Estos espacios homogéneos son en particular dobleces de la curva elíptica como lo indica la siguiente proposición.

6.2. Proposición. *Sea E/K una curva elíptica y C/K un espacio homogéneo para E/K. Dado un punto $p_0 \in C$, definimos la función*

$$\theta : E \longrightarrow C \qquad \theta(P) = p_0 + P.$$

1. *θ es un isomorfismo definido en $K(p_0)$.*
2. *Para cuales quiera $p \in C$ y $P \in E$,*

$$p + P = \theta(\theta^{-1}(p) + P).$$

3. *Para todos $p, q \in C$,*

$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

4. *La función diferencia*

$$\nu : C \times C \longrightarrow E \qquad \nu(q, p) = q - p$$

es un morfismo definido en K.

6.1.3 El Grupo de Weill-Chatelet

Nos interesará también tomar en cuenta los espacios homogéneos bajo isomorfismo, lo que nos conduce a la siguiente definición.

Definición. Dos espacios homogéneos C/K y C'/K para E/K son *equivalentes* si existe un isomorfismo $\theta : C \longrightarrow C'$ definido sobre K compatible con la acción de E en C y C'. E actúa en si mismo por translación. La clase de E bajo la equivalencia anterior es la *clase trivial.*

Las clases de equivalencia de la relación anterior forman un grupo.

Definición. El grupo de clases de esta relación es el grupo de *Weill-Chatelet para* E/K, y se denota con $WC(E/K)$.

Podemos ahora caracterizar la clase trivial.

6.3. Proposición. *Sea* C/K *un espacio homogéneo para* E/K. *Entonces* C/K *está en la clase trivial si, y sólo si* $C(K) \neq \emptyset$.

6.4. Teorema. *Sea* E/K *una curva elíptica. Existe una biyección natural*

$$WC(E/K) \to H^1(G_{K/K}, E)$$

donde si C/K *es un espacio homogéneo, escogemos entonces cualquier punto* $p_0 \in C$ *y asignamos*

$$\{C/K\} \to \{\sigma \to p_0^\sigma - p_0\}.$$

El siguiente teorema se puede escribir también para curvas de genero mayor, aún que en ese caso la demostración es sumamente más complicada.

6.5. Teorema. *Sea* C/K *un espacio homogéneo para* E/K. *Escogiendo un punto* $p_0 \in C$ *y considerando la función*

$$sum : Div^0(C) \longrightarrow E$$
$$\sum \eta_i(p_i) \to \sum [\eta_i](p_i - p_0).$$

Tenemos entonces que se cumplen:

1. *Existe una sucesión exacta corta*

$$1 \to \overline{K}^* \to \overline{K}(C)^* \to Div^0(C) \to E \to 0.$$

2. *La función sum no depende de la eleción de* p_0.
3. *La función sum conmuta con la acción de* $G_{\bar{K}/K}$ *sobre* $Div^0(C)$ *y* E.
4. *La función sum define los siguientes isomorfismos*

$$Pic^0(C) \to E,$$
$$Pic^0_K(C) \to E(K)$$

6.2 Cálculos de Grupos de Mordell-Weil

Una estrategia para calcular el grupo de Mordell-Weil consiste en estudiar el grupo

$$E'(K)/\phi(E(K)),$$

donde $\phi : E \longrightarrow E'$ es una isogenia entre curvas elípticas.

Descenso Via 2-Isogenia

6.6. Proposición. *Sean E/K y E'/K dos curva elípticas definidas por las ecuaciones*

$$E : y^2 = x^3 + ax^2 + bx, \qquad E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X;$$

y sea

$$\phi : E \longrightarrow E' \qquad \phi(x, y) = (y^2/x^2, y(b - x^2)/x^2)$$

la isogenia de grado 2 y nucleo $E[\phi] = \{O, (0,0)\}$. Sea

$$S = M_K^{\infty} \cup \{v_p | p \text{ divide } 2b(a^2 - 4b)\}.$$

Entonces existe una sucesión exacta

$$0 \to E'(K)/\phi(E(K)) \to K(S,2) \to WC(E/K)[\phi]$$

$$O \to 1$$

$$(0,0) \to a^2 - ab$$
$$d \to \{c_d/K\}$$

$$(X, Y) \to X$$

donde C_d/K es el espacio homogeneo para E/K definido por la ecuación

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

Entonces el grupo de Selmer es

$$S^{(\phi)}(E/K) \cong \{d \in K(S,2) | C_d(K_v) \neq \emptyset \text{ para todo } v \in S\}$$

Y por último la función

$$\psi : C_d \longrightarrow E' \qquad \psi(z, w) = (d/z^2, dw/z^3)$$

cumple que si $P \in C_d(K)$, entonces

$$\delta(\psi(P)) \equiv d \ (mod\ K^{*2}).$$

6.2.1 Dobleces en Curvas Elípticas

Empezaremos por describir el grupo de isomorfismos de una curva elíptica E/K.

6.7. Proposición. *La función*

$$E \times Aut(E) \to Isom(E)$$

$$(P, \alpha) \to \tau_P \circ \alpha$$

es una biyección entre conjuntos. Ésta define $Isom(E)$ con el producto de E y $Aut(E)$ como

$$(P, \alpha)(Q, \beta) = (P + \alpha Q, \alpha \circ \beta).$$

6.8. Proposición. *Sea E/K una curva elíptica.*

1. *Sea $C/K \in Twist((E,O)/K)$. Entonces $C/K \neq \emptyset$, y por lo tanto C/K puede darnos la estructura de grupo de alguna curva elíptica sobre K.*
2. *Conversamente, si E'/K es una curva elíptica isomorfa a E sobre $\bar{K}$, entonces E'/K representa a un elemento de $Twist((E,O)/K)$.*

6.9. Proposición. *Suponiendo que $char(K) \neq 2, 3$. Sea*

1. *$n(j) = 2$ si $j(E) \neq 0, 1728$,*
2. *$n(j) = 4$ si $j(E) = 1728$,*
3. *$n(j) = 6$ si $j(E) = 0$.*

Entonces $Twist((E,O)/K)$ es canónicamente isomorfo a $K^*/K^{*n(j)}$. Más precisamente, si

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

es una ecuación de Weierstrass para E/K, y sea $D \in K^*$. Entonces la curva elíptica $E_D \in Twist((E;O)/K)$ correspondiente a D (mod $K^{*n(j)}$) tiene las siguiente ecuación de Weierstrass

1. *$E_D : y^2 = x^3 + D^2Ax + D^3B$ si $j(E) \neq 0, 1728$,*
2. *$E_D : y^2 = x^3 + DAx$ si $j(E) = 1728$,*
3. *$E_D : y^2 = x^3 + DB$ si $j(E) = 0$.*

6.10. Corolario. *Si definimos la relación de equivalencia $\sim$ en $K \times K^*$ de la forma*

$$(j, D) \sim (j', D')$$

si $j = j'$ y además $D/D' \in (K^*)^{n(j)}$. Las clases de K-ismorfismos de curvas elípticas E/K están en correspondencia biunívoca con los elementos de

$$K \times K^*/\sim .$$

6.2.2 Resultados

La versión débil del teorema de Mordell-Weill para el caso de los números racionales indica que si $E/\mathbb{Q}$ es una curva elíptica, entonces el grupo $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. A través del algoritmo de descenso es posible probar a partir de este resultado que $E(\mathbb{Q})$ es finitamente generado. Uno de los casos particulares de las curvas elípticas E/K es cuando tienen $j(E) = 1728$. Estas curvas son todas isomorfas entre sí en $\bar{K}$, sin embargo esto no implica que lo sean en K.

Una de estas curvas está dada por la ecuación

$$y^2 = x^3 + x;$$

y de las proposiciones 6.8 y 6.9 podemos escribir cada una de estas curvas con la ecuación

$$E : y^2 = x^3 + Dx,$$

donde D es un representante de algún elemento de $\mathbb{Q}^*/\mathbb{Q}^{*4}$. De esta forma se puede determinar unívocamente cada una de estas curvas si suponemos que D es un entero libre de potencias cuartas. Se puede observar que

$$\Delta(E) = -64D^3,$$

por lo que E tiene buena reducción en todos los primos que no dividan a $2D$.

6.2.3 Curvas de la forma $Y^2 = X^3 + DX$

6.11. Proposición. *Para cada primo p, sea E_p como en la proposición anterior, y sea $\phi : E_p \longrightarrow E'_p$ la isogenia de grado 2 con nucleo $E_p[\phi] = \{O, (0,0)\}$, dada por $\phi(x,y) = (y^2/x^2, y(D-x^2)/x^2)$.*

1. $E_{D\ tor}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{si } D = 4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si } -D \text{ es un cuadrado perfecto,} \\ \mathbb{Z}/2\mathbb{Z} & \text{en otro caso.} \end{cases}$
2. $rank\ E_D(\mathbb{Q}) \leq 2v(2D) - 1.$

Demostración. 1. Como D es libre de potencias cuartas y $\Delta(D) = -64D^3$, tenemos que E tiene buena reducción para todos los primos que no dividan $2D$. Si p es uno de estos primos y consideramos la reducción $\tilde{E}$ sobre el campo $\mathbb{F}_p$, entonces, como lo indica el teorema 4.8, $\tilde{E}$ es supersingular si, y sólo si el coeficiente de x^{p-1} en $(x^3 + Dx)^{p-1/2}$ es cero. Para el caso $p \equiv 3\ (mod\ 4)$, $\tilde{E}/\mathbb{F}_p$ es supersingular; y por la proposición 4.10 concluimos que

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 \text{ para todo } p \equiv 3\ (mod\ 4).$$

Si usamos la proposición 4.2 podemos ver que si $p \neq 2$ y E tiene buena reducción módulo p, entonces $E_{tor}(\mathbb{Q})$ se inyecta en la reducción $\tilde{E}(\mathbb{F}_p)$. Tenemos entonces que $\#E_{tor}(\mathbb{Q})$ divide a $p + 1$ para todos excepto un número finito de números primos $p \equiv 3\ (mod\ 4)$, y en particular divide a 4. Como

$\{O,(0,0)\} \subset E(\mathbb{Q})[2]$ tenemos que las únicas posibilidades para este grupo son $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ y $\mathbb{Z}/4\mathbb{Z}$.

Podemos ver que $E[2] \subset E(\mathbb{Q})$ si, y sólo si el polinomio $x^3 + Dx$ se descompone completamente en $\mathbb{Q}$, es decir, si, y sólo si $-D$ es cuadrado perfecto. Si $-D$ no es cuadrado perfecto, $E(\mathbb{Q})[2]$ tiene orden cuatro si, y sólo si $(0,0) \in 2E(\mathbb{Q})$. Podemos concluir entonces que

$$(0,0) = [2](D^{1/2}, (4D^3)^{1/4}).$$

Asumiendo que D es libre de potencias cuartas, tenemos que

$$E_{tor}(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \text{ si, y sólo si } D = 4.$$

2. Consideremos la curva dada por

$$E' : Y^2 = X^3 - 4DX$$

y la isogenia entre estas curvas

$$\phi : E \longrightarrow E' \qquad \phi(x,y) = \left(y^2/x^2, y(D-x^2)/x^2\right).$$

Sea $S \subset M_{\mathbf{Q}}$ el conjunto con ∞ y las valuaciones con primos que dividan a $2D$, y para cada $d \in \mathbb{Q}$, el correspondiente espacio homogéneo $C_d/\mathbb{Q} \in WC(E/\mathbb{Q})$ dado por la ecuación

$$C_d : dW^2 = d^2 - DZ^4.$$

De la misma forma, usando la isogenia dual $\widehat{\phi} : E' \longrightarrow E$ tenemos el espacio homogéneo dentro de $WC(E'/\mathbb{Q})$ definido por

$$C'_d : dW^2 = d^2 + DZ^4$$

(se observa que se puede cambiar libremente $\mathbf{Z}$ por $\mathbf{Z}/2$ en las condiciones de 6.6).

Sea $v(2D)$ el número de primos que dividen $2D$, Como $\mathbb{Q}$ está generado por -1 y los primos que dividen $2D$, tenemos

$$\dim_2 \ E(\mathbb{Q})/2E(\mathbb{Q}) \leq 2 + 2v(2D) - \dim_2 \ E'(\mathbb{Q})[\hat{\phi}] + \dim_2 \ \phi(E(\mathbb{Q})[2])$$

donde $\dim_2$ es la dimensión como espacio vectorial sobre $\mathbf{F}_2$. Tenemos dos casos

1. Caso $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Aquí, $\phi(E(\mathbb{Q})[2]) \cong 0$ y

$$\dim_2 \ E(\mathbb{Q})/2E(\mathbb{Q}) = rank E(\mathbb{Q}) + 1.$$

2. Caso $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Tenemos ahora $\phi(E(\mathbb{Q})[2]) \cong \mathbf{Z}/2\mathbf{Z}$ y

$$\dim_2 \ E(\mathbb{Q})/2E(Q) = rank E(\mathbb{Q}) + 2.$$

Claramente $E'(\mathbb{Q})[\hat{\phi}] \cong \mathbb{Z}/2\mathbb{Z}$. De lo último tenemos

$$rank\ E(\mathbb{Q}) \leq 2v(2D).$$

En el caso de que $d \leq 0$ teremos que $C_d(\mathbb{R}) = \emptyset$ o $C'_d(\mathbb{R}) = \emptyset$, por lo cual podemos usar 6.6 para reducir nuestra cota en al menos uno,

$$rank\ E(\mathbb{Q}) \leq 2v(2D) - 1.$$

□

Para el caso $D = p$ impar tenemos el siguiente resultado, su demostración se encuentra en [Sil86].

6.12. Proposición. *Para cada primo p, sea E_p como en la proposición anterior, y sea $\phi : E_p \longrightarrow E'_p$ la isogenia de grado 2 con núcleo $E_p[\phi] = \{O, (0,0)\}$, dada por*

$$\phi(x,y) = (y^2/x^2, y(D-x^2)/x^2).$$

1. $E_{p\ tor}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.
2. $S^{(\hat{\phi})}(E'_p/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.
3. $S^{(\phi)}(E_p/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & si\ p \equiv 7,11\ (mod\ 16) \\ (\mathbb{Z}/2\mathbb{Z})^2 & si\ p \equiv 3,5,13,15\ (mod\ 16) \\ (\mathbb{Z}/2\mathbb{Z})^3 & si\ p \equiv 1,9\ (mod\ 16). \end{cases}$

6.3 Algoritmo de Desenso Para Calcular $E(K)$

A continuación se menciona un algoritmo que nos permite estudiar el grupo de Mordell-Weil de una curva elíptica dada. Éste se basa en propiedades de los dobleces y de campos locales. La demostración de este resultado se encuentra en [Sil86].

6.13. Proposición. *Sea E/K una curva elíptica dada por una ecuación de Weierstrass*

$$y^2 = (x-e_1)(x-e_2)(x-e_3), \qquad donde\ e_1, e_2, e_3 \in K.$$

Sea $S \subset M_K$ el conjunto de valuaciones que comprende las arquimedianas, las valuaciones pares y las valuaciones para las cuales E tiene mala reducción. Sea también

$$K(S,2) = \{b \in K^*/K^{*2} \mid ord_v(b) \equiv 0\,(mod 2)\ para\ v \notin S\}.$$

Existe un homomorfismo inyectivo

$$E(K)/2E(K) \to K(S,2) \times K(S,2)$$

dado por

$$P=(x,y)=\begin{cases}.(x-e_1,x-e_2) & \text{si } x\neq e_1,e_2\\ \left(\dfrac{e_1-e_3}{(e_1-e_2}},e_1-e_2\right) & \text{si } x=e_1\\ \left(e_2-e_1,\dfrac{e_2-e_3}{(e_2-e_1)}\right) & \text{si } x=e_2\\ (1,1) & \text{si } x=\infty, \text{ es decir, } P=O.\end{cases}$$

Sea $(b_1,b_2)\in K(S,2)\times K(S,2)$ *fuera de la imagen de los puntos* O, $(e_1,0)$ *y* $(e_2,0)$. *Entonces* (b_1,b_2) *es la imagen de un punto* $P=(x,y)\in E(K)/2E(K)$ *si, y sólo si las ecuaciones*

$$\begin{aligned} b_1z_1^2-b_2z_2^2 &= e_2-e_1\\ b_1z_2^2-b_1b_2z_3^2 &= e_3-e_1\end{aligned}$$

tienen una solución $(z_1,z_2,z_3)\in K^*\times K^*\times K$; *si esta solución existe, entonces podemos tomar*

$$P=(x,y)=(b_1z_1^2+e_1,b_1b_2z_1z_2z_2).$$

Para ejemplificar como funciona este último resultado veamos el siguiente ejemplo.

6.14. Ejemplo. Consideremos la siguiente curva elíptica:

$$E: y^2=x(x-2)(x-10).$$

Esta ecuación tiene discriminante $\Delta=2^{14}5^2$, por lo que tiene mala reducción en 2 y 5. Si reducimos la ecuación módulo 3, entonces tenemos que $\#\widetilde{E}(\mathbb{F}_3)=4$. Además usando que $E[2]\subset E_{tor}(\mathbb{Q})$ y que $E_{tor}(\mathbb{Q})$ se inyecta en $\widetilde{E}(\mathbb{F}_3)$, podemos ver que $E_{tor}(\mathbb{Q})=E[2]$. Lo cual implica que

$$E_{tor}(\mathbb{Q})\cong\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}.$$

En este caso tenemos $S=\{2,5,\infty\}\subset M_{\mathbb{Q}}$ (ver proposición 6.13), por lo que un conjunto completo de representantes de $\mathbb{Q}(S,2)$ está dado por

$$\{\pm1,\pm2,\pm5,\pm10\},$$

el cual podemos identificar con $\mathbb{Q}(S,2)$ (de esta forma tenemos 64 casos por revisar). Si usamos ahora la proposición 6.13, tenemos entonces

$$O\longmapsto(1,1)\quad(0,0)\longmapsto(5,-2)\quad(2,0)\longmapsto(2,-1)\quad(10,0)\longmapsto(10,2).$$

Basta con saber para cuáles pares (b_1,b_2) las ecuaciones

$$b_1z_1^2-b_2z_2^2=e_2-e_1 \tag{6.1}$$

$$b_1z_2^2-b_1b_2z_3^2=e_3-e_1 \tag{6.2}$$

tiene una solución con $z_1,z_2,z_3\in\mathbb{Q}$. Para esto hay que dividir en casos y analizarlos por separado.

1. Si $b_1 < 0$ y $b_2 > 0$, entonces la ecuación 6.1 no tiene soluciones en $\mathbb{R}$, con lo que hemos eliminado 16 casos.
2. Si $b_1 < 0$ y $b_2 < 0$, entonces la ecuación 6.2 no tiene solución en $\mathbb{R}$, con lo que eliminamos otros 16 casos.
3. La imagen de puntos de $E(\mathbb{Q})_{tor}$ es $\{(1,1),(5,-2),(2,-1),(10,2)\}$.
4. Para la pareja $(b_1,b_2) = (1,-1)$ basta con inspeccionar las ecuaciones para ver que $(1,1,3)$ es solución de 6.1 y de 6.2, lo cual corresponde al punto $(1,-3) \in E(\mathbb{Q})$.
5. Si sumamos el punto $(1,-3)$ con los puntos no triviales de $E(\mathbb{Q})_{tor}$ obtenemos los nuevos puntos $(20,60)$, $(18,-48)$ y $(10/9,-80/27)$ dentro de $E(\mathbb{Q})$.
6. Si $b_1 \not\equiv 0 (\text{mod } 5)$ y $b_2 \equiv 0 (\text{mod } 5)$, entonces la ecuación 6.1 implica que z_1 y z_2 son enteros en $\mathbb{Q}_5$. De la ecuación 6.2 obtenemos que $z \equiv 0 (\text{mod } 5)$, y de nuevo por 6.1 tendríamos que $0 \equiv 2 (\text{mod } 5)$. Por lo tanto no hay solución en $\mathbb{Q}_5$ y por ende tampoco en $\mathbb{Q}$. Con lo encontramos ocho nuevos casos para (b_1,b_2) en los que no hay puntos en $E(\mathbb{Q})$:

$$\{(1,\pm 5),(1,\pm 10),(2,\pm 5),(2,\pm 10)\}.$$

7. Si multiplicamos los puntos del inciso anterior por la pareja $(5,2)$,entonces obtenemos otros ocho pares que no son imagen de puntos de $E(\mathbb{Q})$.
8. Para $(b_1,b_2) = (1,2)$: Las ecuaciones son

$$\begin{aligned} z_1^2 - 2z_2^2 &= 2 \\ z_2^2 - 2z_3^2 &= 10 \end{aligned}$$

   Como 2 no es un residuo cuadrático módulo 5, entonces 6.2 implica que $z_1 \equiv z_3 \equiv 0 (\text{mod } 5)$. Pero esta misma ecuación implica $0 \equiv 10 (\text{mod } 25)$, por lo cual no has solución en $\mathbb{Q}_5$.
9. Tomando el par del inciso anterior y multiplicandolo por los siete puntos no triviales de los incisos 3, 4 y 5 obtenemos siete nuevos pares que no son imagen de ningún punto de $E(\mathbb{Q})$. Con lo que hemos completado todos los casos.

De todo lo anterior podemos afirmar que

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Capítulo 7

Curvas Elípticas de Rango Mayor

En este capítulo enfocaremos nuestra atención al grupo $E(\mathbb{Q})$ de una curva elíptica $E/\mathbb{Q}$. Sabemos este grupo es finitamente generado, es decir,

$$E(\mathbb{Q}) \simeq Tor \times \mathbf{Z}^r$$

donde r es lo que llamamos el rango de la curva.

Calcular el rango de una curva elíptica es un problema bastante difícil. Se conjetura que puede haber curvas elípticas con cualquier rango, o en su defecto que este no está acotado. El uso de superficies elípticas para el estudio de estas curvas se ha convertido en una herramienta útil para construir curvas de rango mayor.

En 1986 Thomas J. Kretschmer ([Kre86]) publica un artículo en el que da un algoritmo para construir curvas elípticas con rango grande, en particular muestra una curva elíptica de rango exactamente igual a 10. En este artículo presenta la siguiente tabla que nos muestra como había avanzado este problema hasta ese momento.

1948	Wiman	$r \geq 4$	[Wim48]
1974	Penney, Pomerance	$r \geq 6$	[DEP74]
1975	Penney, Pomerance	$r \geq 7$	[DP75]
1977	Grunewald, Zimmert	$r \geq 8$	[FJG77]
1977	Brumer, Kramer	$r \geq 9$	[AB77]
1979	Nakata	$r \geq 9$	[Nak79]
1982	Mestre	$r \geq 12$	[Mes82]

En 1991 Jean-Francois Mestre publica un artículo donde estudia curvas elípticas definidas sobre el campo $\mathbb{Q}(t)$ de rango mayor o igual a 11 ([Mes91a]). En este mismo año publica otro artículo donde muestra que las curvas encontradas en el anterior tienen rango mayor o igual a 12 ([Mes91b]). Estos resultados son de gran importancia ya que se ocupan dichas curvas como superficies

elípticas que parametrizan familias de curvas elípticas sobre $\mathbb{Q}$ con las que posteriormente se pueden construir curvas con rango mayor. En este capítulo primero se revisa con cuidado este primer artículo y después se muestra como a partir de él se ha avanzado en el problema hasta llegar a una curva de rango mayor o igual a 23.

7.1 Las Construcciones de J. F. Mestre

En esta sección se discute la forma en que Mestre construye curvas elípticas sobre $\mathbb{Q}(t)$ de rango mayor o igual a once ([Mes91a]).

7.1.1 Curvas Elípticas de Rango ≥ 11 sobre $\mathbb{Q}(t)$

Primero veamos un resultado en forma general que Mestre usa sólo en dos casos particulares en su artículo.

7.1. Proposición. *Sea p un número primo y f un polinomio mónico de grado np en $K[X]$. Entonces existe un único polinomio mónico $g \in K[X]$ de grado n tal que el grado de $f - g^p$ es menor que $n(p-1)$.*

Demostración. Sea

$$f(X) = \sum_{i=0}^{np} a_i X^{np-i}$$

con $a_0 = 1$. El problema se reduce en encontrar condiciones en un polinomio

$$g(X) = \sum_{j=0}^{n} b_j X^{n-j}$$

para que el grado de $f - g^p$ sea menor a $n(p-1)+r$, con $0 \leq r \leq n$. El caso más simple es $r = n$, donde una condición necesaria y suficiente para que $f - g^p$ tenga grado menor que np es tomar $b_0 = a_0 = 1$.

Por Θ_k se denotará cualquier expresión polinomial de grado a lo más k. De esta forma se pueden escribir las siguientes igualdades:

$$\begin{aligned} g(X) &= X^n + b_1 X^{n-1} + \ldots + b_r X^{n-r} + \Theta_{n-(r+1)}, \\ g(X)^p &= \sum_{l=0}^{p} \binom{p}{l} (X^n + b_1 X^{n-1} + \ldots + b_r X^{n-r})^{p-l} \Theta^l_{n-(r+1)}. \end{aligned}$$

El grado de

$$(X^n + b_1 X^{n-1} + \ldots + b_r X^{n-r})^{p-l} \Theta^l_{n-(r+1)}$$

es a lo más $np - l(r+1)$, por lo tanto para $l > 0$ el grado de este producto es menor que $np - r$, por lo que los términos de grado mayor o igual que $np - r$ en $g(X)^p$ y en $(X^n + b_1 X^{n-1} + \ldots + b_r X^{n-r})^p$ coinciden.

Por otro lado se tiene

$$(X^n + ... + b_r X^{n-r})^p = X^{np} + pb_1 X^{np-1} + (pb_2 + \binom{p}{2} b_1^2) X^{np-2} + \\ ... + (pb_r + A_r(b_1, ..., b_{r-1})) X^{np-r} + \Theta_{np-(r+1)},$$

donde A_r es un polinomio en las variables $b_1, ..., b_{r-1}$. Sean

$$\begin{aligned} a_1 &= pb_1 \\ a_2 &= pb_2 + \binom{p}{2} b_1^2 \\ &\vdots \\ a_r &= pb_r + A_r(b_1, ..., b_{r-1}) \end{aligned}$$

donde se puede escribir

$$b_i = \frac{a_i - A_i(b_1, ...b_{i-1})}{p}.$$

De esta forma se puede entonces llegar al caso $i = n$, donde g queda completamente determinado. □

Nos interesará el siguiente caso particular.

7.2. Corolario. *Sea K un campo de característica distinta de tres y f un polinomio de grado doce en $K[X]$. Entonces existe una única terna (g, r_1, r_2) de polinomios en $K[X]$ tal que $f = g^3 + r_1 g + r_2$, donde el grado de g es cuatro y los grados de r_1 y r_2 son menores o iguales a tres.*

Demostración. Se usa la proposición anterior con $n = 4, p = 3$ y el algoritmo de la división para $f - g^3$ entre g, donde r_1 es el cociente y r_2 el residuo. □

Sean f, g, r_1, y r_2 como en el corolario anterior. Consideremos ahora la curva plana C definida por la ecuación

$$y^3 + r_1(x)y + r_2(x) = 0.$$

Esta curva contiene los puntos $P_i = (x_i, g(x_i))$, donde x_i son las doce raíces del polinomio f. Si el grado de r_1 es menor que tres, entonces la curva C es una cúbica. La idea de Mestre consiste en tomar $K = \mathbb{Q}(t)$ y escoger un polinomio p tal que:

1. El grado de r_1 sea menor o igual a dos.
2. C sea una curva elíptica sobre K .
3. Los puntos P_i, $i = 1, ..., 12$ sean linealmente independientes en $Pic\ C$.
4. Las raíces de p estén en K.

Encontrando dicho polinomio y tomando P_{12} como el neutro del grupo de Mordel-Weil de C, entonces este grupo (C, P_{12}) es de rango mayor o igual a once.

Sean $Z = (z_1, ..., z_{12})$ y $p = \prod_{i=1}^{12} (X - z_i)$. Si $s(Z) \in Q[z_1, ..., z_{12}]$ es el coeficiente de grado tres del polinomio $r_1(X)$ (o el coeficiente de grado 7 en $r_1(X)g(X)$) obtenido de p como en el corolario 7.2, entonces por ser p homogéneo en las variables $X, z_1, ..., z_{12}$ y ser $r_1(X)g(X)$ un polinomio homogéneo de grado 7 en X, se tiene que $s(Z)$ es un polinomio simétrico homogéneo de grado cinco en las variables $z_1, ..., z_{12}$.

7.3. Lema. *De acuerdo a lo anterior se tiene:*

a) Si $U = (u, ..., u)$, *entonces* $s(Z + U) = s(Z)$.

b) Si p *es el cubo de un polinomio, entonces* $s(Z) = 0$.

c) Si p *es un polinomio par, entonces* $s(Z) = 0$.

Demostración. a) Tenemos $p(X) = g(X)^3 + r_1(X)g(X) + r_2(X)$. Para calcular $s(Z + U)$ fijémonos en

$$\prod (X - (z_i + u)) = p(X - u) = g(X - u)^3 + r_1(X - u)g(X - u) + r_2(X - u).$$

Sustituyendo $Y = X - u$ en lo anterior tenemos

$$p(Y) = g(Y)^3 + r_1(Y)g(Y) + r_2(Y),$$

donde el coeficiente de grado 3 de $r_1(Y)$ es el mismo que el de $r_1(X)$, es decir $s(Z) = s(Z + U)$. b) Si p es un cubo perfecto, entonces $r_1 = r_2 = 0$. c) Y si $p(X)$ es par, entonces todos sus términos de grado impar son cero. Así se puede pensar a $p(X)$ como un polinomio de grado seis en la variable X^2 por lo que el polinomio $g(X)$ es un polinomio de grado 2 en la variable X^2 (ver proposición 7.1),así que $g(X)$ es par. De este modo el coeficiente de grado 7 de $g(X)^3$ es cero y por lo tanto también el de $r_1(X)g(X)$. □

7.4. Lema. *Sean* a, b, c, d *ideterminadas. Entonces el punto*

$$V = (a, b, c, d, a, b, c, d, a, b, c, d)$$

es un punto doble de la variedad S *definida por la ecuación* $s(Z) = 0$ *en el espacio afín de dimensión igual a 12.*

Demostración. Para $Z = V$ se tiene que p es un cubo perfecto y por el lema anterior se deduce que V es un punto de S. Para ver que es un punto doble nos fijaremos en la derivada parcial $\frac{\partial s}{\partial z_1}$, para las demás derivadas parciales la situación es análoga. Sea $p_\varepsilon = p(a+\varepsilon, b, c, d, a, b, c, d, a, b, c, d)$, basta con probar que el coeficiente principal del polinomio r_1 asignado a p_ε es divisible entre ε^2 dentro de $Q[a, b, c, d, \varepsilon][X]$.

Se puede escribir

$$\begin{aligned} p_\varepsilon &= (X-a-\varepsilon)(X-a)^2(X-b)^3(X-c)^3(X-d)^3 \\ &= (1-\varepsilon/(X-a))(X-a)^3(X-b)^3(X-c)^3(X-d)^3 \end{aligned}$$

y usando la expansión de Taylor alrededor de $\varepsilon = 0$ se tiene

$$\sqrt[3]{p_\varepsilon} = (X-a)(X-b)(X-c)(X-d) + \frac{\varepsilon}{3}(X-b)(X-c)(X-d) + \frac{\varepsilon^2}{X-a}\Theta,$$

donde Θ es un polinomio en $\mathbb{Q}[a,b,c,d,\varepsilon,X][[\frac{1}{X-a}]]$. Es fácil ver que los términos que determinan los coeficientes de grado mayor o igual a 8 de p_ε son los que no tienen a $\frac{\varepsilon^2}{X-a}$ como factor, por lo que

$$g = (X-a)(X-b)(X-c)(X-d) + \frac{\varepsilon}{3}(X-b)(X-c)(X-d).$$

Así tenemos $\sqrt[3]{p_\varepsilon} \equiv g \ mod\ \varepsilon^2$ dentro del anillo $Q[a,b,c,d,\varepsilon,X][[\frac{1}{X-a}]]$ y por lo tanto tenemos $p_\varepsilon \equiv g^3 \ mod\ \varepsilon^2$. Con esto se prueba que ε^2 divide a $r_1 g + r_2$ y por ser g mónico tenemos que ε^2 divide al coeficiente principal de r_1. □

7.5. Lema. *Sean a,b,c,d,t cinco indeterminadas. Si definimos*

$$V = (a,b,c,d,a,b,c,d,a,b,c,d) \qquad y \qquad W = (d,d,d,c,c,c,b,b,b,a,a,a),$$

entonces $s(V+tW) = 0$.

Demostración. Los coeficientes de p, pensado como polinomio en X, son polinomios en t con sus coeficientes en $\mathbb{Q}[a,b,c,d]$. Usando que los coeficientes de $p(Z)$ son homogéneos y simétricos en las variables $z_1,\ldots,z_{12}$, es fácil ver que en estos los coeficientes de los términos de máximo grado y los de grado cero coinciden para $Z = V + tW$. Más aún, si el grado de uno estos polinomios es n, entonces los coeficientes de grado r coinciden con los coeficientes de grado $n-r$ (los coeficientes de los polinomios s, g, r_1 y r_2 cumplen también con esta propiedad, lo cual será útil posteriormente). De esto y el lema anterior tenemos que $s(V+tW)$ se puede escribir de la forma $t^2 s_1$, donde s_1 es un polinomio en t de grado a lo más uno.

Probaremos que $s_1 = 0$, para esto basta encontrar dos valores distintos de t que anulen a s_1, es decir dos raíces de un polinomio de grado uno para que éste sea cero y así $s(V+tW) = 0$. Si $t = -1$, entonces p es par y por el lema 7.3 se tiene $s(V+tW) = 0$. Si $t = 1$ podemos usar $u = -(a+b+c+d)/2$ como en el lema 7.3, de modo que $s(V+tW) = s(V+tW+U)$, pero para $Z = V+tW+U$ se tiene de nuevo que p es par. □

Los resultados anteriores se pueden resumir en el siguiente lema.

7.6. Lema. *Sean a, b, c, d cuatro indeterminadas y p el polinomio cuyas raíces x_i son las coordenadas del vector*

$$t(d,d,d,c,c,c,b,b,b,a,a,a) + (a,b,c,d,a,b,c,d,a,b,c,d).$$

Si g, r_1 y r_2 son los polinomios asociados a p del corolario 7.2, entonces el polinomio r_1 es de grado menor o igual a dos y la cúbica

$$y^3 - r_1(x)y + r_2(x) = 0$$

contiene a los doce puntos $P_i = (x_i, g(x_i))$, $i = 1, ..., 12$.

Con todo lo anterior basta encontrar valores adecuados para a, b, c, d de modo que la curva C no sea singular, los puntos P_i sean linealmente independientes y el invariante modular de C sea una función racional no constante.

Construcción de la curva

Ahora es posible la construcción de la curva deseada, para esto asignamos a a, b, c, d los valores -1, 0, 2, 11. Con esto se obtiene la siguiente ecuación para definir C :

$$z^3 + a_1x^2z + a_2xz + a_3z + a_4x^3 + a_5x^2 + a_6x + a_7 = 0,$$

donde

$$\begin{aligned}
a_1 &= -26940t^2 + 51220t - 26940,\\
a_2 &= -1320t^3 + 17280t^2 + 17280t - 1320,\\
a_3 &= -18876t^4 - 153828t^3 + 301221t^2 - 153828t - 18876,\\
a_4 &= -1489600t^3 + 1489600t^2 + 1489600t - 1489600,\\
a_5 &= 5816880t^4 + 8043880t^3 - 27463500t^2 + 8043880t + 5816880,\\
a_6 &= 3416160t^5 - 24166320t^4 + 19202040t^3 + 19202040t^2 - 24166320t + 3416160,\\
a_7 &= -745360t^6 - 15468024t^5 + 18853764t^4 - 138394t^3 + 18853764t^2 - 15468024t - 745360.
\end{aligned}$$

En donde las coordenadas de los puntos P_i están dadas por

$$P_1 = (11t - 1, -1584t^2 + 1826t - 240), \quad P_2 = (11t, -396t^2 + 73t + 154),$$

$$P_3 = (11t + 2, 1980t^2 - 1399t - 414), \quad P_4 = (2t + 11, -414t^2 - 1399t + 1980),$$

$$P_5 = (2t - 1, 234t^2 - 487t + 84), \quad P_6 = (2t, 180t^2 - 134t - 44),$$

$$P_7 = (2, -44t^2 - 134t + 180), \quad P_8 = (11, 154t^2 + 73t - 396),$$

$$P_9 = (-1, -110t^2 + 121t + 156), \quad P_{10} = (-t, 156t^2 + 121t - 110),$$

$$P_{11} = (-t + 2,84t^2 - 487t + 234), \quad P_{12} = (-t + 11, -240t^2 + 1826t - 1584).$$

Tomando a P_{12} como el neutro del grupo y a través de la forma bilineal de Neron-Tate se puede calcular la matriz de alturas de estos puntos que tiene determinante igual a $2^{12}3^4$ (para ver ésto Mestre usa las fórmulas del Teorema 5.20 mencinando que $\chi = 3$) lo cual prueba la independencia de los puntos anteriores.

Un método alterno

De la misma forma que el método anterior pero tomando $p = g^2 - r$, donde g es un polinomio mónico de grado 6 y r de grado menor o igual a 5, se tiene que si r es de grado 4, entonces la curva $y^2 = r(x)$ es de género uno y los doce puntos de la forma $P_i = (x_i, g(x_i))$ pertenecen a la curva, aquí x_i representan las raíces de p.

Buscando ahora que p sea de la forma $q(x - t)q(x + t)$, con

$$q(x) = \prod_{i=1}^{6}(x - a_i),$$

y que r tenga grado menor o igual a cuatro, se encuentran, usando métodos semejantes a los de la construcción anterior, valores para los a_i con los cuales

$$q(x) = (x + 17)(x + 16)(x - 10)(x - 11)(x - 14)(x - 17)$$

sirve para nuestro propósito. De esta forma se llega a la curva definida por:

$$\begin{aligned} y^2 \;=\; & (429t^2 + 53260)x^4 - (5434t^2 + 1239000)x^3 + (-3432t^4 - 2451t^2 + 1222156)x^2 \\ & +(21736t^4 - 3637984t^2 + 134780352)x + 6864t^6 - 1074992t^4 \\ & +53200096t^2 - 758849264 \end{aligned}$$

(ver página 27).

En este caso los doce puntos son:

$P_1 = (-2t + 10, -138t^2 - 258t + 2184)$ $\quad P_2 = (-2t + 11, 346t^2 - 2998t - 1512)$
$P_3 = (-2t - 17, 1578t^2 + 22902t + 88536)$ $\quad P_4 = (-2t - 16, -1490t^2 - 22394t - 77220)$
$P_5 = (-2t + 14, 710t^2 - 6734t + 3720)$ $\quad P_6 = (-2t + 17, -1006t^2 + 9472t - 15708)$
$P_7 = (2t + 17, 1006t^2 + 9472t + 15708)$ $\quad P_8 = (2t + 14, -710t^2 - 6734t - 3720)$
$P_9 = (2t - 16, 1490t^2 - 22394t + 77220)$ $\quad P_{10} = (2t - 17, -1578t^2 + 22902t - 88536)$
$P_{11} = (2t + 11, -346t^2 - 2998t - 1512)$ $\quad P_{12} = (2t + 10, 138t^2 - 258t - 2184)$

Aquí también se toma el punto P_{12} como el neutro, en este caso el determinante de la matriz de alturas es igual a 8100 por lo que los puntos son independientes.

En [Mes91b] Mestre muestra como estas curvas son de rango mayor o igual a doce y para casi todos los valores asignados a t se obtienen curvas elípticas de rango mayor o igual a doce, es decir toda una familia de curvas elípticas.

7.2 Curvas elípticas sobre $\mathbb{Q}$

Usando curvas elípticas de rango mayor sobre $\mathbb{Q}(t)$ se construyen curvas de rango mayor sobre los número racionales. A continuación se presenta el avance en la construcción de curvas elípticas de rango mayor utilizando este método.

1992	J. -P. Mestre	$r \geq 15$	[Mes92]
1992	K. Nagao	$r \geq 17$	[Nag92]
1992	S. Fermigier	$r \geq 19$	[Fer92]
1993	K. Nagao	$r \geq 20$	[Nag93]
1994	K. Nagao, T. Couya	$r \geq 21$	[Nag94]

Existen resultados que aún no se han publicado, sin embargo pueden encontrarse en paginas electrónicas.

1996	S. Fermigier	$r \geqslant 22$
1998	R. Martin, W. McMillen	$r \geqslant 23$

7.2.1 Construcción de Mestre

Usando la superficie elíptica que se generó en 7.1.1, Mestre construyó una curva elíptica de rango al menos 15 ([Mes92]). Tomemos

$$t = \frac{3z^2 - 478z + 1287}{z^2 - 429}$$

con $z = 77$. Ésto nos da como resultado la curva elíptica cuya ecuación de Weierstrass está dada por:

$$\begin{aligned} y^2 + xy &= x^3 - 209811944511283096494755399948 5x \\ &\quad +2665399255159028620601003590596090945994289 7. \end{aligned}$$

En esta curva se encontraron los siguientes puntos linealmente independi-

entes

$$
\begin{aligned}
P_1 &= (501737473225534, -6905875723539454906517)\\
P_2 &= (506962472826784, -7112110805804266149017)\\
P_3 &= (723528240924034, -1592517472019040741 6017)\\
P_4 &= (812523671448034, -1981415333131936676 4017)\\
P_5 &= (-177569372855966, 763618035004620421 1983)\\
P_6 &= (-419463909011966, 639201619397055285 5983)\\
P_7 &= (-499080158224466, -2656234672725490419017)\\
P_8 &= (-489670250151966, -3461360602620746284017)\\
P_9 &= (-161285098583966, -7503202055979337116017)\\
P_{10} &= (576026995032034, 9845125145592749267983)\\
P_{11} &= (569204876688994, 9573248090546012288143)\\
P_{12} &= (437566790688034, 4315766925018741755983)\\
P_{13} &= (383738756328034, 1627462454566927475983)\\
P_{14} &= (380556863867362, 1386435548400000375823)\\
P_{15} &= (373690874760034, 6581768811763422119 83).
\end{aligned}
$$

7.2.2 Construcciones de Fermigier

En 1992 Stéfane Fermingier publica el artículo donde muestra una curva elíptica de rango mayor o igual a 19. En el mismo artículo menciona resultados de Nagao y de Tunnel en el mismo año.

Abril de 1992	Tunnel	$r \geq 17$
Mayo de 1992	Nagao	$r \geq 18$

Curva elíptica de grado $\geqslant 19$

Usando el método que muestra Mestre en [Mes91a] se trabaja con una curva elíptica sobre $Q(t)$ que se obtiene a partir de un polinomio de la forma $p(x) = q(x-t)q(x+t)$, donde $q(x) = \prod_{i=1}^{6}(x-a_i)$. Este polinomio se descompone de la forma $p = g^2 - r$, en donde se busca que el polinomio r sea de grado menor o igual a cuatro para poder definir la cuártica, que a su vez es una curva elíptica, con la ecuación

$$y^2 = r(x).$$

Para la construcción de esta curva Fermigier toma los siguientes valores:

$$\begin{aligned} a_1 &= -36 \\ a_2 &= -25 \\ a_3 &= -18 \\ a_4 &= 13 \\ a_5 &= 31 \\ a_6 &= 38 \end{aligned}$$

De esta forma tiene construida una curva elíptica sobre $Q(t)$. Si se usa $t = 979/87$ se tiene entonces una curva definida por

$$\begin{aligned} y^2 = {} & 22913923/2523x^4 - 231116966/2523x^3 + 107277707205691/19096587x^2 \\ & -163923859763944/19096587x + 1303700052367898928/144542067003 \end{aligned}$$

que tiene como forma mínima de Weierstrass

$$\begin{aligned} y^2 + xy - y = {} & x^3 + x^2 - 2063758701246626370773726978x \\ & +3283864779330613307510374708583380911488 1. \end{aligned}$$

Los 19 puntos independientes son:

$$\begin{aligned} P_1 &= (-30987785091199, 258909576181697016447) \\ P_2 &= (-2888951703967, 261435145473088184895) \\ P_3 &= (-71487320458034575/7921, 158780942822372481126851794 3/704969) \\ P_4 &= (-5811612460699807/2401, 228795661808340252722389 59/117649) \\ P_5 &= (13824498650633, 83368523386975203271) \\ P_6 &= (761787717625797737/51529, -872181661081924408957800795/11697083) \\ P_7 &= (-6768903225745, -215633697068279328993) \\ P_8 &= (-26753594302623, -262493028566521557409) \\ P_9 &= (-43702888408807, -198899103401955431409) \\ P_{10} &= (-3473544815195797742755/66896041, \\ &\quad -720367355474239205275292698047/547142719339) \\ P_{11} &= (-4844597663662106466271/94965025, \\ &\quad 6772653411890968324173429431214 3/925434168625) \\ P_{12} &= (-50527110390373, 90106963524511847991) \\ P_{13} &= (-45015432587775, 185797905595910416127) \\ P_{14} &= (-385165144189, -183394325158424667243) \\ P_{15} &= (12603290965505, 93970415796904223487) \\ P_{16} &= (-17345672207357056815/421201, \\ &\quad -59881991231482114022330423257/273359449) \\ P_{17} &= (19374570094625, -11265860759711920353) \\ P_{18} &= (-1148870915488663/169, -4740331068046201478248 53/2197) \\ P_{19} &= (-12480355043284 9879/32041, 1158739203591364356910897749/5735339) \end{aligned}$$

Curva elíptica de rango $\geqslant 22$

Con es mismo método que el anterior Fermingier construye en 1996 una curva elíptica de rango mayor o igual a 22. Este resultado no está publicado aún pero se puede encontrar en una página electrónica que Él mismo construyó. La dirección es:

http://www.fermigier.com/fermigier/elliptic.html

La curva elíptica que presenta está definida por la ecuación

$$\begin{aligned} y^2 + xy + y &= x^3 - 940299517776391362903023121165864x \\ &\quad +1070736307071974303342529551544927453465112501136 2 \end{aligned}$$

En este caso los puntos independientes son

$$
\begin{aligned}
P_1 &= (32741153161482344264/3025, -22308967458711097957853216969 7/166375)\\
P_2 &= (215521674613198983365/24649, -68729491550613535542357043789 47/3869893)\\
P_3 &= (637312541911044643/81, -14203561901292968321935640 87/729)\\
P_4 &= (-11906250919327880080/361, -16580788535875788634285886853/6859)\\
P_5 &= (-136152345735493381/4, -14482270545045735913281693/8)\\
P_6 &= (-27830298157016213012252/7134241,\\
&\quad 72099692861364392796183359497454267/19055557711)\\
P_7 &= (4127671322151440, 26261076920456131162916 46)\\
P_8 &= (6175679781777296, 22662543359970331246784 49)\\
P_9 &= (12047255022287093, 10619932365259439209804 77)\\
P_{10} &= (416685837455186583191/32761,\\
&\quad 532126822278670966916031158736 9/5929741)\\
P_{11} &= (1499158131390757671080 24/10220809,\\
&\quad 87043268381086469491776631579171 17/32675926373)\\
P_{12} &= (58759417448623559/4, 20309685531507133986546 57/8)\\
P_{13} &= (237195157887349854919517/16024009,\\
&\quad -11477798111611307979707215505421441/64144108027)\\
P_{14} &= (9568474434078537574436/687241,\\
&\quad 31952055634313568197787427280508 6/569722789)\\
P_{15} &= (1725892668710258675291/177241,\\
&\quad 11737805066346484577096645302503 9/74618461)\\
P_{16} &= (-35277008506980340471/1024, 48766027143946934186731674507/32768)\\
P_{17} &= (-275274276352970566 9/121, 60005322521859823812335856 99/1331)\\
P_{18} &= (-18552633109178014, -46654662158243394367179 66)\\
P_{19} &= (-11325170733869118773764 9969/3304065361,\\
&\quad 31015252789483147082000987237322934173 9/189920981015641)\\
P_{20} &= (-7572001778163591251/729, -86590661426506799357663502953/19683)\\
P_{21} &= (-38052604855403228515221 1/11242609,\\
&\quad 73081235744931307684790623068490233/37696467977)\\
P_{22} &= (-15038894977220215881106 81/42784681,\\
&\quad -16070588517011675015153464092471958 5/279854598421)
\end{aligned}
$$

7.2.3 Construcciones de Nagao

Otro personaje que construye curvas elípticas de rango mayor a partir de superficies es Koh-ichi Nagao, primero una de rango mayor o igual a 17 en 1992,

luego una de rango mayor o igual a 20 en 1993 y junto con Tomonori Kouya construye una de rango mayor o igual a 21 en 1994.

Curva elíptica de rango ≥ 17

En 1992 Nagao presenta los siguientes resultados ([Nag92]). Se considera la curva definida por (9.1), y se buscó en los números de la forma $t = t_1/t_2$, donde (t_1, t_2) recorre todos los enteros coprimos tales que $1 \leq t_1 \leq 1000$ y $1 \leq t_2 \leq 100$. De esta forma se encontró que para $t = 537/71$ y $t = 866/35$ se tiene curvas elípticas de rango mayor o igual a 17.

Para $t = 537/71$ En este caso se tiene la curva definida por la ecuación mínima de Weierstrass

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

con

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 0 \\ a_3 &= 0 \\ a_4 &= -1895782483362476188257825431 \\ a_6 &= 428107465551850284688462121997629913671 45. \end{aligned}$$

En la curva generada por esta ecuación se tienen los siguientes puntos inde-

pendientes

$$
\begin{aligned}
P_1 &= (9529946590244278/81, 8773393179301791329823 49/729)\\
P_2 &= (20121870453749702/169, 269523069343670334044110 17/2197)\\
P_3 &= (832895565844694, -2400533295507442676 4879)\\
P_4 &= (170323128927446, -2158931233727022802795)\\
P_5 &= (2705247588331766/49, -1118970806288804913188 77/343)\\
P_6 &= (42800399533958, -200188548806606122939)\\
P_7 &= (911893195333944758/22801, -6058102971831011894711674 69/3442951)\\
P_8 &= (825902562282742/49, -42873975604122721153117/343)\\
P_9 &= (1381131197535594758/32041, 1163925394071743348949284 359/5735339)\\
P_{10} &= (2321852577604836512 38/4923961,\\
&\quad 2637393845318100394599410665999/10926269459)\\
P_{11} &= (750266915475561127/1444, 1595769831662863516873110 7/54872)\\
P_{12} &= (55048888392278, 324451948662567802901)\\
P_{13} &= (56063905437398, 335773236821174910101)\\
P_{14} &= (222469439971613318/3721, 8588767557139680666757684 1/226981)\\
P_{15} &= (892018268333445638/961, 8415771655744254665321409 71/29791)\\
P_{16} &= (1087869867462051014/29929, -7666820638639021398380612 87/5177717)\\
P_{17} &= (1403950398237398, 52580177817811779812501)
\end{aligned}
$$

Para $t = 866/35$

en este caso tenemos la curva definida por la ecuación mínima de Weierstrass similar a la anterior dada por los coeficientes

$$
\begin{aligned}
a_1 &= 0\\
a_2 &= 1\\
a_3 &= 0\\
a_4 &= -18678018087690013395692891145\\
a_6 &= 96678875493491972147105766840567965108 6763
\end{aligned}
$$

con los siguientes puntos independientes.

$$
\begin{aligned}
P_1 &= (98713239378079331954/12581209, 44155864801840452651790531875/44625548323)\\
P_2 &= (5360438106451911/81, 8324089271233969805 00/729)\\
P_3 &= (13270945713669554/169, 2555271033060881176965/2167)\\
P_4 &= (857729078027047559/10609, 399120995547426717209614 20/1092727)\\
P_5 &= (79430124839906, 14615920705150940175)\\
P_6 &= (4607314783851323, -31259704732574980231 8252)\\
P_7 &= (2573692194283109/4, -12786252251165355001 6935/8)\\
P_8 &= (17056161852252446/49, -20781930058909222955 89500/343)\\
P_9 &= (17056161852252119/52441, -65636603930681139397 6716300/45008989)\\
P_{10} &= (81650469905306, -48961061265151525875)\\
P_{11} &= (14515046737185390509/187489, 13237740834430354843 17172500/81182737)\\
P_{12} &= (95102457210723860443 1/12243001, 52807456328691914144 0933947500/42838260499)\\
P_{13} &= (63250318746985598981/811801, 64026337245755911907 97301500/731432701)\\
P_{14} &= (383087327491229/4, -2199020909677353716955/8)\\
P_{15} &= (1738525538929581791/22201, 93109030339091587402 38180/3307949)\\
P_{16} &= (443811832334711, -8954505736358951228460)\\
P_{17} &= (4025625174011254909/27889, -53246538128436020194 20280500/4657463).
\end{aligned}
$$

Curva elíptica de rango ≥ 20

Usando el mismo método que Mestre en [Mes91a] en el método alterno Nagao construye en [Nag93] una curva elíptica a partir de una cuártica sobre el campo $\mathbb{Q}(t)$. Se usa el polinomio $p(x) = q(x-t)q(x+t)$ donde $q(x) = \prod_{i=1}^{6}(x-a_i)$, en este caso se toman

$$
\begin{aligned}
a_1 &= 95\\
a_2 &= 71\\
a_3 &= 66\\
a_4 &= 58\\
a_5 &= 13\\
a_6 &= 0
\end{aligned}
$$

para obtener una curva elíptica de rango al menos 12 sobre $\mathbb{Q}(t)$. Cuando tomamos $t = 619/195$ o $t = 349/48$ se obtienen curvas elípticas de rango mayor ó igual a 20. En el primer caso se obtiene una curva elíptica con un modelo mínimo de Weierstrass dado por la ecuación

$$
\begin{aligned}
y^2 + xy &= x^3 - 43109298076633367795836209589116 6x\\
&\quad +5156283555366643659035652799871176909391533088196
\end{aligned}
$$

con los siuientes puntos independientes:

$$
\begin{aligned}
P_1 &= (1117677105220842826524/37249,\\
&\quad 3153047947718548901150587231643 4/7189057\\
P_2 &= (38095017214360176, 6634638907482675334232862)\\
P_3 &= (12826315700535974 7/4, 3943883738880797593764991 5/8)\\
P_4 &= (1735413707212417277 64/4489,\\
&\quad 2045813113492578321709774085406/300763)\\
P_5 &= (1140370389786990198798604 44/2903808769,\\
&\quad 109302982665018419697665213569619919108 6/156477543135103)\\
P_6 &= (1025796831966896255655769 80/3236130769,\\
&\quad 889405931520755349254783091883555261398/184093771056103)\\
P_7 &= (5205906656889497350 68/11881,\\
&\quad 10865365165484759274005818215450/1295029)\\
P_8 &= (201537570874848579/4, 8441463032785227366069857 1/8)\\
P_9 &= (8566017671075667672/169, 2340866321116566203164824767 4/2197)\\
P_{10} &= (84810811649507676, 2405469597959670444470536 2)\\
P_{11} &= (-21830796739843140, 2040388505636168283880914)\\
P_{12} &= (-2234086367006310516/121, 3476314228926730107073128678/1331)\\
P_{13} &= (-3988902929131123146014 76/47513449,\\
&\quad 939615725382816974616861962133589434/327510203957)\\
P_{14} &= (-3885037831198474090 0/5041,\\
&\quad 10136471367585467909913817882 54/357911)\\
P_{15} &= (4109615365287428206780 4/58874929,\\
&\quad 7124833440519895938250643194029123 54/451747330217)\\
P_{16} &= (3030869760973710007623516/266375041,\\
&\quad 5708794986061809828924957672204713682/4347507044161)\\
P_{17} &= (5668123803956059068/361, 1030763898473140190428188903 0/6859)\\
P_{18} &= (-580/3610851797274320483 24/267289801,\\
&\quad 9/1827975235853363156896624255334773 8/4369920956549)\\
P_{19} &= (-2563815983991139621336 04/10169721,\\
&\quad 1315536690579965438790878526287 78/32431240269)\\
P_{20} &= (4792288702845019969 56/167281,\\
&\quad 1358883162010987994766160965472 98/68417929)
\end{aligned}
$$

En este mismo artículo se mencionan otras tres curvas elípticas de rango al

menos 19 definidas con los parámetros dado en la siguiente tabla

$a_1 =$	34	34	50
$a_2 =$	31	31	42
$a_3 =$	28	28	37
$a_4 =$	27	27	29
$a_5 =$	1	1	4
$a_6 =$	0	0	0
$t =$	7582/623	6441/59	8429/52

Curva elíptica de rango ≥ 21

En 1994 Nagao publica un artículo junto con Kouya ([Nag94]) en el que presentan una curva elíptica de rango al menos 21. En este caso se usa la misma técnica que en el anterior pero con los valores

$$\begin{aligned} a_1 &= 399 \\ a_2 &= 380 \\ a_2 &= 352 \\ a_4 &= 47 \\ a_5 &= 4 \\ a_6 &= 0 \\ t &= 14721/376 \end{aligned}$$

con los cuales se obtiene la curva elíptica con un modelo mínimo de Weierstrass dado por la ecuación

$$\begin{aligned} y^2 + xy + y \;=\; & x^3 + x^2 - 215843772422443922015199527021598 35x \\ & -19474361277787151947255961435459054151501792241320535 \end{aligned}$$

con los siguientes puntos independientes:

$$
\begin{aligned}
P_1 &= (800843008889340065933/16, 22662214190910903990783584765347/64)\\
P_2 &= (10610541066763914590637/2209, 1087744114825178454840094794778034/103823)\\
P_3 &= (907186946780634143, 728916386168451830641677698)\\
P_4 &= (19683320108556444219408310 7/227919409,\\
&\quad 22778073989304408195874101847939237638 94/3440899317673)\\
P_5 &= (18546347413906465252800007 5/366301321,\\
&\quad 22569985783858324284947383046648197814 6/7010640982619)\\
P_6 &= (-12485261071234691432503/123904,\\
&\quad 15433033534289399822821717527025 39/43614208)\\
P_7 &= (-59703014087684747037/361, 74188124509415406852503612696 2/6859)\\
P_8 &= (-73270463404799613067/361, 86687813785863879389111794348 2/6859)\\
P_9 &= (-360733396398627565, 10698584048409672894788397 4)\\
P_{19} &= (-389445180957906897, 74288355118790673852542098)\\
P_{11} &= (-14744583503498585126654 07/14205361,\\
&\quad 22784934015783680843104090282593326 32/53540005609)\\
P_{12} &= (-11430585603546889269177927 7/278589481,\\
&\quad 16972779768877136292841029639987095378/4649937027371)\\
P_{13} &= (-21972533600828202797/81, 10079078658496350456387600530 2/729)\\
P_{14} &= (-25047938415396324842058977/71216721,\\
&\quad 68347192566984494300752205261293775206 2/600997908519)\\
P_{15} &= (34348280818851183522137152847 07/5137262501809,\\
&\quad 42799124838389250442349391653296975768124338 46/11643877735262694377)\\
P_{16} &= (-227656313261676647, 13366002432726894909529779 8)\\
P_{17} &= (-40980894341059921378352 93/12552849,\\
&\quad 56600884139913517593014036598908897 06/44474744007)\\
P_{18} &= (26578287358691780202126 17/1495729,\\
&\quad 41744997315499971865961317212732013 76/1839376567)\\
P_{19} &= (88396500431424342412499432 3/850947241,\\
&\quad 23250077986002217145041708721276812178/24822/91967211)\\
P_{20} &= (37543938954172817109003/73441,\\
&\quad 12240979159912800999038354900202 98/19902511)\\
P_{21} &= (19165312347502458410162233/17214201,\\
&\quad 75593839815741485450348997055551694952/71421719949)
\end{aligned}
$$

7.2.4 Curva elíptica de rango $\geqslant 23$

El resultado más reciente en la búsqueda de curvas de rango mayor no ha sido publicado aún, sin embargo se puede consultar en la página electrónica

http://www.math.niu.edu/~rusin/known-math/98/hirank

Aquí se presenta una curva de rango al menos 23 y se menciona que fue encontrada por Roland Martin y William McMillen. Está fechado como resultado de 1998 y la curva que se presenta tiene por ecuación

$$\begin{aligned} y2 + xy + y &= x3 - 1925296640867401282806596461641844172 3x \\ &\quad + 3268550072771637625792334707145204429590744305634561400 6 \end{aligned}$$

Los puntos independientes tiene las siguientes coordenadas:

$$\begin{aligned} P1 &= (169021360446217242755846613925 95/119224493521, \\ &\quad -69455519784971993679807552308609739430858248812/41166906143372569) \\ P2 &= (66478822724661038216347720465 71/30891226081, \\ &\quad -17137023844710987140049387309945953892946213544/5429411004770479) \\ P3 &= (12772293320356497066648467275 92/2961427561, \\ &\quad 14433808433392723974587210307423920166963040 46/161157926442059) \\ P4 &= (17548347719164769821320906 51/369369961, \\ &\quad 49412130720987886904443301152758710388796/7098921280459) \\ P5 &= (90274303195370369866709299 8/307406089, \\ &\quad 65384341040093032650247499528307090293 53/5389750958437) \\ P6 &= (10357951013506147653495081 9/45091225, \\ &\quad 23069788336355187008872985450437441454 8/302787575875) \\ P7 &= (31762044569407766003397375255/14054813809, \\ &\quad 14113810892913497531647688085589210029472 04/1666240341498377) \\ P8 &= (29436984213667648723395/17956, \\ &\quad 56573350120462407053573194528022 33/2406104) \end{aligned}$$

$P9 = (1127027270330215920, 3523978127407100674110377602)$

$P10 = (6864642445028218997115 15/139129,$
$-3945636519458824035804688734351058 16/51895117)$

$P11 = (11962675953816366561795/1369,$
$-1167962768316319592876571517317044/50653)$

$P12 = (3052068080540269517575 7355/3345241,$
$-1519151145890614031007596981065323331 12/6118445789)$

$P13 = (1144977553805075601935763531 6/967521025,$
$-1150775031908416918955115365651634494501651/30094741482625)$

$P14 = (4969418243982621661795591770/1285294201,$
$1845694350555353263636697454229180527073 27/46079082400051)$

$P15 = (4804651135376128298407773 15/160801,$
$-1053155064770271481485216922467820744136 8/64481201)$

$P16 = (979071542846797779179825421660 35/57601436172721,$
$964874722537391293613786748114488474882993683572/4371696135204725654 81)$

$P17 = (2499893548263134327189771 95/4397409,$
$3941156276776007263792745630379334937996/9221366673)$

$P18 = (5484007412308650780838813 5/3996001,$
$3874969787906537097210612941192154609 88/7988005999)$

$P19 = (9690141319063801580189469420/87590881,$
$-9531440780799429063609036700365366695935 42/819763055279)$

$P20 = (8821424424066027387538 80/76729,$
$-7753945566808376512921663769887473 4/21253933)$

$P21 = (2812175950395226936581984/24025,$
$4712624271973109965160039085789391367/3723875)$

$P22 = (7126269737101017406079752337071371/2947180538019481,$
$8301545457599868400690020572696822268650535079968 4/$
$1599963631643498413786 21)$

$P23 = (2143448685801212487450/841, 1009984922118966827735475374 8208/24389).$

Bibliografía

[AB77] K. Kramer A. Brumer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743.

[Ahl79] Ahlfors, *Complex analysis*, McGrawn-Hill, N.Y., 1979.

[DEP74] C. Pomerance D. E. Penney, *A serch for elliptic curves with large rank*, Math. Comp. **28** (1974), 851–853.

[DP75] C. Pomerance D.E. Penny, *Three elliptic curves with rank at least seven*, Math. Comp. **29** (1975), 965–968.

[Eis96] D. Eisembud, *Commutative algebra with a view toward algebriac geometry*, 2da. ed., Springer-Verlag, 1996.

[Fer92] S. Fermigier, *Un example de courbe elliptique defini sur Q de rang ≥ 19*, CRAS **315** (1992), 719–722.

[FJG77] R. Zimmert F. J. Grunewald, *Uber einige rationale elliptische kurven mit freiem rang ≥ 8*, J. Reine Angw. Math. **296** (1977), 100–107.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, 1977.

[Kob87] N. Koblitz, *A course of number theory and cryptography*, Springer-Verlag, 1987.

[Kre86] T. J. Kretschmer, *Construction of elliptic curves with large rank*, Mathematics of Computation **46** (1986), 627–635.

[Lan86] S. Lang, *Algebraic number theory*, Springer-Verlag, 1986.

[Len87] H.W. Lenstra, *Factoring integers with elliptic curves*, Annals. of Math. **126** (1987), 649–673.

[Mes82] J. F. Mestre, *Construction dúne courbe elliptique de rang ≥ 12*, C.R. Acad. Sci. Paris **295** (1982), 643–644.

[Mes91a] J. F. Mestre, *Courbes elliptiques de rang ≥ 11 sur $Q(t)$*, C.R. Acad. Sci. Paris **313** (1991), 139–142.

[Mes91b] J. F. Mestre, *Courbes elliptiques de rang ≥ 12 sur Q*, C.R Acad. Sci. Paris **313** (1991), 171–174.

[Mes92] J. F. Mestre, *Un example de courbe elliptique sur Q de rank ≥ 15*, Acad. Sci. Paris **314** (1992), 453–455.

[Mor96] P. Morandi, *Field and galois theory*, Springer-Verlag, 1996.

[Nag92] K. Nagao, *An example of an elliptic curve over Q with rank* $\geq$ 17, Procd. Japan Acad. 68. Ser. A (1992), 287-289.

[Nag93] K. Nagao, *An example of an elliptic curve over Q with rank* $\geq$ 20, Proc, Japan Acad. **69** (1993), 691-693.

[Nag94] N. Kouya K. Nagao, *An example of an elliptic curve over Q with rank* $\geq$ 21, Proc, Japan Acad. **70** (1994), 104-105.

[Nak79] K.Ñakata, *On some elliptic curves defined over Q of free rank* $\geq$ 9, Manuscripta Math. **29** (1979), 183–194.

[Ser76] J. P. Serre, *Local fields*, Springer-Verlag, 1976.

[Shi90] T. Shioda, *On mordell-weil lattices*, Comm. Math. Univ. Sancti Pauli **39** (1990), 211–240.

[Sil86] J. H. Sillverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[Sil92] J. H. Sillverman, *Rational points on elliptic curves*, Springer-Verlag, 1992.

[Sil96] J. H. Sillverman, *Avanced topics in arithmetic of elliptic curves*, Springer-Verlag, 1996.

[Wal90] J.M. Luck P. Moussa M. Waldshmidt, *Number theory and physics*, Springer-Verlag, 1990.

[Wim48] A. Wiman, *Uber rationale punkte auf kurven driftter ordnung vom geschlechte eins*, Acta Math. **80** (1948), 223–257.