UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE MATEMÁTICA

Tesis para Optar el Título Profesional de
Licenciado en Matemática

TÍTULO

EL TEOREMA DE MORDELL Y LOS SUBGRUPOS DE TORSIÓN DE UNA CURVA ELÍPTICA SOBRE EL CUERPO GAUSSIANO

POR

RONALD MAS HUAMÁN

ASESOR

MG. MANUEL TORIBIO CANGANA

LIMA- PERU

2013

Agredecimientos

Mi agradecimiento especial a mi familia, en especial a mi madre María por sus sabios consejos, Liliana por sus constantes motivaciones.

Finalmente, quisiera agradecer al Mg. Manuel Toribio por su paciencia y dedicación en alentarme a mejorar este trabajo.

Ronald Jesús Mas Huaman
UNI, 5 de Setiembre del 2013.

Resumen

En el presente trabajo se ha estudiado las ecuaciones a las que llamaremos *curvas elípticas*, estas son de la forma

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

con $a_1, a_2, a_3, a_4, a_6 \in K$ (cuerpo) y sin puntos singulares, ecuación que también recibe el nombre de *ecuación de Weierstrass*. Trabajando sobre un cuerpo de característica diferente de 2 y 3, dicha ecuación toma la forma reducida

$$y^2 = x^3 + Ax + B \,\text{con}\, A, B \in K.$$

Definiendo la operación de adición de puntos de una curva elíptica, como la reflexión sobre el eje x del punto de intersección que se obtiene al trazar una recta sobre los dos puntos que deseamos adicionar, veremos que el conjunto de puntos $(x, y) \in K \times K$ que cumplan con la ecuación anterior y agregandolé un punto que denotamos por $\mathcal{O}$ posee la estructura de grupo abeliano, la prueba de ello no es complicada de ver, a excepción posiblemente de la asociatividad a la que dedicaremos una sección completa en este trabajo. El espacio proyectivo bidimensional $\mathbb{P}^2_K$ juega un papel importante en el estudio de las curvas elípticas, debido a que existe una identificación entre los puntos del plano afín y los puntos finitos del espacio proyectivo.

Se demuestra que el conjunto de puntos racionales de una curva elíptica $E(\mathbb{Q})$, puede ser generada apartir de rectas tangentes y secantes trazadas desde un conjunto finito de puntos racionales (finitamente generado), esto es conocido como el teorema de Mordell-Weill. Esta prueba se deriva de dos resultados importantes como son probar que $E(\mathbb{Q})/2E(\mathbb{Q})$ sea finito, donde tendremos en cuenta que el polinomio $p(x) = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$ puede ser descompuesto en $\mathbb{Q}$ ó en una extensión finita de $\mathbb{Q}$, a los que hemos denominado *caso particular y caso general del teorema de Mordell-Weill* respectivamente, el otro resultado tiene que ver con el *método del descenso* introducido por Fermat en 1640. El conjunto de puntos racionales puede ser descrito como $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$ donde $E(\mathbb{Q})_{tors}$ es el *subgrupo de torsión* y $\mathbb{Z}^r$ es la *parte libre*.

Para determinar $E(\mathbb{Q})_{tors}$ se utiliza el teorema de Lutz-Nagell, que nos proporciona una lista finita de posibles puntos de torsión, esto será complicado cuando tenemos una lista grande. Felizmente Barry Mazur (1937) consiguió caracterizar todos los subgrupos de torsión de una curva elíptica definida sobre $\mathbb{Q}$. Nuestro interés por determinar los subgrupos de torsión de una curva elíptica nos lleva a la siguiente pregunta ¿ Es posible encontrar un algoritmo similar al de Lutz-Nagell para calcular los subgrupos de torsión de una curva elíptica definida sobre una extensión finita de $\mathbb{Q}$?, esto es sobre $\mathbb{Q}(i)$, es más podrá ser posible encontrar una caracterización definitiva de $E(\mathbb{Q}(i))_{tors}$ (subgrupo de torsión de una curva elíptica sobre el cuerpo gaussiano). La respuesta es sí. En la parte final de este trabajo nos hemos avocado a determinar el subgrupo de torsión de una curva elíptica sobre el cuerpo gaussiano, imitando el teorema de Lutz-Nagell para curvas elípticas definidas sobre $\mathbb{Q}$, al que llamaremos *el teorema de Lutz-Nagell sobre el cuerpo gaussiano*, demostramos que si $(x, y) \in E(\mathbb{Q}(i))_{tors}$ entonces $x, y \in \mathbb{Z}[i]$, además si $y \neq 0$ tenemos que $y^2 \mid 4A^3 + 27B^2$ con $A, B \in \mathbb{Z}[i]$. La caracterización definitiva de $E(\mathbb{Q}(i))_{tors}$ nos lo dará el teorema de Kenku-Momose el cuál afirma que el subgrupo de torsión de una curva elíptica sobre el cuerpo gaussiano es isomorfo a uno de los 26 grupos que mencionaremos en este trabajo. Por otro lado, notemos que si $P \in E(\mathbb{Q})_{tors}$ entonces $P \in E(\mathbb{Q}(i))_{tors}$, por tal motivo podemos ver una curva definida sobre los racionales como si estuviese definida sobre el cuerpo gaussiano. Este estudio lo realizó años más tarde en el 2005, Yasutsugu Fujita (1965) y caracterizó al conjunto $E(\mathbb{Q}(i))_{tors}$ para curvas definidas sobre los racionales como isomorfo a uno de los 20 grupos que detallaremos en la parte final.

Índice general

Introducción

El estudio de las ecuaciones diofánticas tiene una historia estrechamente relacionada a la antigua Grecia, son llamadas así en honor al matemático griego Diofanto de Alejandría (200-290 A.C.) quién dedico su obra Aritmética, a la determinación de soluciones enteras o racionales, de ecuaciones algebraicas. Nuestro trabajo se concentrará en estudiar ecuaciones del tipo

$$y^2 + axy + by + x^3 + cx^2 + dx + e = 0$$

con $a, b, c, d, e \in K$. Estas ecuaciones reciben el nombre de **curvas elípticas**, además si la característica de K no es 2 ni 3, dicha ecuación adopta la forma reducida.

$$y^2 = x^3 + Ax + B \, con \, A, B \in K.$$

En 1922 Louis Mordell (1988-1972) demostró que el conjunto de puntos racionales de una curva elíptica es un grupo abeliano generado por un número finito de puntos racionales, años mas tarde, en 1928 André Weil (1906-1998) generalizó el teorema a todos los cuerpos númericos. Como consecuencia de ello tenemos que todas las soluciones racionales de una curva elíptica se dividen en dos partes, una parte de torsión y una parte libre.

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus Z^r.$$

Nosotros nos enfocaremos en la parte de torsión $E(\mathbb{Q})_{tors}$ el cuál consta de todos los puntos racionales de orden finito. Usando como herramienta principal el teorema dado por E. Lutz y T. Nagell, el cuál es un algoritmo muy simple que nos permite conocer una cantidad finita de los posibles puntos de torsión. Habiendo llegado a este punto uno se hace la siguiente pregunta ¿Será posible de que algunos resultados sean válidos si trabajamos sobre el cuerpo gaussiano?, esto debido a que el cuerpo gaussiano cumple muchas propiedades similares a las del cuerpo de los números racionales, para empezar el anillo de enteros gaussianos es un dominio euclidiano

por ende una dominio de factorización única, también posee una cantidad finita de unidades, es más los primos gaussianos tienen una estrecha relación con los primos enteros. A manera de motivación veamos dos problema que involucren a las curvas elípticas primero sobre el cuerpo de los números racionales y luego sobre el cuerpo gaussiano.

Motivación para estudiar curvas sobre $\mathbb{Q}$

Para que valores enteros positivos de x la siguiente suma es un cuadrado perfecto

$$1^2 + 2^2 + 3^2 + \cdots + x^2$$

Esto equivale a encontrar las soluciones enteras positivas de

$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

Una ecuación de este tipo representa una **curva elíptica**. Para resolver esto usaremos el método de Diofanto el cual consiste en usar los puntos ya conocidos para generar nuevos puntos. Empezaremos con los puntos (0,0) y (1,1). La recta que pasa por esos puntos es $y = x$. Ahora veamos cuales son los puntos de intersección , para eso resolveremos la siguiente ecuación:

$$x^2 = \frac{x(x+1)(2x+1)}{6} = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x.$$

Ordenando la ecuación tenemos

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0.$$

Como nosotros conocemos 2 soluciones: $x = 0$ y $x = 1$. Esto es debido a que las raíces son las primeras coordenadas de los puntos de intersección entre la recta y la curva. Nosotros también podemos conocer la tercera raíz ya que conocemos la suma de raíces de esta ecuación:

$$0 + 1 + x = \frac{3}{2}$$

De aquí $x = 1/2$ y como $y = x$, tenemos que $y = 1/2$. Ahora escojamos un punto (1/2,-1/2) que pertenece a la curva, esto es debido a que la curva es simétrica y repetimos el mismo procedimiento usando los puntos (1/2,-1/2) y (1,1). La recta

que pasa por estos puntos es $y = 3x - 2$ y para hallar los puntos de intersección resolvemos

$$(3x-2)^2 = \frac{x(x+1)(2x+1)}{6}.$$

Ordenando la ecuación tenemos

$$x^3 - \frac{51}{2}x^2 + \ldots = 0$$

De aquí como

$$\frac{1}{2} + 1 + x = \frac{51}{2}$$

Por lo tanto $x = 24$ y como $y = 3x - 2$, tenemos que $y = 70$. Esto significa que

$$1^2 + 2^2 + 3^2 + ... + 24^2 = 70^2$$

Si nosotros repetimos el mismo procedimiento con el punto recién encontrado como uno de nuestros puntos, nosotros encontraremos muchas soluciones racionales, sin embargo esta es la única solución entera aparte de la trivial $x = 1$.

Motivación para estudiar curvas sobre $\mathbb{Q}(i)$

Consideremos la ecuación diofántica

$$v^2 = 2u^4 - 1.$$

Esta ecuación posee como soluciones enteras a $(1, 1)$ y $(13, 239)$, haciendo un cambio de variables

$$x = \frac{2iv - 2}{u^2}\,,\; y = \frac{-4(v+i)}{u^3}$$

esta ecuacion se transforma en una curva elíptica

$$y^2 = x^3 + 8$$

donde las soluciones iniciales $(1, 1)$ y $(13, 239)$ corresponden a los números racionales gaussianos

$$(-2+2i, -4-4i)\,,\; (\frac{2(-1+239i)}{13^2}, (\frac{-4(239+i)}{13^3})$$

.

Capítulo 1

Teoría de cuerpos y teoría de Galois

Los cuerpos son estructuras adecuados para plantear y resolver ecuaciones, debido a sus propiedades de factorización y divisibilidad. Desde la época de los babilonios, los matemáticos intentaban resolver ecuaciones cuadráticas, uno de sus mayores logros fue demostrar que la ecuación

$$x^2 - 2$$

no es soluble en el cuerpo de los racionales, ya que $\sqrt{2}$ no pertenece a los números racionales. Pero lo interesante de esto es que existe un cuerpo en el cuál dicha ecuación se puede resolver, llamado cuerpo de descomposición, por ejemplo, el polinomio $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ tiene como cuerpo de descomposición a $\mathbb{Q}(\sqrt{2})$ (esto quiere decir el menor cuerpo que contiene todas las raíces de $p(x)$).

1.1. Extensiones de cuerpos

Definición 1.1.1. *Decimos que el cuerpo E es una extensión del cuerpo F, si F es un subcuerpo de E.*

Denotaremos como E/F a la extensión E de F.

Definición 1.1.2. *Sea E una extensión del cuerpo F.*

1. *Se dice que E es una extensión finita de F, si E considerado como un espacio vectorial sobre F es de dimensión finita.*

2. *La dimensión del espacio vectorial F sobre E lo denotamos por $[E : F]$ y lo llamaremos grado de extension de E sobre F.*

Ejemplo 1.1.1. Sea $\mathbb{Q}(\sqrt{2})$ extensión del cuerpo $\mathbb{Q}$, como $\mathbb{Q}(\sqrt{2})$ tiene base $\{1, \sqrt{2}\}$ como un $\mathbb{Q}$- espacio vectorial, entonces $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

Teorema 1.1. *Si F es una extensión finita de N y N una extensión finita de M, entonces F es una extensión finita de M y se cumple que*

$$[F : M] = [F : N][N : M]$$

Demostración. Sea $\{u_1, u_2, \dots u_m\}$ una base de F como un N- espacio vectorial y $\{v_1, v_2, \dots v_n\}$ una base de N como un M- espacio vectorial. Afirmamos que

$$\{u_i v_j | i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$$

es una base de F como M- espacio vectorial. Veamos la prueba:
Sea $u \in F$, entonces $u = \sum_{i=1}^{m} \alpha_i u_i$ con $\alpha_i \in N$, pero para cada i, tenemos que $\alpha_i = \sum_{j=1}^{n} \beta_{ij} v_j$, entonces

$$u = \sum_{i=1}^{m} (\sum_{j=1}^{n} \beta_{ij} v_j) u_i = \sum \beta_{ij} (u_i v_j)$$

Ahora mostremos que son linealmente independientes. Supongamos que $\sum \beta_{ij}(u_i v_j) = 0$, entonces $\sum_{i=1}^{m} (\sum_{j=1}^{n} \beta_{ij} v_j) u_i = 0$, como $\{u_i\}$ son linealmente independientes, tenemos que para cada i fijo se cumple $\sum_{i=1}^{n} \beta_{ij} v_j = 0$, como $\{v_j\}$ son linealmente independientes, tenemos $\beta_{ij} = 0$, para cada j, lo cual completaría la prueba. □

Definición 1.1.3. *Sea E una extensión de F y sean M y N subcuerpos de E tales que son extensiones de F, la composición de M y N que denotamos por MN, es el subcuerpo más pequeño de F que contiene a M y N.*

Observaciones:

1. MN es la intersección de todos los subcuerpos de E que contienen a M y N.
2. $MN = \{mn / m \in M, n \in N\}$

Ejemplo 1.1.2. Sea $E = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$, $N = \mathbb{Q}(\sqrt{3})$ entonces $MN = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Una forma de conseguir un cuerpo de extensión es adjuntarle elementos a dicho cuerpo. De ahí la siguiente definición.

Definición 1.1.4. *Sea E una extensión de F y $\{\alpha_i\}_{i\in I}$ un subconjunto de elementos de E. Entonces $F(\{\alpha_i\}_{i\in I})$ es el subcuerpo más pequeño de E que contiene a F y $\{\alpha_i\}_{i\in I}$.*

Observaciones:

1. Si $\{\alpha_i\}_{i\in I} = \{\alpha_1, \ldots, \alpha_n\}$ es finito. Entonces

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n).$$

   Esto nos quiere decir que el orden en que adjuntemos los elementos no interesa.

2. Si $\{\alpha_i\}_{i\in I} = \{\alpha_1, \ldots, \alpha_n\}$. Entonces

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n).$$

Lema 1.1. *Sean E un cuerpo y R un dominio de integridad que es también un espacio vectorial sobre E de dimensión finita entonces R es un cuerpo*

Demostración. Sea $r \in R$ con $r \neq 0$ y $dim_E(R) = m$ definimos el conjunto

$$M = \{r, r^2, \ldots r^n\} \, con \, n > m.$$

Entonces M es un conjunto linealmente dependiente. Si $\sum_{i=0}^{n} c_i r^i = 0$ con $c_i \in E$ entonces existen algunos $c_i \in E$ diferentes de cero. Sea $n_0 \in \mathbb{Z}_{>0}$ el menor de los índices tal que $c_{n_0} \neq 0$ esto quiere decir que $c_{n_0} r^{n_0} + c_{n_0+1} r^{n_0+1} + \ldots c_n r^n = 0$, multiplicando por $c_{n_0}^{-1}$ y como $r^{n_0} \neq 0$ tenemos que

$$1 + c_{n_0^{-1}} c_{n_0+1} r + \ldots c_{n_0^{-1}} c_n r^{n-n_0} = 0.$$

Por lo tanto tomando $r^{-1} = -c_{n_0^{-1}} c_{n_0+1} - \ldots c_{n_0^{-1}} c_n r^{n-n_0-1}$ tenemos la prueba del lema. □

1.2. Extensiones algebraicas

Definición 1.2.1. *Sea E una extensión de F y sea $\alpha \in E$. Decimos que α es algebraico sobre F si existe un polinomio no nulo p en $F[x]$ tal que α es raíz de p. Decimos que E es una extensión algebraica de F ó que la extensión E/F es algebraico, si para todo $\alpha \in E$ es algebraico sobre F.*

Lema 1.2. *Dada la extensión E/F y $\alpha \in E$, son equivalentes:*

1. *α es algebraico sobre F.*

2. *$F(\alpha)/F$ es finito.*

3. *$F(\alpha) = \{f(\alpha)/f \in F[x]\}$.*

Demostración. 1) $\rightarrow$ 2) Como $\alpha \in E$ es algebraico sobre F entonces existe un $f(x) \in F[x]$ irreductible, mónico y de grado mínimo (con $grad(f(x)) = n$), tal que $f(\alpha) = 0$. Afirmó que $\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F. Veamos primero que es linealmente independiente, si $\sum_{i=0}^{n-1} c_i\alpha^i = 0$, $c_i \in F$ y algún $c_i \neq 0$, entonces α sería una raíz del polinomio $g(x) = \sum_{i=0}^{n-1} c_i x^i$ lo cuál contradice la minimalidad de n, por lo tanto es linealmente independiente. Para terminar con la prueba necesitamos mostrar que

$$S = E + E\alpha + E\alpha^2, \ldots E\alpha^{n-1} = E(\alpha)$$

claramente se puede ver que $S \subset E(\alpha)$ para probar la otra inclusión es suficiente mostrar que S es un cuerpo, se puede ver que S es un anillo con identidad, sea $\beta \neq 0 \in S$ entonces $\beta = \sum_{i=0}^{n-1} \lambda_i\alpha^i$, con $\lambda_i \in F$, definamos el polinomio $v(x) = \sum_{i=0}^{n-1} \lambda_i x^i$ que cumple que $v(\alpha) = \beta \neq 0$, como $f(x)$ es irreductible y no divide a $v(x)$ tenemos que $f(x)$ y $v(x)$ son primos entre sí por lo tanto existen $p(x), q(x) \in F[x]$ tal que $p(x)f(x) + q(x)v(x) = 1$, de ahí que $q(\alpha)v(\alpha) = 1$ por lo tanto S es un cuerpo, con lo cuál probaríamos nuestra afirmación.

2) $\rightarrow$ 3) Sabemos que $E[\alpha] \subseteq E(\alpha)$ y como $E(\alpha)/E$ es finito, tenemos que $E[\alpha]$ es un anillo que a la vez también es un espacio vectorial sobre E de dimensión finita y por el lema 1.1 tenemos que $E[\alpha]$ es un cuerpo, por lo tanto $E(\alpha) = \{f(\alpha)/f \in E[x]\}$.

3) $\rightarrow$ 1) Como $\alpha^{-1} \in F(\alpha)$ entonces existe un $f(x) \in F[x]$ tal que $f(\alpha) = 0$, definimos $g(x) = xf(x) - 1$ que cumple $g(\alpha) = 0$, por lo tanto α es algebraico sobre F. □

Definición 1.2.2. *Sea $\alpha \in E$ algebraico sobre F. El único polinomio mónico $g \in F[x]$ generador del ideal $J = \{f \in F[x] : f(\alpha) = 0\}$ de $F[x]$ es llamado el polinomio minimal de α sobre F.*

Teorema 1.2. *Sí $\alpha \in E$ es algebraico sobre F entonces el polinomio minimal g sobre F tiene las siguientes propiedades:*

i) g es irreducible en $F[x]$.

ii) Para $f \in F[x]$ tenemos que: $f(\alpha) = 0$ si y sólo si g divide a f.

iii) g es el polinomio mónico en $F[x]$ de menor grado teniendo a α como raíz.

Demostración. Consultar [9, pág 18] □

Denotaremos al polinomio minimal de α sobre F por $m_\alpha(x)$
Observaciones:

1. $m_\alpha(x)$ depende del cuerpo F.
2. $m_\alpha(x)$ es de grado uno si y sólo si $\alpha \in F$.

Proposición 1.1. *Dada la extensión E/F y $\alpha \in E$ algebraico sobre F. Se cumple:*

1. *Si $grad(m_\alpha(x)) = d$ entonces $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ es una base de $F(\alpha)$ como un espacio vectorial sobre F.*
2. *$[F(\alpha) : F] = grad(m_\alpha(x))$*
3. *Sea $T : F(\alpha) \to F(\alpha)$ definida por $T(\beta) = \alpha\beta$. Entonces T es una transformación lineal de F espacios vectoriales, y su polinomio minimal*

$$m_T(x) = m_\alpha(x).$$

Prueba.-

1. Esto ya se vió en el lema 1.2.
2. Como la base tiene d elementos, entonces $[F(\alpha) : F] = gr(m_\alpha(x))$.
3. $T(\beta_1 + \beta_2) = \alpha(\beta_1 + \beta_2) = \alpha\beta_1 + \alpha\beta_2 = T(\beta_1) + T(\beta_2)$
   $T(c\beta) = \alpha c\beta = cT(\beta)$, con $c \in F$.

□

Corolario 1.1. *Sea $\alpha_1, \ldots, \alpha_n \in E$ con $F(\alpha_i)/F$ finito para cada i. Entonces $F(\alpha_1, \ldots, \alpha_n)/F$ es finito.*

Demostración. Esto se desprende del lema 1.2 e inducción sobre n. □

Corolario 1.2. *Si $E = F(\{\alpha_i\}_{i\in I})$ con cada α_i algebraico sobre F, entonces E/F es algebraico.*

Demostración. Sea $\alpha \in E$, entonces α es una función racional de $\{\alpha_i\}_{i\in I}$, así en particular $\alpha \in F(\alpha_1, \ldots, \alpha_n)$, para algún n, por el corolario 1.1 $F(\alpha_1, \ldots, \alpha_n)$ es finito, así por la parte (1) del lema 1.2 α es algebraico sobre F. Por lo tanto E/F es algebraico. □

Proposición 1.2. *Sea E una extensión algebraica de F y sea M un subcuerpo tal que $F \subseteq M \subseteq E$. Entonces M es una extensión algebraica de F y E es una extensión algebraica de M.*

Demostración. Como E es una extensión algebraica de F, todo elemento de E es algebraico sobre F, y $M \subseteq E$ entonces todo elemento de M es algebraico sobre F por lo tanto M es una extensión algebraica de F. De manera similar sea $\alpha \in E$, entonces α es una raíz de algún polinomio $f(x) \in F[x]$ y $F[x] \subseteq M[x]$, así α es raíz de algún polinomio en $M[x]$ entonces α es algebraico sobre M por lo tanto R es algebraico sobre M. □

Proposición 1.3. *Sea $f(x) \in F[x]$ un polinomio irreductible de grado d entonces $F[x]/\langle f(x)\rangle$ es un cuerpo y un espacio vectorial sobre F de dimensión d.*

Demostración. Empecemos probando que $F[x]/\langle f(x)\rangle$ es un espacio vectorial sobre F de dimensión d. Afirmamos que

$$S = \{\overline{1}, \overline{x}, \ldots, \overline{x}^{d-1}\}$$

es una base de $F[x]/\langle f(x)\rangle$. Veamos que lo genera sea $\overline{g}(x) \in F[x]/\langle f(x)\rangle$ entonces existen $q(x), r(x) \in F[x]$ tales que $g(x) = f(x)q(x) + r(x)$ con $r(x) = 0$ ó $grad(r(x)) < d$ por lo tanto

$$\overline{g}(x) = \overline{r}(x) = \sum_{i=0}^{d-1} c_i \overline{x}^i$$

es una combinación lineal de elementos de S. Ahora veamos que dicho conjunto es linealmente independiente, supongamos que $\sum_{i=0}^{d-1} c_i \overline{x}^i = \overline{h}(x) = 0$ entonces $f(x)|h(x)$ lo cuál es imposible debido a que $grad(h(x)) < grad(f(x))$ por lo tanto

$c_0 = c_1 = \ldots c_{d-1} = 0$. Por otro lado sean $\overline{g}, \overline{h} \in F[x]/\langle f(x)\rangle$ tales que $\overline{g}(x)\overline{h}(x) = 0$, entonces $f(x)$ divide a $g(x)h(x)$ como $f(x) \in F[x]$ es irreductible entonces $f(x)$ divide a $g(x)$ ó divide a $h(x)$ esto quiere decir que $\overline{g}(x) = 0$ ó $\overline{h}(x) = 0$ entonces $F[x]/\langle f(x)\rangle$ es un dominio de integridad que es un espacio vectorial sobre F de dimensión finita, por el lema 1.1 $F[x]/\langle f(x)\rangle$ es un cuerpo. □

Sea $\alpha \in E$ con E/F, definimos un homomorfimo de anillos:

$$\begin{array}{rccc} \varphi: & F[x] & \to & E \\ & f(x) & \to & f(\alpha) \end{array}$$

Lema 1.3. *Sea $\alpha \in E$ un elemento algebraico sobre F. Entonces φ induce*

$$\overline{\varphi} : F[x]/\langle m_\alpha(x)\rangle \to F(\alpha)$$

un isomomorfismo de cuerpos y de F- espacios vectoriales.

Demostración. Sea

$$\begin{array}{rccc} \pi: & F[x] & \to & F[x]/\langle m_\alpha(x)\rangle \\ & f(x) & \to & \overline{f}(x) = f(x) + \langle m_\alpha(x)\rangle \end{array}$$

la proyección canónica. Vamos a probar primero que $\overline{\varphi}$ esta bien definida. Sean $\overline{f}(x), \overline{g}(x) \in F[x]/\langle m_\alpha(x)\rangle$ tales que $\overline{f}(x) = \overline{g}(x)$ entonces $g(x) - f(x)$ es divisible por $m_\alpha(x)$, así $g(x) = f(x) + m_\alpha(x)q(x)$, para algún polinomio $q(x) \in E[x]$, pero $\varphi(g(x)) = g(\alpha) = f(\alpha) + m_\alpha(\alpha)q(\alpha) = f(\alpha) = \varphi(f(x))$, por otro lado como $\overline{f}(x), \overline{g}(x) \in F[x]/\langle m_\alpha(x)\rangle$ entonces existen $f(x), g(x) \in F[x]$ tales que $\overline{f}(x) = \pi(f(x))$ y $\overline{g}(x) = \pi(g(x))$ como $\varphi(f(x)) = \overline{\varphi}(\pi(f(x)))$ tenemos que $\overline{\varphi}(\overline{f}(x)) = \overline{\varphi}(\overline{g}(x))$. Claramente se puede ver que $\overline{\varphi}$ es un homomorfismo de cuerpos y una función de F-espacios vectoriales. Para terminar con la prueba veamos si es biyectiva, sea $\overline{\varphi}(\overline{f}(x)) = 0$, entonces $\overline{\varphi}(\pi(f(x))) = \varphi(f(x)) = 0$, por la definición de φ tenemos que $f(\alpha) = 0$ entonces $f(\alpha) \in \langle m_\alpha(x)\rangle$ de ahí que $\overline{f}(x) = 0$. Por lo tanto es inyectiva, además como $F[x]/\langle m_\alpha(x)\rangle$ y $F(\alpha)$ son F-espacios vectoriales de igual dimensión finita, terminaría la prueba. □

Ejemplo 1.2.1. Sea $i = \sqrt{-1} \in \mathbb{C}$ un elemento algebraico sobre $\mathbb{R}$ entonces

$$\mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1\rangle$$

1.3. Cuerpos de descomposición y extensión de isomorfismos

Definición 1.3.1. *Dado $f \in K[x]$ de grado positivo y F una extensión de K. Decimos que f se descompone en F si f puede ser escrito como un producto de factores lineales en $F[x]$, esto quiere decir si existen $\alpha_1, \alpha_2, ..., \alpha_n \in F$ tal que*

$$f(x) = a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

donde a es el coeficiente principal de f.

El menor cuerpo (en el sentido de inclusión) en el cual f se descompone linealmente se llama cuerpo descomposición de f sobre K y lo denotamos por $K(\alpha_1, \alpha_2, ..., \alpha_n)$.

Teorema 1.3. *Dado $f(x) \in K[x]$ de grado positivo entonces existe una extensión F de K en el cuál $f(x)$ posee una raíz.*

Demostración. Si $f(x)$ se descompone en $K[x]$ no hay nada que probar, supongamos que $f(x)$ es irreductible en $K[x]$. Definimos el anillo cociente

$$F = K[x]/\langle f(x)\rangle$$

por lo visto anteriormente F es un cuerpo con $K \subseteq F$, además $f(x) = 0$ en F por lo tanto x es una raíz de $f(x)$ en F. □

Teorema 1.4. *(Existencia y unicidad del cuerpo de descomposición)*
Si K es un cuerpo y f es un polinomio de grado positivo en $K[x]$, entonces existe un cuerpo de descomposición de f sobre K.

Demostración. Aplicando el principio de inducción sobre $grad(f(x)) = n$. Si $n = 1$ tenemos que $f(x) = ax+b$ con $a, b \in K$ y $a \neq 0$, entonces $f(x) = a(x+a^{-1}b) \in K[x]$, así K es el cuerpo de descomposición de $f(x)$. Supongamos que el teorema se cumple para $n = d - 1$, entonces $f(x) \in K[x]$ es un polinomio con $grad(f(x)) = d - 1$. Sea $f(x) \in F[x]$ de grado d. Entonces por el teorema 1.3, existe una extensión E de F en el cuál $f(x)$ posee una raíz α_1, además $E = F(\alpha_1)$. Entonces $f(x) = (x - \alpha_1)g(x) \in F[x]$. Por inducción $g(x)$ tiene un cuerpo de descomposión de K sobre F. Por lo tanto $g(x) = (x - \alpha_2)\cdots(x - \alpha_d) \in K[x]$ y $f(x) = (x - \alpha_1)\cdots(x - \alpha_d) \in K[x]$ se descompone. Además $K \supseteq F(\alpha_2, \ldots, \alpha_n)$, entonces $K = F(\alpha_2, \ldots, \alpha_n)$, así $K = F(\alpha_1)(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$. Por lo tanto K es un cuerpo de descomposición de $f(x)$. □

Lema 1.4. *Sea $\sigma_0 : E_1 \to E_2$ un isomorfismo de cuerpos. Sea $f_1(x) \in E_1[x]$ irreducible y sea $F_1 = E_1(\beta_1)$ con $f_1(\beta_1) = 0$. Sea $f_2(x) = f_1^{\sigma_0}(x)$ y sea $F_2 = E_2(\beta_2)$ con $f_2(\beta_2) = 0$. Entonces σ_0 se extiende a un único isomorfismo $\sigma : F_1 \to F_2$ con $\sigma(\beta_1) = \beta_2$*

Demostración. Como σ_0 es un isomorfismo tenemos que $f_2(x)$ es irreducible si y sólo si f_1 también lo es. Por el lema 1.4, tenemos el isomorfismo

$$\overline{\varphi}_i : E_i[x]/\langle f_i(x)\rangle \to E_i(\beta_i) = F_i,\ i = 1, 2$$

definiendo $\sigma = \overline{\varphi}_2\sigma_0\overline{\varphi}_1^{-1}$ tenemos la prueba. □

Corolario 1.3. *Sea $f(x) \in E[x]$ irreducible. Supongamos que β_1 y β_2 son raíces de $f(x)$ y sea $F_i = E(\beta_i)$, i=1,2. Entonces existe un único isomorfismo $\sigma : F_1 \to F_2$ con $\sigma|_E = id$ y $\sigma(\beta_1) = \beta_2$. En particular, si $F = E(\beta_1) = E(\beta_2)$, existe un único automorfismo σ de F con $\sigma|E = id$ y $\sigma(\beta_1) = \beta_2$.*

Demostración. Consultar [9, pág 24] □

Lema 1.5. *Sea $\sigma_0 : E_1 \to E_2$ un isomorfismo de cuerpos. Sea $f_1(x) \in E_1[x]$ y sea $f_2(x) = f_1(x)^{\sigma_0} \in E_2[x]$. Sea F_1 el cuerpo de descomposición de $f_1(x)$ y sea F_2 el cuerpo de descomposición de $f_2(x)$. Entonces σ_0 se extiende a un isomorfismo $\sigma : F_1 \to F_2$.*

Demostración. Sea $f_1(x) \in E_1[x]$ irreducible sobre $E[x]$ tal que $f_1(x)$ posee k factores lineales. Definamos $d_F(f_1) = grad(f_1) - k$, procederemos a la prueba por inducción sobre $d_F(f_1)$. Si $d_F(f_1) = 0$, entonces $f_1(x)$ es el producto de factores lineales y $F_1 = E_1$, $F_2 = E_2$, así $\sigma = \sigma_0$.
Si $d_F(f_1) > 0$, entonces $f_1(x)$ tiene un factor irreducible $g_1(x)$ de grado mayor que 1. Sea $\alpha_1 \in F_1$ raíz de $g_1(x)$ y sea $\alpha_2 \in F_2$ raíz de $\sigma_0(g_1(x))$. Entonces $E(\alpha_1) \subseteq F_1$ y $E(\alpha_2) \subseteq F_2$. Por el lema anterior, existe un isomorfismo $\sigma_1 : E(\sigma_1) \to E(\sigma_2)$ tal que $\sigma_1|_E = \sigma_0$ y $\sigma_1(\alpha_1) = \alpha_2$. Sea $K = E[\alpha_1]$ y consideremos que $f_1(x) \in K[x]$. Ahora $g_1(x) \in K[x]$ tiene como factor a $x - \alpha_1$, así $f_1(x)$ tiene a los más $k + 1$ factores irreducibles en $K[x]$, de ahí que $d_K(f_1) < d_F(f_1)$. Como F_1 es el cuerpo de descomposición de $f_1(x) \in E_1[x]$ y $K \subseteq F_1$, entonces F_1 es el cuerpo de descomposición de $f_1(x) \in K[x]$, de manera similar se realiza para F_2, así por inducción σ_1 se extiende a σ. □

1.4. Extensiones normales, separables y de Galois

Definición 1.4.1. *Una extensión algebraica E de F es una* ***extensión normal****, si para todo polinomio irreducible $f(x) \in F[x]$ con $f(\alpha) = 0$, para algún $\alpha \in E$ se descompone en $E[x]$.*

Ejemplo 1.4.1. El cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es una extensión normal, ya que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el cuerpo de descomposición de

$$(x^2 - 2)(x^2 - 3)$$

Definición 1.4.2.

1. *Sea $f(x) \in F[x]$, si lo factores irreducibles de $f(x) \in F[x]$ se descomponen como producto de factores lineales distintos en algún cuerpo de descomposición de $f(x)$, entonces $f(x)$ es un* ***polinomio separable****. De lo contrario decimos que el polinomio es inseparable.*

2. *Sea E una extensión algebraica de F. Entonces $\alpha \in E$ es un* ***elemento separable****, si $m_\alpha(x)$ es un polinomio separable. De lo contrario decimos que α es un elemento inseparable.*

3. *Sea E una extensión algebraica de F. Entonces E es una* ***extensión separable*** *de F, si para todo $\alpha \in E$ es un elemento separable. De lo contrario decimos que E es una extensión inseparable.*

Ejemplo 1.4.2. El cuerpo $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es una extensión separable pero no normal ya que el polinomio irreducible $x^3 - 2 \in \mathbb{Q}[x]$ no se descompone en $\mathbb{Q}(\sqrt[3]{2})$.

Definición 1.4.3. *Sea E una extensión algebraica de F. El grupo de Galois denotado por $Gal(E/F) \subset Aut(E)$ se define como*

$$Gal(E/F) = \{\sigma : E \to E / \, \sigma \, es \; un \; automorfismo \; y \, \sigma|_F = id\}.$$

Lema 1.6. *Sea E una extensión algebraica de F y sea K un cuerpo tal que $F \subseteq K \subseteq E$. Entonces $Gal(E/K)$ es un subgrupo de $Gal(E/F)$.*

Demostración. Definamos el automorfismo $\sigma : E \to E$ con $\sigma|_K = id$ claramente satisface que $\sigma|_F = id$. □

Definición 1.4.4. *Sea G un grupo de automorfismos de un cuerpo E, denotaremos*

$$E^G = \{u \in E \, tal \, que \, \sigma(u) = u, \, para \, todo \, \sigma \in G\}$$

cómo el cuerpo que queda fijo bajo los autormorfismos que pertenecen a G.

Definición 1.4.5. *Sea E una extensión algebraica de F decimos que E es una extensión de Galois de F si $E^{Gal(E/F)} = F$.*

Teorema 1.5. *Sea E/F un extensión las siguientes proposiciones son equivalentes:*

1. *E es el cuerpo de descomposición de un polinomio separable $f \in F[x]$.*
2. *$F = E^G$ para algún grupo finito G de automorfismo de E.*
3. *E es normal y separable y $[E : F] < \infty$.*
4. *E es de Galois sobre F.*

Demostración. Consultar [7,pág 31]. □

1.5. El teorema fundamental de la teoría de Galois

Teorema 1.6. *Sea G un grupo finito de automorfismos de un cuerpo E y sea $F = E^G$, entonces*

$$[E : F] = |G|.$$

Demostración. Empezaremos probando que $[E : F] \leq |G|$. Sea $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ un grupo finito de automorfismos del cuerpo E y sea $\{\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\}$ un conjunto formado por elementos de E linealmente independiente sobre F. Consideremos el siguiente sistema de ecuaciones en E

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_n)x_n &= 0 \\ &\cdots \\ \sigma_m(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_n)x_n &= 0 \end{aligned}$$

como este sistema posee más variables que ecuaciones, entonces este sistema posee soluciones no triviales en E. De todas las soluciones tomemos aquella que posee la menor cantidad de elementos diferentes de cero, supongamos que $c_1, \ldots, c_s, 0, \ldots, 0$ sea dicha solución. Veamos que $s > 1$, ya que si $s = 1$ tendríamos que $c_1\sigma_1(\alpha_1) = c_1\alpha_1 = 0$ de ahí que $c_1 = 0$. Entonces podríamos asumir que $c_s = 1$ (si fuese necesario multiplicamos por c_s^{-1} a la solución y hacemos un cambio de variable). Finalmente veamos que no todos los $\{c_i\}_{i=1}^s$ estan en F ya que si fuese así tendríamos que

$c_1\sigma_1(\alpha_1) + \cdots + c_s\sigma_1(\alpha_s) = c_1\alpha_1 + \cdots + c_s\alpha_s = 0$ entonces $\{\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\}$ sería linealmente dependiente. Por lo tanto podemos asumir que $c_1 \notin F$, entonces

$$c_1\sigma_i(\alpha_1) + \cdots + c_{s-1}\sigma_i(\alpha_{s-1}) + \sigma_i(\alpha_s) = 0, i = 1, \ldots, n. \tag{1.1}$$

Como $c_1 \notin F$, existe un $\sigma_k \in G$ tal que $\sigma_k(c_1) \neq c_1$. Como G es un grupo, sabemos que para todo $\sigma_i \in F$ existe un $\sigma_j \in G$ tal que $\sigma_i = \sigma_k\sigma_j$. Entonces aplicando σ_k a la ecuación 1.1 tenemos que

$$\sigma_k(c_1)\sigma_i(\alpha_1) + \cdots + \sigma_k(c_{s-1})\sigma_i(\alpha_{s-1}) + \sigma_i(\alpha_s) = 0, i = 1, \ldots, n. \tag{1.2}$$

Restando (1.2) - (1.1) tenemos que

$$(c_1 - \sigma_k(c_1))\sigma_i(\alpha_1) + \cdots + (c_{s-1} - \sigma_k(c_{s-1}))\sigma_i(\alpha_{s-1}) = 0, i = 1, \ldots, n.$$

con $i = 1, \ldots, n$. Como $c_1 - \sigma_k(c_1) \neq 0$, entonces sería una solución con menor cantidad de elementos diferentes de cero que s lo cuál sería una contradicción. Por lo tanto $[E : F] \leq |G|$. La prueba de que $[E : F] \geq |G|$ se deja como ejercicio para el lector. □

Corolario 1.4. *1. Sea G un grupo finito de automorfismo de E y $F = E^G$ entonces todo automorfismo de E que deja fijo F pertenece a G.*

2. Sean G_1, G_2 grupos finito de automorfismos distintos de F y sean $F_1 = E^{G_1}$, $F_2 = E^{G_2}$, entonces F_1 y F_2 son distintos

Demostración. 1. Por el teorema anterior sabemos que $[E : F] = |G| = n$, supongamos que existe un $\sigma \in Aut(E)$ que deja fijo a F pero que no pertenece a G, entonces F sería un cuerpo fijo por algún grupo de autormorfismos que tenga por lo menos $n + 1$ elementos; lo cuál sería una contradicción debido a que $n + 1 > [E : F]$.

2. Supongamos que $F_1 = F_2$, entonces F_1 queda fijo por G_2, entonces $G_2 \subseteq G_1$, de igual manera aplicando la misma idea para F_2 llegamos a la prueba.

□

Lema 1.7. *Sea G un grupo de automorfismos de E que dejan fijo F y sea H un subgrupo de G con $M = E^H$ entonces para todo $\sigma \in G$ tenemos que $\sigma(M) = E^{\sigma H \sigma^{-1}}$.*

Demostración. Sea $u \in M$ y $\tau \in H$, entonces $\sigma\tau\sigma^{-1}(\sigma(u)) = \sigma\tau(u) = \sigma(u)$, así $\sigma(M) \subseteq E^{\sigma H\sigma^{-1}}$. Por otro lado si $\sigma\tau\sigma^{-1}(u') = u'$ para algún $u' \in E$ y para todo $\tau \in H$, entonces $\tau\sigma^{-1}(u') = \sigma^{-1}(u')$, así $\sigma^{-1}(u') = u \in E^H = M$ y $u' = \sigma(u)$, así $E^{\sigma H\sigma^{-1}} \subseteq \sigma(M)$. □

Teorema 1.7. *(Teorema fundamental de la Teoría de Galois)*
Sea E una extensión finita de Galois de F y sea $G = Gal(E/F)$.

1. *Existe una biyección uno a uno entre los cuerpos intermedios $F \subseteq M \subseteq E$ y los subgrupos $\{1\} \subseteq G_M \subseteq G$ dado por $M = E^G$.*

2. *H es normal en G si y sólo si E^H es normal sobre F, de ahí que*

$$Gal(E^H/F) \cong G/H.$$

3. *$H_1 \supset H_2$ si y sólo si $E^{H_1} \subset E^{H_2}$.*

4. *Si $H_1 \supset H_2$ entonces $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$.*

Demostración. El teorema también es conocido como el teorema de correspondencia de la Teoría de Galois, veamos la prueba.

1. Definamos

$$\varphi : \{subgrupos\, de\, G\} \to \{cuerpos\, intermedios\, entre\, F\, y\, E\}.$$

   Veamos que es biyectiva, si $H_1 \neq H_2$ entonces $E^{H_1} \neq E^{H_2}$ por la parte (2) del corolario anterior φ es inyectiva. Por otro lado sea $F \subseteq M \subseteq E$ y definamos

$$H = \{\sigma \in G |\, \sigma(u) = u,\, u \in M\} = Gal(E/M) \subseteq Gal(E/F).$$

   Por lo tanto la extensión E/F es de Galois por el teorema 1.5, pero $F \subseteq M$ así $f(x) \in M[x]$. Entonces $f(x)$ es el cuerpo de descomposición de el polinomio separable $f(x) \in M(x)$, así la extensión E/M es de Galois por el teorema 1.5. Por lo tanto $M = E^{Gal(E/M)} = E^H$. Por lo tanto φ es uno a uno ya que si $\varphi^{-1}(M) = G_M$, entonces $M = E^{G_M}$.

2. $\Rightarrow$)Sea H un subgrupo normal de G y sea $M = E^H$ entonces para todo $\sigma \in Gal(E/F)$, por el lema 1.7 tenemos que

$$\sigma(M) = E^{\sigma H\sigma^{-1}} = E^H = M.$$

   Definamos la función

$$\begin{array}{rccc} \varphi: & Gal(E/F) & \to & Gal(M/F) \\ & \sigma & \to & \sigma|B \end{array}$$

por la definición el $Nu(\varphi) = \{\sigma \in G | \, \sigma|M = id\} = G_M$, por lo tanto $Im(\varphi) \cong Gal(E/F)/Nu(\varphi) = G/G_M$. Por otro lado sea $\sigma_0 \in Gal(M/F)$, entonces $\sigma_0 : M \to M$ se extiende a $\sigma : E \to E$ por el lema 1.5 y $\sigma|F = id$, así $\sigma \in Gal(E/F)$. Entonces $\varphi(\sigma) = \sigma_0$, así $\varphi : Gal(E/F) \to Gal(M/F)$ es sobreyectiva, por lo tanto $Gal(M/F) \cong G/G_M$.
$\Leftarrow$) Si M/F es una extensión normal por el teorema 1.5 tenemos que M es el cuerpo de descomposición de un polinomio separable $f(x) \in F[x]$, supongamos que $u_1, \ldots, u_r \in M$ son las raíces de dicho polinomio, entonces $M = F(u_1, \ldots, u_r)$, cómo $\sigma(f(x)) = f(x)$ para todo $\sigma \in G = Gal(E/F)$ y σ permuta las raíces de $f(x)$ tenemos que para todo i existe un j tal que $\sigma(u_i) = u_j$ con $1 \leq i, j \leq r$, de ahí que $\sigma(M) = M$, por el lema 1.7 tenemos que $E^{G_M} = M = \sigma(M) = E^{\sigma G_M \sigma^{-1}}$ entonces $G_M = \sigma G_M \sigma^{-1}$ por la parte 1). Por lo tanto G_M es un subgrupo normal de G.

3. $\Rightarrow$) Si $H_1 \supset H_2$ entonces $E^{H_1} \subset E^{H_2}$. $\Leftarrow$) Si $E^{H_1} \subset E^{H_2}$ entonces $Gal(E/E^{H_1}) \supset Gal(E/E^{H_2})$, pero $Gal(E/E^{H_i}) = H_i$ con $i = 1, 2$.

4. Si $H_2 = \{id\}$, cómo el cuerpo E es de Galois sobre E^{H_1} por el teorema 1.5 E es el cuerpo de descomposición de un polinomio separable y por el teorema 1.6 $[E : E^{H_1}] = Gal(E/E^{H_1})$. Si $H_2 \neq \{id\}$ tenemos que $(H_1 : 1) = (H_1 : H_2)(H_2 : 1)$ por lo tanto

$$[E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}].$$

□

Ejemplo 1.5.1. Sea $F = \mathbb{Q}$ y consideremos el polinomio $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. El cuerpo de descomposición de este polinomio es

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \, | \, a, b, c, d \in \mathbb{Q}\}.$$

Cómo f posee 4 raíces distintas en E entonces $[E : F] = 4 = |G|$ y además sabemos que cada $\sigma \in G$ permuta las raíces $\{\pm\sqrt{2}, \pm\sqrt{3}\}$ tenemos que

$$G = Gal(E/F) = \{\sigma_1 = id, \sigma_2, \sigma_3, \sigma_4\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

donde

$$\begin{aligned}
\sigma_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6},\\
\sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}\\
\sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}\\
\sigma_4(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}
\end{aligned}$$

Los cuerpos intermedios entre E y F son aquellos cuerpos que contienen a F y están contenidos en E, estos son:

$$M_1 = F,\ M_2 = \mathbb{Q}(\sqrt{2}),\ M_3 = \mathbb{Q}(\sqrt{3}),\ M_4 = \mathbb{Q}(\sqrt{6}),\ M_5 = E.$$

Por otro lado los subgrupos H de G son

$$H_1 = G,\ H_2 = \{id, \sigma_3,\ H_3 = \{id, \sigma_2,\ H_4 = \{id, \sigma_4,\ H_5 = \{id\}\}.$$

Donde existe una correspondencia uno a uno entre los $\{H_i\}$ y $\{M_i\}$ con $i = 1, 2, \ldots, 5.$ dado por

$$M_i = E^{H_i}\, con\, i = 1, 2, \ldots, 5.$$

Podemos observar además que $|Gal(M_i/F)| = [M_i : F]$ con $i = 1, 2, \ldots, 5.$

Capítulo 2

Teoría básica de una curva elíptica

El estudio de las curvas elípticas han sido de gran interés debido a sus diversas aplicaciones matemáticas como la criptografía, en este capítulo veremos que una curva elíptica posee la estructura de un grupo abeliano con cierta operación que la llamaremos adición.

2.1. Ecuación de Weierstrass

Definición 2.1.1. *Una curva elíptica E sobre el cuerpo K esta definida por la ecuación*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

con $a_1, a_2, a_3, a_4, a_6 \in K$ y $\Delta \neq 0$, donde Δ es la discriminante de E y esta definida por

$$\begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 &= a_1^2 + a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1a_6^2 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

Observaciones:

1. La ecuación (2.1) es conocida como la ecuación de Weierstrass.
2. Decimos que la curva elíptica esta definida sobre K, debido a que $a_1, a_2, a_3, a_4, a_6 \in K$.

3. La condición $\Delta \neq 0$ no sólo asegura que las raíces sean diferentes, más adelante veremos que esta curva no posee puntos singulares.

Una ecuación de Weierstrass

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

puede ser simplificada. Analicemos tres casos:

1. Si la característica del cuerpo no es 2 ni 3, entonces podemos dividir por 2 y completando cuadrados obtenemos:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right)$$

que puede ser escrito como

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

con $y_1 = y + a_1x/2 + a_3/2$ y con constantes a_2', a_4', a_6' y como la característica es diferente de 3, considerando $x_1 = x + a_2'/3$ obtenemos

$$y_1^2 = x_1^3 + Ax_1 + B \tag{2.2}$$

con $A, B \in K$.

2. Si la característica de K es 2, entonces hay que considerar dos casos:
Si $a_1 \neq 0$ la curva elíptica toma la forma

$$y^2 + xy + x^3 + a_2x^2 + a_6 = 0 \tag{2.3}$$

esta curva es no singular si y sólo si $a_6 \neq 0$.

Si $a_1 = 0$ la curva elíptica toma la forma

$$y^2 + a_3y + x^3 + a_4x + a_6 = 0 \tag{2.4}$$

esta curva es no singular si y sólo si $a_3 \neq 0$.

3. Si la característica de K es 3, también hay que considerar dos casos:
Si $a_1^2 \neq -4a_2$ de lo visto en (1) la curva elíptica toma la forma

$$y^2 = x^3 + Cx^2 + Ax + B \tag{2.5}$$

con $A, B, C \in K$.

Si $a_1^2 = -4a_2$ la curva elíptica toma la forma

$$y^2 = x^3 + Ax + B \tag{2.6}$$

con $A, B \in K$.

Nuestro estudio se concentrará en estudiar las curvas elípticas de la forma

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

con $A, B \in K$, donde se cumple lo siguiente:

1. Reemplazando $a_1 = 0, a_2 = 0, a_4 = A, a_3 = 0$ y $a_6 = B$ en la discriminante de la ecuación (2.1) tenemos que

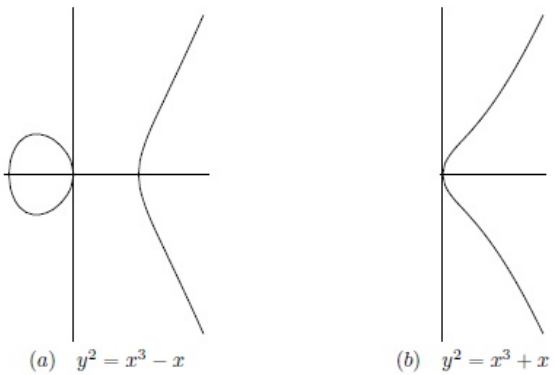
$$\Delta = -16(4A^3 + 27B^2)$$

2. Si las raíces de la ecuación $y^2 = x^3 + Ax + B$ son r_1, r_2, r_3, entonces se puede probar que la discriminante de la ecuación es

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -16(4A^3 + 27B^2) \neq 0$$

   Como la discriminante de esta ecuación es diferente de cero, esto prueba el hecho que sus raíces sean distintas.

No es posible ver la gráfica de una curva elíptica sobre muchos cuerpos arbitrarios, sin embargo nosotros podemos ver la gráfica sobre los números reales. Estas tienen dos formas básicas



Formas básicas de una curva elíptica

En el primer caso la ecuación $y^2 = x^3 - x$ tiene tres raíces reales diferentes. En el segundo caso, la ecuación $y^2 = x^3 + x$ tiene sólo una raíz real.

2.2. Espacio proyectivo

Dado un cuerpo K, definamos la relación

$$\sim = \big\{((x_1, y_1, z_1), (x_2, y_2, z_2)) \in (K^3 \backslash \{(0,0,0)\}) \times (K^3 \backslash \{(0,0,0)\}) :$$

$$(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2) \quad \text{para algún } \lambda \in K \backslash \{0\}\big\}$$

no es difícil ver que dicha relación es de equivalencia. Denotaremos $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ en caso que $((x_1, y_1, z_1), (x_2, y_2, z_2)) \in \sim$.

Definición 2.2.1. *Definamos el espacio proyectivo bidimensional, denotado por* $\mathbb{P}^2_K$ *como*

$$\mathbb{P}^2_K = (K^3 - \{(0,0,0)\}) \times (K^3 - \{(0,0,0)\}) / \sim$$

Denotaremos la clase de equivalencia de $(x, y, z) \in K \backslash \{(0,0,0)\}$ como $(x : y : z)$. Si $(x : y : z)$ es un punto con $z \neq 0$ entonces $(x : y : z) = (x/z : y/z : 1)$ son los **puntos finitos** en $\mathbb{P}^2_K$. Sin embargo, si $z = 0$ entonces dividir por z puede ser tomado como un punto al infinito y por lo tanto los puntos $(x : y : 0)$ son llamados **puntos al infinito** en P^2_K.

Definición 2.2.2. *Definamos el* ***plano afín*** *bidimensional sobre* K*, denotado por* A^2_K *como*

$$A^2_K = \big\{(x, y) \in K \times K\big\}$$

Sean $U = \{(x : y : z) | \, z \neq 0\}$ y $L_\infty(K) = \{(x : y : z) | \, z = 0\}$ tenemos que

$$\begin{array}{ccccccccc} \psi_1 : & A^2_K & \to & U & y & \psi_2 : & \mathbb{P}^1_K & \to & L_\infty(K) \\ & (x, y) & \to & (x : y : 1) & & & (x : y) & \to & (x : y : 0) \end{array}$$

ψ_1 y ψ_2 son biyecciones.
De esta manera el plano afín esta identificado con los puntos finitos de P^2_K, además $P^2_K = U \cup L_\infty(K)$, esta unión es disjunta.

Definición 2.2.3. *Un polinomio* $F \in K[x, y, z]$ *se dice que es homogéneo de grado positivo* n *si todos sus términos poseen el mismo grado* n*.*

Es decir un polinomio $F \in K[x, y, z]$ es homogéneo de grado n si

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$$

para todo $\lambda \in K$.

Definición 2.2.4. *Dado un polinomio $F \in K[x, y, z]$ homogéneo no constante, definamos el conjunto de los K-puntos racionales de la curva proyectiva sobre el cuerpo K cómo*

$$C(K) = \{(x : y : z) \in P_K^2 \,|\, F(x, y, z) = 0\}$$

Observaciones:

1. Si $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ con (x_1, y_1, z_1) y (x_2, y_2, z_2) pertenecientes a $(x : y : z) \in C(K)$ entonces

   $$F(x_1, y_1, z_1) = 0 \text{ si y sólo si } F(x_2, y_2, z_2) = 0,$$

   esto quiere decir que no depende de quién sea el representante.

2. Si $F(x, y, z)$ no fuese homogéneo no podríamos hablar de un cero en $\mathbb{P}_K^2$, esto debido a que si el polinomio por ejemplo fuese $F(x, y, z) = x^3 + 5xy - 6z$ tenemos que $F(1, 1, 1) = 0$ sin embargo $F(2, 2, 2) = 16$, aquí si dependería de su representante, este es uno de los motivos por lo que trabajaremos con polinomios homogéneos.

3. Para nuestro interés estudiaremos el polinomio $f(x, y) = y^2 - x^3 - Ax - B$ el cuál no es homogéneo, pero agregadole potencias de z, de la siguiente manera $F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$ logramos que lo sea.

Veamos el significado de que dos rectas paralelas se cortan en el infinito. Sean

$$y = mx + b_1, \;\; y = mx + b_2$$

dos rectas paralelas con $b_1 \neq b_2$, su forma homogénea sería

$$y = mx + b_1 z, \;\; y = mx + b_2 z.$$

Resolviendo ambas ecuaciones tendríamos que $z = 0$ y $y = mx$ con $x \neq 0$ por lo tanto estas rectas se intersectan en el punto

$$(x : mx : 0) = (1 : m : 0).$$

De igual manera, si $x = c_1$ y $x = c_2$, con $c_1 \neq c_2$ su forma homogénea sería

$$x = c_1 z, \;\; x = c_2 z.$$

Resolviendo tendríamos que $z = 0$ y $x = 0$, entonces $y \neq 0$ por lo tanto el punto de intersección de ambas rectas sería

$$(0 : y : 0) = (0 : 1 : 0).$$

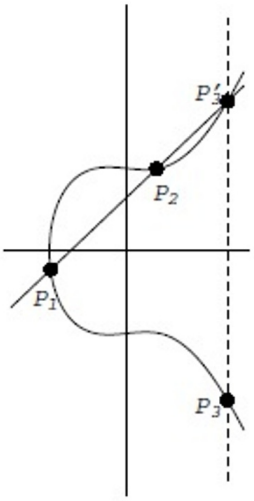
Para el caso de una curva elíptica, veamos que puntos se encuentran en el infinito, sea la curva elíptica $y^2 - x^3 - Ax - B = 0$ definida sobre K , su forma homogénea sería $y^2 z - x^3 - Axz^2 - Bz^3 = 0$, los puntos en la curva elíptica original de la forma (x, y) corresponden a los puntos $(x : y : 1)$ en su forma homogénea, pero si $z = 0$ entonces $x = 0$ y como $(x, y, z) \neq (0, 0, 0)$, tenemos que el único punto de P_K^2 que pertenece a la curva elíptica es

$$(0 : y : 0) = (0 : 1 : 0) = (0 : -1 : 0).$$

Es más debido a que $(0 : 1 : 0)$ pertenece a una recta vertical podemos afirmar que toda recta vertical intersecta a la curva elíptica E en dicho punto.

2.3. Ley de Grupo

Definamos la operación de adición de puntos en una curva elíptica de la siguiente manera:



Adición de puntos

Dado un par de puntos $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ que pertenecen a una curva elíptica, tracemos una recta L que pase a través de P_1 y P_2. Vemos que L intersecta a la curva E en un tercer punto P_3', reflejamos P_3' sobre el $eje\,x$ (cambia el signo de la segunda coordenada del punto P_3'). Decimos que

$$P_1 + P_2 = -P_3' = P_3$$

2.3.1. Fórmula de adición

Supongamos primero que $P_1 \neq P_2$ y que ningún punto es $\mathcal{O}$. Tracemos la recta L que pasa a través de P_1 y P_2, su pendiente será:

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Se presentan dos casos:

1. Si $x_1 \neq x_2$. La recta L esta dada por

   $$y = m(x - x_1) + y_1$$

   Para ver donde intersecta la recta L a la curva elíptica E, reemplazamos y en la ecuación de la curva

   $$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

   Ordenando obtenemos

   $$0 = x^3 - m^2x^2 + \ldots$$

   Las tres raíces de esta ecuación cúbica corresponden a los tres puntos de intersección de L con E. Como P_1, P_2 son puntos de L y E entonces se conoce dos raíces de esta ecuación que serían las primeras coordenadas de estos puntos se puede conocer la tercera raíz x, ya que $x_1 + x_2 + x = m^2$, ordenando obtenemos:

   $$\begin{aligned} x &= m^2 - x_1 - x_2 \\ y &= m(x - x_1) + y_1 \end{aligned}$$

   Ahora reflejando sobre el $eje\,x$ obtenemos el punto $P_3 = (x_3, y_3)$ con

   $$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

2. Si $x_1 = x_2$ pero $y_1 \neq y_2$, la linea que pasa por P_1 y P_2 es una linea vertical por lo tanto intersecta a E en $\mathcal{O}$. Reflejando $\mathcal{O}$ respecto al $eje\,x$ genera el mismo punto $\mathcal{O}$. Por lo tanto, en este caso $P_1 = P_2 = \mathcal{O}$.

2.3.2. Fórmula de duplicación

Ahora consideremos el caso donde $P_1 = P_2 = P = (x_1, y_1)$. La recta que pasa por esos puntos es una recta tangente. Por lo tanto, cuando dos puntos coinciden tomamos una recta L que pase por ellos este será la recta tangente. Calculemos la pendiente m de esta recta L:

$$2y\frac{dy}{dx} = 3x^2 + A \text{ , } entonces \;\; m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

1. Si $y_1 = 0$ entonces la recta es vertical y $P_1 + P_2 = \mathcal{O}$, además el numerador $3x_1^2 + A \neq 0$.

2. Si $y_1 \neq 0$, la recta L es:

   $$y = m(x - x_1) + y_1$$

   De igual manera como en el caso anterior obtenemos la ecuación cúbica

   $$0 = x^3 - m^2x^2 + ...$$

   En este caso sólo conocemos una raíz, digamos que sea x_1, pero es una raíz doble en ya que L es tangente a E en P y sea $2P = (x_3, y_3)$. Por lo tanto

   $$\begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

   Reemplazando $m = \frac{3x_1^2+A}{2y_1}$ obtenemos que

   $$x_3 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4y_1^2} \tag{2.7}$$

   y

   $$y_3 = \frac{x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - A^3 - 8B^2}{(2y_1)^3} \tag{2.8}$$

Esta fórmula de duplicación también puede estar dada en función de una de las raíces del polinomio $p(x) = x^3 + Ax + B$ con $A, B \in K$, supongamos que $r \in K$ es una raíz de dicho polinomio entonces

$$B = -r^3 - Ar$$

reemplazando en la ecuación (2.7) tenemos que

$$x_3 = \frac{x_1^4 - 2Ax_1^2 - 8(-r^3 - Ar)x_1 + A^2}{4y_1^2}$$

$$= \frac{x_1^4 - 2Ax_1^2 - 8(-r^3 - Ar)x_1 + A^2}{4y_1^2} + 4r(r^3 + Ar + B)$$
$$= \frac{(2rx_1 - x_1^2)^2 + 2(2rx_1 - x_1^2)(A + 2r^2) + (A + 2r^2)^2}{4y_1^2} + r$$

Por lo tanto

$$x_3 = \big[\frac{-x_1^2 + 2rx_1 + A + 2r^2}{2y_1}\big]^2 + r \tag{2.9}$$

Finalmente supongamos $P_2 = \mathcal{O}$. La recta que pasa por P_1 y $\mathcal{O}$ es una recta vertical que intersecta E en el punto P_1' el cuál es reflejada por P_1 respecto al $eje\, X$ para conseguir $P_3 = P_1 + P_2$. Por lo tanto

$$P_1 + \mathcal{O} = P_1$$

para todo P_1 en E. Podemos decir además que $\mathcal{O} + \mathcal{O} = \mathcal{O}$. Notemos que, si P_1 y P_2 tienen coordenadas en un cuerpo K con $A, B \in K$ entonces $P_1 + P_2$ también tiene coordenadas en K. Por lo tanto $E(K)$ es cerrado con la suma de puntos.

Ejemplo 2.3.1. Para la curva elíptica definida sobre $\mathbb{R}$ dada por $y^2 = x^3 + 3x + 5$ Sean $P_1 = (2, \sqrt{19})$ y $P_2 = (3, \sqrt{41})$ puntos de dicha curva, por lo visto en la sección 2.3.1 tenemos que

$$P_1 + P_2 = (-0{,}8211, 1{,}4081).$$

Ejemplo 2.3.2. Para la curva elíptica definida sobre $\mathbb{R}$ dada por

$$y^2 = x^3 - 36x$$

Sea $P_1 = P_2 = (7, \sqrt{91})$ punto que pertenece a dicha curva, por lo visto en la sección 2.3.2 tenemos que

$$P_1 + P_2 = (19{,}8489, -84{,}2940).$$

Teorema 2.1. *Dada la curva elíptica E definida sobre K por*

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

Entonces E satisface siguientes propiedades:

1. *P+$\mathcal{O}$=P, para todo $P \in E$ (Existencia del neutro)*
2. *Dado $P \in E$ existe un $P' \in E$ con $P + P' = \mathcal{O}$. Este punto P' se denota por $-P$. (Existencia del inverso)*

3. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ *para todo* $P_1, P_2, P_3 \in E$. *(Asociatividad)*

4. $P_1 + P_2 = P_2 + P_1$, *para todo* $P_1, P_2 \in E$ *(Conmutatividad)*

En otras palabras los puntos de la curva elíptica E *tienen la estructura un grupo abeliano con la suma aquí definida.*

Prueba.-

1. La propiedad de la existencia del neutro viene de la definición.
2. Sea P' el reflejo de P respecto del $eje\,X$ entonces $P + P' = \mathcal{O}$, esto es debido a la simetría respecto del $eje\,X$ que posee la curva.
3. La prueba de la asociatividad se verá con mayor detalle en la siguiente sección.
4. La conmutatividad es obvia ya que el reflejo del punto de intersección entre la curva y la recta que pasa por P_1 y P_2 es la misma.

□

2.4. Asociatividad de la ley de grupo

Sean los puntos $P, Q, R \in E$, para la prueba es suficiente probar que

$$-((P + Q) + R) = -(P + (Q + R))$$

Definamos las rectas

$$l_1 = \overline{PQ}, \quad l_2 = \overline{\mathcal{O}, Q + R}, \quad l_3 = \overline{R, P + Q},$$
$$m_1 = \overline{QR}, \quad m_2 = \overline{\mathcal{O}, P + Q}, \quad m_3 = \overline{P, Q + R}.$$

Tenemos las siguientes intersecciones:

$\cap$	m_1	m_2	m_3
l_1	Q	$-(P + Q)$	P
l_2	$-(Q + R)$	$\mathcal{O}$	$Q + R$
l_3	R	$P + Q$	X

Estos puntos $P_{ij} = l_i \cap m_j$ con $i, j = 1, 2, 3$ y $(i, j) \neq (3, 3)$ pertenecen a E a excepción posiblemente de $X = P_{33}$. Probaremos más adelante que teniendo los ocho puntos $P_{ij} \neq P_{33}$ en E entonces $P_{33} \in E$. En el desarrollo de la prueba encontraremos 3 inconvenientes que debemos tener en cuenta, estos son:

i) Primero considerar que algunos de los puntos pueden estar en el infinito, para ello necesitaremos usar coordenadas proyectivas.

ii) Segundo una recta puede ser tangente a E, lo que significa que dos P_{ij} pueden ser iguales. En este caso introduciremos el concepto del orden en que una recta intersecta a una curva.

iii) Tercero dos de las rectas podrían ser iguales.

Empecemos estudiando las rectas en $\mathbb{P}^2_K$.

Definición 2.4.1. *Una recta en el espacio proyectivo $\mathbb{P}^2_K$ se define como la ecuación lineal $ax + by + cz = 0$. Esta también se puede describir paramétricamente como:*

$$\begin{aligned} x &= a_1u + b_1v \\ y &= a_2u + b_2v \\ z &= a_3u + b_3v \end{aligned} \tag{2.10}$$

con $u, v \in K$, y $(u, v) \neq (0, 0)$.

Ejemplo 2.4.1. Si $a \neq 0$, la recta

$$ax + by + cz = 0$$

se puede describir por

$$x = -(b/a)u - (c/a)v, \quad y = u, \quad z = v.$$

De la definición podemos afirmar que la matriz

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}$$

posee rango 2.
Esto debido a que si todos los vectores (a_i, b_i) con $i \in \{1, 2, 3\}$ son múltiplos uno del otro, digamos $(a_i, b_i) = \lambda_i(a_1, b_1)$ con $i \in \{2, 3\}$. Entonces $(x, y, z) = x(1, \lambda_2, \lambda_3)$ para todo u, v y $x \neq 0$, así obtendríamos un punto, en vez de una recta en el espacio proyectivo.

Por otro lado si $(u_1, v_1) = \lambda(u_2, v_2)$ para algún $\lambda \in K$, entonces (u_1, v_1) y (u_2, v_2) nos darán dos puntos equivalentes en el espacio $\mathbb{P}^2_K$. Por lo tanto, podemos ver a (u, v) como si recorrieran los puntos $(u : v)$ del espacio proyectivo unidimensional $\mathbb{P}^1_K$.

Ahora introduciremos la definición de el orden en que una recta intersecta una curva. El siguiente lema nos ayudará a darle sentido a dicha definición.

Lema 2.1. *Sea $G(u, v)$ un polinomio homogéneo no nulo y sea $(u_0 : v_0) \in \mathbb{P}^1_K$, entonces existe un entero $k \geq 0$ y un polinomio homogéneo $H(u, v)$ con $H(u_0, v_0) \neq 0$ tal que*

$$G(u, v) = (v_0 u - u_0 v)^k H(u, v).$$

Demostración. Supongamos que $v_0 \neq 0$. Sea m el grado de G y definamos $g(u) = G(u, v_0)$. Factorizando la mayor potencia de $u - u_0$ posible, podemos escribir $g(u) = (u - u_0)^k h(u)$ para algún k y algún polinomio h de grado $m - k$ con $h(u_0) \neq 0$. Definamos $H(u, v) = (v^{m-k}/v_0^m)h(uv_0/v)$, luego $H(u, v)$ es homogéneo de grado $m - k$. Entonces

$$\begin{aligned} G(u, v) &= \left(\frac{v}{v_0}\right)^m g\left(\frac{uv_0}{v}\right) = \frac{v^{m-k}}{v_0^m}(v_0 u - u_0 v)^k h\left(\frac{uv_0}{v}\right) \\ &= (v_0 u - u_0 v)^k H(u, v), \end{aligned}$$

como queríamos. □

Dada la curva C en el plano afín $f(x, y) = 0$ con f un polinomio y la recta L en términos del parámetro t como $x = a_1 t + b_1, \quad y = a_2 t + b_2$. Definamos

$$\tilde{f}(t) = f(a_1 t + b_1, a_2 t + b_2)$$

decimos que L intersecta a la curva C en $t = t_0$ si $\tilde{f}(t_0) = 0$.

Definición 2.4.2. *Decimos que L intersecta a C con orden $n \in \mathbb{Z}^+$ en el punto (x, y) correspondiente a $t = t_0$ si $(t - t_0)^n$ es la mayor potencia de $(t - t_0)$ que divide a $\tilde{f}$. En particular si $n \geq 2$ diremos que dicha recta L es tangente a C.*

La versión homogénea de la definición anterior es la siguiente. Dada la curva C en $\mathbb{P}^2_K$ definida por $F(x, y, z) = 0$ con $F(x, y, z)$ un polinomio homogéneo de grado n y sea L una recta dada paramétricamente por (2.10). Definamos el polinomio homogéneo $\tilde{F}(u, v)$ con variables u, v como

$$\tilde{F}(u, v) = F(a_1 u + b_1 v, a_2 u + b_2 v, a_3 u + b_3 v).$$

Definición 2.4.3. *Decimos que L intersecta a C con orden $n \in \mathbb{Z}^+$ en el punto $P = (x_0 : y_0 : z_0)$ correspondiente a $(u : v) = (u_0 : v_0)$ si $(v_0u - u_0v)^n$ es la mayor potencia de $(v_0u - u_0v)$ que divide a $\tilde{F}(u, v)$. Denotamos esto por*

$$\mathrm{ord}_{L,P}(F) = n.$$

En particular si $\tilde{F}$ es nulo decimos que el $\mathrm{ord}_{L,P}(F) = \infty$. La ventaja de la formulación homogénea es que nos permite tratar los puntos en el infinito y los puntos finitos de manera uniforme.

De la definición podemos afirmar que si la recta L intersecta a las curvas C_1 y C_2 con $C_1 \neq C_2$ definidas por $F_1(x, y, z) = 0$ y $F_2(x, y, z) = 0$ respectivamente, además $F_1(x, y, z)$ y $F_2(x, y, z)$ polinomios homogéneos en un mismo punto $P \in P_K^2$ con $\mathrm{ord}_{L,P}(F_1) = m$ y $\mathrm{ord}_{L,P}(F_n) = n$ se cumple que:

a) $\mathrm{ord}_{L,P}(F_1 \pm F_2) \geq \mathrm{mín}\{m, n\}$.

b) $\mathrm{ord}_{L,P}(F_1F_2) \geq mn$.

c) Sí $m \geq n$, entonces $\mathrm{ord}_{L,P}(F_1/F_2) \geq m - n$.

Lema 2.2. *Sean L_1 y L_2 rectas en P_K^2. Se cumple*

1. *Si L_1 y L_2 se intersectan en un único punto $P \in P_K^2$ entonces $ord_{L_1,P}(L_2) = 1$.*

2. *Si $L_1(x, y, z) = \alpha L_2(x, y, z)$, para algún $\alpha \in K^*$ entonces $ord_{L_1,P}(L_2) = \infty$.*

Demostración. Empecemos probando la parte (1).

1. Sea el punto P que pertenece L_1 y L_2 con parametros asociados (u_0, v_0), entonces $\tilde{L_2}(u_0, v_0) = 0$ y además $\tilde{L_2}$ es un polinomio homogéneo de grado 1 entonces existe $\alpha \in K^*$ tal que $\tilde{L_2}(u, v) = \alpha(v_0u - u_0v)$.

2. Sean las rectas $L_1(x, y, z) = ax+by+cz = 0$ y $L_2(x, y, z) = \alpha ax+\alpha by+\alpha cz = 0$, para algún $\alpha \in K^*$, supongamos que $c \neq 0$ parametrizando la recta L_2 por $x = u$, $y = v$, $z = c^{-1}\alpha^{-1}(-\alpha au - \alpha bv)$ con $u, v \in K$. Luego

$$\begin{aligned} \tilde{L_1}(u, v) &= L_1(u, v, c^{-1}\alpha^{-1}(-\alpha au - \alpha bv)) \\ &= au + bv + cc^{-1}(-au - bv)) \\ &= 0. \end{aligned}$$

   Sean v_0 y u_0 parámetros asociados al punto de intersección $P \in P_K^2$, entonces $(v_0u - u_0v)^n$ divide a 0, para todo $n \in \mathbb{Z}_{>0}$. Por lo tanto $ord_{L_1,P}(L_2) = \infty$.

□

Definición 2.4.4. Decimos que una curva C en $\mathbb{P}^2_K$ definida por $F(x,y,z)=0$ con $F(x,y,z)$ un polinomio homogéneo de grado 3 es *no singular* en un punto P si al menos una de sus derivadas parciales F_x, F_y, F_z no se anula en P.

Ejemplo 2.4.2. Sea la curva elíptica definida en coordenadas homogéneas por

$$F(x,y,z) = y^2z - x^3 - Axz^2 - Bz^3 = 0$$

Supongamos que la característica del cuerpo K no es ni 2 ni 3. Veamos que dicha curva no posee puntos singulares, hallemos sus derivadas parciales

$$F_x = -3x^2 - Az^2, \quad F_y = 2yz, \quad F_z = y^2 - 2Axz - 3Bz^2.$$

Supongamos que $P=(x:y:z)$ es un punto singular. Si $z=0$ como $F_x = F_z = 0$ tenemos que $x=y=0$, entonces $P=(0:0:0)$ pero este punto no pertenece al espacio proyectivo bidimensional. Por lo tanto $z \neq 0$, luego podemos tomar $z=1$. Si $F_y = 0$, entonces $y=0$. Como $(x:y:1)$ pertenece a la curva, x debe satisfacer $x^3 + Ax + B = 0$. Si $F_x = -(3x^2 + A) = 0$, entonces x es raíz del polinomio y de su derivada, por lo tanto es una raíz doble ($\triangle = 0$). Como hemos asumido que dicha curva no tiene raíces múltiples, esto sería una contradicción. Por lo tanto, una curva elíptica no tiene puntos singulares.

Definición 2.4.5. *Si P es un punto no singular de una curva $F(x,y,z)=0$ con $F(x,y,z)$ un polinomio homogéneo de grado 3 entonces la recta tangente en P esta dada por*

$$F_x(p)x + F_y(P)y + F_z(P)z = 0.$$

Ejemplo 2.4.3. Sea la curva

$$y^2z - x^3 - Axz^2 - Bz^3 = 0$$

la *recta tangente* en $(x_0:y_0:z_0)$ es

$$(-3x_0^2 - Az_0^2)x + 2y_0z_0y + (y_0^2 - 2Ax_0z_0 - 3Bz_0^2)z = 0.$$

En coordenadas afines, haciendo $z_0 = z = 1$, tenemos la recta que usamos para sumar un punto consigo mismo en una curva elíptica

$$(-3x_0^2 - A)(x - x_0) + 2y_0(y - y_0) = 0.$$

Por lo visto al inicio, sabemos que el punto al infinito de una curva elíptica esta dado por $(0:1:0)$. La recta tangente en dicho punto está dada por $0x+0y+z=0$, que la llamamos **recta en el infinito** en $\mathbb{P}^2_K$. Esto corresponde con el hecho de que $\mathcal{O}+\mathcal{O}=\mathcal{O}$ en una curva elíptica.

Lema 2.3. *Dada la curva C en $\mathbb{P}^2_K$ por $F(x,y,z)=0$ con $F(x,y,z)$ un polinomio homogéneo de grado 3. Si P es un punto no singular de F entonces existe una única recta en $\mathbb{P}^2_K$ que intersecta a C en P, con orden $k\geq 2$.*

Demostración. Consultar [10,pág 24] □

La asociatividad de la suma en una curva elíptica se desprenderá fácilmente del siguiente resultado.

Teorema 2.2. *Dada la curva C en $\mathbb{P}^2_K$ descrita por $C(x,y,z)=0$, con $C(x,y,z)$ un polinomio homogéneo de grado 3 y sean l_1,l_2,l_3,m_1,m_2,m_3 rectas en $\mathbb{P}^2_K$ tales que $l_i\neq m_j$ y $l_i\cap m_j=P_{ij}$, con $i,j=1,2,3$. Si P_{ij} es un punto no singular en la curva C para todo $(i,j)\neq(3,3)$, además si para algún i, existen $k\geq 2$ puntos iguales del conjunto de puntos $\{P_{i1},P_{i2},P_{i3}\}$, entonces l_i intersecta a C con orden al menos k en este punto, de igual manera si para algún j existen $k\geq 2$ puntos iguales del conjunto de puntos $\{P_{1j},P_{2j},P_{3j}\}$, entonces m_j intersecta a C con orden al menos k en este punto. Bajo estas condiciones tenemos que P_{33} pertenece a la curva C.*

Prueba.-Sean las rectas $l_1=ax+by+cz=0$ en su forma paramétrica

$$\begin{aligned} x &= a_1u+b_1v \\ y &= a_2u+b_2v \\ z &= a_3u+b_3v \end{aligned} \tag{2.11}$$

y $m_j(x,y,z)=a'_jx+b'_jy+c'_jz=0$ con $j=1,2,3$, como la recta l_1 y m_j pasan por P_{11},P_{12} y P_{13} que pertenecen a C, con $j=1,2,3$, sean $(u_1:v_1),(u_2:v_2),(u_3:v_3)$ los parámetros en l_1 para estos puntos entonces $\tilde{C}(u_i,v_i)=0$ para $i=1,2,3$ y $\tilde{m}_j(u_j,v_j)=0$ con $j=1,2,3$. Como $\tilde{m}_j(u,v)$ se anula sólo en P_{ij}, decimos que la forma lineal $\tilde{m}_j$ es no nula. Por lo tanto, el producto $\tilde{m}_1(u,v)\tilde{m}_2(u,v)\tilde{m}_3(u,v)$ y $\tilde{C}$ son polinomios homogéneos de grado 3 no nulos que se anulan en $(u_1:v_1),(u_2:v_2),(u_3:v_3)$, hallemos una relación entre ellos.

Lema 2.4. *Sean $R(u,v)$ y $S(u,v)$ polinomios homogéneos de grado 3, con $S(u,v)$ no nulo, y supongamos que existen tres puntos $(u_i : v_i)$, $i = 1,2,3$ donde R y S se anulan. Además, si k de estos puntos son iguales, tenemos que R y S se anulen con orden al menos k en este punto (esto es, que $(v_i u - u_i v)^k$ divida a R y S). Entonces existe una constante $\alpha \in K$ tal que $R = \alpha S$.*

Prueba.-Empecemos probando que un polinomio homogéneo $S(u,v)$ de grado 3, puede tener como máximo 3 ceros $(u : v)$ en $\mathbb{P}^1_K$ (contando multiplicidades). Sabemos que los puntos $(u : v) \in P^1_K$ están conformados por los puntos $(1 : 0)$ y $(u : v) \neq (1 : 0)$, este último se puede escribir de la forma $(u : 1)$, empecemos analizando $(1 : 0)$. Supongamos que $S(u,v)$ se anula con orden k en $(1 : 0)$ entonces $S(u,v) = v^k S_0(u,v)$ con $S_0(1,0) \neq 0$. Como $S_0(u,1)$ es un polinomio de grado $3-k$ entonces puede tener a lo más $3-k$ ceros, contando multiplicidades (si K es algebraicamente cerrado entonces tiene $3-k$). Luego $S_0(u,v)$ tiene a lo más $3-k$ ceros. Por lo tanto, $S(u,v)$ tiene a lo más $k + (3-k) = 3$ ceros en $\mathbb{P}^1_K$. Sea $(u_0 : v_0)$ cualquier punto en $\mathbb{P}^1_K$ distinto de los $(u_i : v_i)$. Como S puede tener a lo más tres ceros, $S(u_0, v_0) \neq 0$. Sea $\alpha = R(u_0, v_0)/S(u_0, v_0)$. Entonces $R(u,v) - \alpha S(u,v)$ es un polinomio homogéneo de grado 3 que se anula en los cuatro puntos $(u_i : v_i)$, $i = 0,1,2,3$. Por lo tanto, $R - \alpha S$ debe ser idénticamente nulo. □

Regresando a la prueba del teorema, notamos que $\tilde{C}$ y $\tilde{m}_1\tilde{m}_2\tilde{m}_3$ se anulan en los puntos $(u_i : v_i)$, $i = 1,2,3$. Además, si k de los puntos P_{1j} son iguales, entonces k de las funciones lineales $\tilde{m}_j(u,v)$, $j = 1,2,3$, se anulan en este punto, luego el producto $\tilde{m}_1(u,v)\tilde{m}_2(u,v)\tilde{m}_3(u,v)$ se anulan con orden al menos k. Por suposición, $\tilde{C}$ se anula con orden al menos k en esta situación. Por el lema anterior, existe una constante $\alpha \in K$ tal que

$$\tilde{C} = \alpha \tilde{m}_1 \tilde{m}_2 \tilde{m}_3.$$

Definamos:

$$C_1(x,y,z) = C(x,y,z) - \alpha m_1(x,y,z) m_2(x,y,z) m_3(x,y,z).$$

Como $l_1(x,y,z) = ax + by + cz = 0$, vamos a probar que C_1 es un múltiplo de l_1. Como sabemos que la recta l_1 tiene al menos un coeficiente no nulo, supongamos que $a \neq 0$. Los otros casos son similares. La parametrización de la recta l_1 se puede tomar como

$$x = -(b/a)u - (c/a)v, \quad y = u, \quad z = v. \tag{2.12}$$

Entonces

$$\begin{aligned}\tilde{C}_1(u,v) &= C_1(-(b/a)u-(c/a)v,u,v)\\ &= \tilde{C}(u,v)-\alpha\tilde{m}_1(u,v)\tilde{m}_2(u,v)\tilde{m}_3(u,v)\\ &= 0.\end{aligned}$$

Escribamos $C_1(x,y,z)$ como un polinomio en x, con polinomios en y,z como coeficientes. Escribiendo

$$x^n=(1/a^n)((ax+by+cz)-(by+cz))^n=(1/a^n)((ax+by+cz)^n+\cdots),\ n=1,2,3$$

podemos reordenar $C_1(x,y,z)$ como un polinomio en $ax+by+cz$ con coeficientes en y,z:

$$C_1(x,y,z)=a_3(y,z)(ax+by+cz)^3+\cdots+a_0(y,z). \tag{2.13}$$

Reemplazando (2.12) en (2.13) tenemos

$$\tilde{C}_1(u,v)=a_0(u,v)=0$$

pues $ax+by+cz$ se anula cuando x,y,z se escriben en términos de u,v. Por lo tanto, $a_0(y,z)=a_0(u,v)$ es el polinomio cero. Se sigue de (2.13) que $C_1(x,y,z)$ es un múltiplo de $l_1(x,y,z)=ax+by+cz$. De igual manera, existe una constante β tal que $C(x,y,z)-\beta l_1l_2l_3$ es un múltiplo de m_1. Definamos:

$$D(x,y,z)=C-\alpha m_1m_2m_3-\beta l_1l_2l_3.$$

un polinomio homogéneo de grado 3. Entonces $D(x,y,z)$ es un múltiplo de l_1 y un múltiplo de m_1.

Lema 2.5. *$D(x,y,z)$ es un múltiplo de $l_1(x,y,z)m_1(x,y,z)$.*

Prueba.-Sea $D=m_1D_1$, vamos a provar que l_1 divide a D_1. Parametrizamos la recta l_1 por (2.12) (nuevamente, consideramos el caso $a\neq 0$), reemplazando en $D=m_1D_1$ tenemos que $\tilde{D}=\tilde{m}_1\tilde{D}_1$. Como l_1 divide a D, tenemos $\tilde{D}=0$. Como $m_1\neq l_1$, tenemos $\tilde{m}_1\neq 0$. Por lo tanto, $\tilde{D}_1(u,v)$ es el polinomio cero. Como arriba, esto implica que $D_1(x,y,z)$ es un múltiplo de l_1, como queríamos. □

Por el lema anterior tenemos que

$$D(x,y,z)=l_1m_1l,$$

donde $l(x,y,z)$ es lineal. Por suposición, $C=0$ en P_{22},P_{23},P_{32}. Además, l_1,l_2,l_3 y m_1,m_2,m_3 se anulan en estos puntos. Por lo tanto, $D(x,y,z)$ se anula en estos puntos. Nuestra meta es mostrar que D es idénticamente 0.

Lema 2.6. $l(P_{22}) = l(P_{23}) = l(P_{32}) = 0$.

Prueba.-Vamos a probar que $l(P_{23}) = 0$.

1. Si $P_{13} \neq P_{23}$. Tenemos que, $l_1(P_{23}) \neq 0$. Como $D(P_{23}) = 0$, se sigue que $m_1(P_{23})l(P_{23}) = 0$.

2. Si $P_{13} = P_{23}$. Tenemos que, por la suposición del teorema, m_3 es tangente a C en P_{23}, luego $\text{ord}_{m_3,P_{23}}(C) \geq 2$. Como $P_{13} = P_{23}$ y P_{23} pertenece a m_3, tenemos $\text{ord}_{m_3,P_{23}}(l_1) = \text{ord}_{m_3,P_{23}}(l_2) = 1$. Por lo tanto, $\text{ord}_{m_3,P_{23}}(\beta l_1 l_2 l_3) \geq 2$. Además, $\text{ord}_{m_3,P_{23}}(\alpha m_1 m_2 m_3) = \mathcal{O}$. Por lo tanto, $\text{ord}_{m_3,P_{23}}(D) \geq 2$, pues D es una suma de términos, cada uno de los cuales se anula con orden al menos 2. Pero $\text{ord}_{m_3,P_{23}}(l_1) = 1$, luego tenemos

$$\text{ord}_{m_3,P_{23}}(m_1 l) = \text{ord}_{m_3,P_{23}}(D) - \text{ord}_{m_3,P_{23}}(l_1) \geq 1.$$

   Por lo tanto, $m_1(P_{23})l(P_{23}) = 0$.

En ambos casos, tenemos $m_1(P_{23})l(P_{23}) = 0$. Si $m_1(P_{23}) = 0$, entonces P_{23} está en m_1, l_2 y m_3, por definición. Como l_2 y m_1 se intersectan en un único punto, entonces $P_{23} = P_{21}$. Por la suposición del teorema, l_2 es por lo tanto tangente a C en P_{23}. De ahí que, como vimos anteriormente llegamos a que $\text{ord}_{l_2,P_{23}}(D) \geq 2$, luego

$$\text{ord}_{l_2,P_{23}}(l_1 l) \geq 1.$$

Si en este caso tenemos $l_1(P_{23}) = 0$, entonces P_{23} está en l_1, l_2, m_3. Por lo tanto $P_{13} = P_{23}$. Por suposición, la recta m_3 es tangente a C en P_{23}. Como P_{23} es un punto no singular de C, por el lema 2.3 $l_2 = m_3$, contrario a nuestra hipótesis. Por lo tanto, $l_1(P_{23}) \neq 0$, luego $l(P_{23}) = 0$. De igual manera se puede probar que $l(P_{22}) = l(P_{32}) = 0$. □

Si $l(x, y, z)$ es idénticamente nulo, entonces D es idénticamente nulo. Por lo tanto, asumamos que $l(x, y, z)$ no es cero y por lo tanto define una recta l. Analicemos por casos.

1. Si $P_{23} \neq P_{22} \neq P_{32}$: entonces l y l_2 son rectas a través de P_{23} y P_{22}. Por lo tanto $l = l_2$. De igual manera, $l = m_2$. Por lo tanto, $l_2 = m_2$, contradicción.

2. Si $P_{32} = P_{22} \neq P_{23}$: entonces m_2 es tangente a C en P_{22}. Como antes,

$$\text{ord}_{m_2,P_{22}}(l_1 m_1 l) \geq 2.$$

Si $m_1(P_{22}) = 0$, entonces P_{22} pertenece a m_1, m_2, l_2. Por lo tanto, $P_{21} = P_{22}$. Esto significa que l_2 es tangente a C en P_{22}. Por el lema (2.3), $l_2 = m_2$, lo cuál es una contradicción. Por lo tanto, $m_1(P_{22}) \neq 0$. Si $l_1(P_{22}) \neq 0$, entonces $\text{ord}_{m_2,P_{22}}(l) \geq 2$. Esto significa que l es la misma recta que m_2. Si $l_1(P_{22}) = 0$, entonces $P_{22} = P_{23}$ pertenece a l_1, l_2, l_3, m_2, luego $P_{12} = P_{22} = P_{32}$. Por lo tanto $\text{ord}_{m_2,P_{22}}(C) \geq 3$. Por el razonamiento de arriba, ahora tenemos $\text{ord}_{m_2,P_{22}}(l_1 m_1 l) \geq 3$. Como hemos probado que $m_1(P_{22}) \neq 0$, tenemos $\text{ord}_{m_2,P_{22}}(l) \geq 2$. Esto significa que l es la misma recta que m_2. Así, hemos probado, bajo la suposición de que $P_{32} = P_{22}$, que l es la misma recta que m_2. Por el lema anterior, P_{23} pertenece a l, y por lo tanto a m_2. También pertenece a l_2 y m_3. Por lo tanto, $P_{22} = P_{23}$, lo cuál sería una contradicción.

3. Si $P_{23} = P_{22} \neq P_{32}$: se sigue igual que el caso anterior.

4. Si $P_{23} = P_{32}$: entonces P_{23} pertenece a l_2, l_3, m_2, m_3. Entonces $P_{22} = P_{32}$, que ya hemos visto que es imposible.

5. Si $P_{23} = P_{22} = P_{32}$: entonces m_2 y l_2 es tangente a C en P_{22}, entonces $l_2 = m_2$, lo cuál es una contradicción.

Por lo tanto, todas las posibilidades nos llevan a contradicciones. Entonces $l(x, y, z)$ debe ser idénticamente 0. Por lo tanto, $D = 0$, luego

$$C = \alpha l_1 l_2 l_3 + \beta m_1 m_2 m_3.$$

Como l_3 y m_3 se anulan en P_{33}, tenemos $C(P_{33}) = 0$, como queríamos. Esto completa la prueba del teorema 2.4. □

Como las hipótesis del teorema se satisfacen entonces todos los puntos en la tabla que vimos al inicio, incluyendo a X, pertenecen a E. Por lo tanto esto probaría la asociatividad de puntos en una curva elíptica. Analicemos el caso en que algunos de los puntos de intersección $P, Q, R, \pm(P + Q), \pm(Q + R)$ son $\mathcal{O}$. En los casos donde al menos uno de P, Q, R es $\mathcal{O}$, la asociatividad es trivial. Si $P + Q = \mathcal{O}$, entonces $(P + Q) + R = \mathcal{O} + R = R$. Por otro lado, la suma $Q + R$ se calcula primero dibujando la recta por Q y R, que intersecta a E en $-(Q + R)$. Como $P + Q = \mathcal{O}$,

el reflejo de Q por el eje x es P. Por lo tanto, el reflejo L' de L pasa por P, $-R$ y $Q+R$. La suma $P+(Q+R)$ se encuentra dibujando la recta por P y $Q+R$, que es L'. Acabamos de observar que el tercer punto de intersección de L' con E es $-R$. Reflejando obtenemos $P+(Q+R)=R$, luego se cumple la asociatividad en este caso. Similarmente, la asociatividad se cumple cuando $Q+R=\mathcal{O}$. Finalmente, necesitamos considerar qué pasa si alguna recta l_i es igual a alguna recta m_j, en ese caso no se podría aplicar el teorema 2.4. Pero se puede ver que la asociatividad se cumple en esos casos. Supongamos que $l_i = m_j$ para algunos i, j. Consideremos los varios casos, supongamos que todos los puntos en la tabla de intersecciones son finitos, excepto por $\mathcal{O}$ y posiblemente X. Note que cada l_i y cada m_j corta a E en tres puntos (contando multiplicidades), uno de los cuales es P_{ij}. Si las dos rectas coinciden, entonces los otros dos puntos deben coincidir en algún orden. Veamos:

1. Si $l_1 = m_1$: entonces P, Q, R son colineales, y se cumple la asociatividad.

2. Si $l_1 = m_2$: en este caso, $P, Q, \mathcal{O}$ son colineales, luego $P+Q=\mathcal{O}$; la asociatividad se sigue por el cálculo directo hecho arriba.

3. Si $l_2 = m_1$: similar al caso previo.

4. Si $l_1 = m_3$: entonces $P, Q, Q+R$ son colineales. Entonces $P+(Q+R)=-Q$. Además, $P+Q=-(Q+R)$, luego $(P+Q)+R=-(Q+R)+R$. Vamos a probar que $-Q=-(Q+R)+R$, sea la recta L que pasa por Q y R, entonces L intersecta a la curva elíptica en $-(Q+R)$. Viendo a L como la recta que pasa por $-(Q+R)$ y R, obtenemos $-(Q+R)+R=-Q$. Por lo tanto cumple la asociatividad.

5. $l_3 = m_1$: entonces $P+Q$ debe ser $\pm(Q+R)$. Si $P+Q=Q+R$, entonces de la conmutatividad y del lema de arriba obtenemos

$$P=(P+Q)-Q=(Q+R)-Q=R.$$

Por lo tanto,

$$(P+Q)+R=R+(P+Q)=P+(P+Q)=P+(R+Q)=P+(Q+R).$$

Si $P+Q=-(Q+R)$, entonces

$$(P+Q)+R=-(Q+R)+R=-Q$$

y

$$P + (Q + R) = P - (P + Q) = -Q,$$

y se cumple la asociatividad.

6. Si $l_2 = m_3$: en este caso, la recta m_3 que pasa por P y $(Q + R)$ intersecta a E en $\mathcal{O}$, luego $P = -(Q + R)$. Como $-(Q + R), Q, R$ son colineales, tenemos que P, Q, R son colineales y la asociatividad se cumple.

7. Si $l_3 = m_2$: similar al caso anterior.

8. Si $l_3 = m_3$: como l_3 no puede intersectar a E en 4 puntos (contando multiplicidades), es fácil ver que $P = R$ ó $P = P + Q$ ó $Q + R = P + Q$ ó $Q + R = R$. El caso $P = R$ se trató en el caso $l_2 = m_2$. Asumamos que $P = P + Q$. Sumando $-P$ y como vimos en la parte 4, tenemos que $\mathcal{O} = Q$, en cuyo caso la asociatividad se cumple. El caso $Q + R = R$ es similar. Si $Q + R = P + Q$, sumando $-Q$ y como vimos en la parte 4, tenemos que $P = R$, que ya hemos tratado.

Si $l_i \neq m_j$ para todo i, j, las hipótesis del teorema se satisfacen y si algunos $l_i = m_j$ se cumple la asociatividad, como probamos arriba. Esto completa la prueba de la asociatividad de la suma en curvas elípticas. □

Capítulo 3

Curvas elípticas sobre $\mathbb{Q}$

En este capítulo nuestro objetivo es probar que el conjunto de puntos racionales de una curva elíptica, denotado por $E(\mathbb{Q})$ es un grupo finitamente generado, para ello probaremos en primer lugar que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito (teorema débil de Mordell). Empezaremos estudiando una curva elíptica que se descompone sobre $\mathbb{Q}$ (Caso particular del teorema débil de Mordell) y finalmente una curva elíptica que se descompone sobre una extensión finita de $\mathbb{Q}$.

3.1. Caso particular del teorema débil de Mordell

Sea E una curva elíptica de la forma:

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

con $e_1, e_2, e_3 \in \mathbb{Z}$ y $e_i \neq e_j$, para $i \neq j$. En caso que, $e_i \in \mathbb{Q}$ pero $e_i \notin \mathbb{Z}$, haciendo un cambio de variable podemos transformar la ecuación a una con $e_i \in \mathbb{Z}$.
Si $y \neq 0$, tenemos que el producto de $(x - e_1)$, $(x - e_2)$ y $(x - e_3)$ es un cuadrado perfecto entonces podemos suponer que cada uno de estos factores contiene un cuadrado, así podemos escribir

$$\begin{aligned} x - e_1 &= au^2 \\ x - e_2 &= bv^2 \\ x - e_3 &= cw^2 \end{aligned}$$

con $u, v, w \in \mathbb{Q}$ y a, b, c enteros libre de cuadrados. Entonces $y^2 = abc(uvw)^2$ con abc un cuadrado. Por lo tanto si nosotros estamos buscando los puntos $(x, y) \in E(\mathbb{Q})$,

podríamos encontrar números mas pequeños como $u, v, w \in \mathbb{Q}$. Esta es la idea básica que realizaremos para la prueba del teorema de Mordell.

Proposición 3.1. *Sea*

$$S = \{p/p\, es\, primo\, y\, p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}$$

Si p es un primo tal que $p \mid abc$, entonces $p \in S$.

Demostración. Sea $p \mid abc$, entonces $p \mid a$, $p \mid b$ ó $p \mid c$. Supongamos que $p \mid a$, como $x - e_1 = au^2$, entonces p^k con $k \in \mathbb{Z}$ impar, es la potencia exacta de p que divide a $x - e_1$. Si $k < 0$, entonces p^k es la potencia de p en el denominador de $x - e_2$ y $x - e_3$, entonces p^{3k} es la potencia de p en el denominador de y^2, lo cual es imposible, debido a que este es un cuadrado. Por lo tanto $k > 0$, esto significa que

$$p^k \mid (x - e_1) \Rightarrow x \equiv e_1\, (mod\, p),$$

de ahi tenemos que

$$x - e_2 \equiv e_1 - e_2\, (mod\, p) \quad y \quad x - e_3 \equiv e_1 - e_3\, (mod\, p).$$

Supongamos que $p \notin S$, entonces $p \nmid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$, esto quiere decir que

$$\begin{aligned} p \nmid e_1 - e_2 \quad &\Rightarrow \quad p \nmid x - e_2 \quad y \\ p \nmid e_1 - e_3 \quad &\Rightarrow \quad p \nmid x - e_3 \end{aligned}$$

Entonces p^k es la potencia exacta de $y^2 = (x - e_1)(x - e_2)(x - e_3)$ con k un entero positivo impar, lo cual es una contradicción. Por lo tanto $p \in S$. □

Como S es un conjunto finito, existe una cantidad finita de combinaciones (a, b, c). El siguiente teorema muestra que el conjunto de combinaciones (a, b, c) que vienen de los puntos (x, y) tienen una estructura de grupo módulo $\mathbb{Q}^*$ con $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ grupo multiplicativo.

Definición 3.1.1. *Sea $\mathbb{Q}^*$ un grupo multiplicativo y su subgrupo $(\mathbb{Q}^*)^2$. Definamos el grupo cociente*

$$\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2} = \{\overline{x} : x \in \mathbb{Q}^*\}\ con\ \overline{x} = \{xu^2 \in \mathbb{Q}^* : u \in \mathbb{Q}^*\}$$

Esto significa que si consideramos dos números racionales $\overline{x_1}, \overline{x_2}$ como equivalentes entonces la razón x_1/x_2 es el cuadrado de un número racional. Todo elemento de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ puede ser representado por ± 1 veces un producto de primos distintos, ya que $\overline{x}$ es congruente a $\overline{x^{-1}}$ módulo cuadrados. Así podemos decir que

$$\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2} = \{\pm\overline{2^m}\,\overline{3^n}\,\overline{5^p}\ldots \mid m, n, p, \ldots \in \{0, 1\}\} \tag{3.1}$$

Notemos que si $x - e_1 = au^2$, entonces $\overline{x - e_1} = \overline{a}$ en $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Teorema 3.1. *Sea E una curva elíptica dada por*

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

definida sobre $\mathbb{Q}$, con $e_1, e_2, e_3 \in \mathbb{Z}$. La función definida por

$$\phi: \quad E(\mathbb{Q}) \quad \rightarrow \quad (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \bigoplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \bigoplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2)$$

$$\begin{array}{ccc}
(x, y) & \rightarrow & (\overline{x - e_1}, \overline{x - e_2}, \overline{x - e_3}) \, con \, y \neq 0 \\
\mathcal{O} & \rightarrow & (\overline{1}, \overline{1}, \overline{1}) \\
(e_1, 0) & \rightarrow & (\overline{(e_1 - e_2)(e_1 - e_3)}, \overline{e_1 - e_2}, \overline{e_1 - e_3}) \\
(e_2, 0) & \rightarrow & (\overline{e_2 - e_1}, \overline{(e_2 - e_1)(e_2 - e_3)}, \overline{e_2 - e_3}) \\
(e_3, 0) & \rightarrow & (\overline{e_3 - e_1}, \overline{e_3 - e_2}, \overline{(e_3 - e_1)(e_3 - e_2)})
\end{array}$$

es un homomorfismo y su nucleo es $2E(\mathbb{Q})$.

Demostración. Empecemos mostrando que ϕ es un homomorfismo, analicemos por casos.

1. Si $P_i = (x_i, y_i) \in E(\mathbb{Q})$, $i = 1, 2, 3$ tales que $y_i \neq 0$ y $P_3 = -(P_1 + P_2)$, como P_1, P_2, P_3 son colineales, entonces sea la recta $y = ax + b$ que contiene a dichos puntos. Definamos el polinomio

   $$P(x) = (x - e_1)(x - e_2)(x - e_3) - (ax + b)^2$$

   Cómo este polinomio se anula en x_1, x_2, x_3 y tiene coeficiente principal 1, entonces podemos escribir

   $$P(x) = (x - e_1)(x - e_2)(x - e_3) - (ax + b)^2 = (x - x_1)(x - x_2)(x - x_3)$$

   Evaluando en cada e_i con $i = 1, 2, 3$ tenemos

   $$(x_1 - e_i)(x_2 - e_i)(x_3 - e_i) = (ae_i + b)^2 \in (\mathbb{Q}^*)^2, \; i = 1, 2, 3$$

de ahi que

$$\overline{(x_1 - e_i)}\,\overline{(x_2 - e_i)}\,\overline{(x_3 - e_i)} = \overline{1},\ i = 1, 2, 3.$$

Luego tenemos que

$$\phi(P_1)\phi(P_2)\phi(P_3) = (\overline{1}, \overline{1}, \overline{1}) \in (\mathbb{Q}^x/\mathbb{Q}^{x^2}) \bigoplus (\mathbb{Q}^x/\mathbb{Q}^{x^2}) \bigoplus (\mathbb{Q}^x/\mathbb{Q}^{x^2})$$

Como $\phi(P_3)$ es congruente a su inverso multiplicativo módulo cuadrados

$$\phi(P_3)^{-1} = \phi(P_3) = \phi(-P_3).$$

Por lo tanto

$$\phi(P_1)\phi(P_2) = \phi(-P_3) = \phi(P_1 + P_2).$$

2. Si $P_1 = (x_1, 0)$ y $P_2 = (x_2, y_2)$ con $y_2 \neq 0$. Entonces $P_3 = -(P_1 + P_2) = (x_3, y_3)$, con $y_3 \neq 0$, por lo anterior tenemos que $\phi(P_2 + P_3) = \phi(P_2)\phi(P_3)$, reemplazando $P_3 = -(P_1 + P_2)$ tenemos que

$$\begin{aligned} \phi(-P_1) &= \phi(P_2 + -(P_1 + P_2)) \\ &= \phi(P_2)\phi(-(P_1 + P_2)) \end{aligned}$$

Por lo tanto

$$\phi(P_1 + P_2) = \phi(P_1)\phi(P_2)$$

3. Si $P_1 = \mathcal{O}$ y $P_2 \neq \mathcal{O}$, tenemos que

$$\phi(P_1 + P_2) = \phi(P_2) = (\overline{1}, \overline{1}, \overline{1})\phi(P_2) = \phi(P_1)\phi(P_2)$$

El caso en que $P_2 = \mathcal{O}$ y $P_1 \neq \mathcal{O}$ es similar.

4. Si $P_1 = (x_1, 0)$ y $P_2 = (x_2, 0)$, como $x_i \in \{e_1, e_2, e_3\}$ entonces podemos considerar $P_1 = (e_1, 0)$ y $P_2 = (e_2, 0)$, así tenemos que

$$\begin{aligned} \phi(P_1) &= (\overline{(e_1 - e_2)(e_1 - e_3)}, \overline{e_1 - e_2}, \overline{e_1 - e_3}) \\ \phi(P_2) &= (\overline{e_2 - e_1}, \overline{(e_2 - e_1)(e_2 - e_3)}, \overline{e_2 - e_3}) \end{aligned}$$

Por lo tanto

$$\phi(P_1)\phi(P_2) = (\overline{(e_1 - e_2)(e_1 - e_3)(e_2 - e_1)}, \overline{(e_1 - e_2)(e_2 - e_1)(e_2 - e_3)}, \overline{(e_1 - e_3)(e_2 - e_3)})$$

Como $P_1 + P_2 = P_3$, tenemos que

$$\phi(P_1 + P_2) = (\overline{e_1 - e_3}, \overline{e_2 - e_3}, \overline{(e_1 - e_3)(e_2 - e_3)})$$

Por lo tanto ϕ es un homomorfismo, veamos ahora que $ker(\phi) = 2E(\mathbb{Q})$.

1. $2E(\mathbb{Q}) \subset ker(\phi)$: Sea $P \in 2E(\mathbb{Q})$ entonces existe $Q \in E(\mathbb{Q})$ tal que $P = 2Q$, entonces
$$\phi(P) = \phi(Q+Q) = \phi(Q)\phi(Q) = \overline{1}$$
De ahí que $P \in ker(\phi)$. Por lo tanto
$$2E(\mathbb{Q}) \subset ker(\phi)$$

2. $ker(\phi) \subset 2E(\mathbb{Q})$: Sea $P = (x, y) \in ker(\phi)$, entonces
$$x - e_i = v_i^2,\ i = 1, 2, 3.$$
Por simplicidad, asumamos que $e_1+e_2+e_3 = 0$, lo que significa que la ecuación para nuestra curva elíptica tiene la forma $y^2 = x^3+Ax+B$. (Si $e_1+e_2+e_3 \neq 0$, el coeficiente de x^2 es diferente de cero. Haciendo un cambio de variables tenemos lo siguiente). Sea
$$f(T) = u_0 + u_1T + u_2T^2$$
tal que $f(e_i) = v_i$, $i = 1, 2, 3$. Para probar la existencia de f es suficiente tomar:
$$f(T) = v_1\frac{1}{(e_1-e_2)(e_1-e_3)}(T-e_2)(T-e_3)+v_2\frac{1}{(e_2-e_1)(e_2-e_3)}(T-e_1)(T-e_3)$$
$$+\ v_3\ \tfrac{1}{(e_3-e_1)(e_3-e_2)}\ (T-e_1)(T-e_2)$$
Definamos $g(T) = x - T - f(T)^2$ tal que cumple $g(e_i) = 0, i = 1, 2, 3$, así
$$T^3 + AT + B = (T-e_1)(T-e_2)(T-e_3)\, divide\, a\, g(T)$$
Por lo tanto $g(T) \equiv 0\,(mod\, T^3 + AT + B)$, así
$$x - T \equiv (u_0 + u_1T + u_2T^2)^2\, mod(\, T^3 + AT + B).$$
Sabemos
$$T^3 \equiv -AT - B\,(mod\, T^3 + AT + B)$$
$$T^4 \equiv T \cdot T^3 \equiv -AT^2 - BT\,(mod\, T^3 + AT + B).$$

Por lo tanto

$$\begin{aligned} x - T &\equiv (u_0 + u_1 T + u_2 T^2)^2 \\ &\equiv u_0^2 + 2u_0u_1T + (u_1^2 + 2u_0u_2)T^2 + 2u_1u_2T^3 + u_2^2T^4 \\ &\equiv (u_0^2 - 2Bu_1u_2) + (2u_0u_1 - 2Au_1u_2 - Bu_2^2)T \\ &\quad +(u_1^2 + 2u_0u_2 - Au_2^2)T^2. \end{aligned}$$

Sabemos que si dos polinomios P_1 y P_2 de grado a los más 2 son congruentes módulo un polinomio de grado 3, entonces la diferencia $P_1 - P_2$ es un polinomio de grado a lo más 2 que es divisible por un polinomio de grado 3. Esto significa que $P_1 = P_2$. Por lo tanto

$$x = u_0^2 - 2Bu_1u_2 \tag{3.2}$$

$$-1 = 2u_0u_1 - 2Au_1u_2 - Bu_2^2 \tag{3.3}$$

$$0 = u_1^2 + 2u_0u_2 - Au_2^2. \tag{3.4}$$

Si $u_2 = 0$, reemplazando en (3.4) tenemos que también $u_1 = 0$. Entonces $f(T)$ es constante, así $v_1 = v_2 = v_3$. Esto significa que $e_1 = e_2 = e_3$, lo cual es una contradicción. Por lo tanto $u_2 \neq 0$, multiplicando (3.4) por u_1/u_2^3 y multiplicando otra vez a la misma ecuación (3.4) por $1/u_2^2$, restando las nuevas ecuaciones obtenemos

$$(\frac{1}{u_2})^2 = (\frac{u_1}{u_2})^3 + A(\frac{u_1}{u_2}) + B.$$

Sea

$$x_1 = \frac{u_1}{u_2},\ y_1 = \frac{1}{u_2}$$

así $(x_1, y_1) \in E(\mathbb{Q})$. Afirmamos que $2(x_1, y_1) = \pm(x, y)$.
De la ecuación (3.4) tenemos que

$$u_0 = \frac{Au_2^2 - u_1^2}{2u_2} = \frac{A - x_1^2}{2y_1}.$$

Reemplazando esto en (3.2) tenemos

$$x = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4y_1^2}.$$

Esta es la primera coordenada de $2(x_1, y_1)$ por (2.7). La segunda coordenada esta determinada por la primera coordenada, así $2(x_1, y_1) = (x, \pm y) = \pm(x, y)$. Por lo tanto $(x, y) = 2(x_1, y_1)$ ó $2(x_1, -y_1)$. En ambos casos tenemos que $(x, y) \in 2E(\mathbb{Q})$.

□

Teorema 3.2. *(El teorema débil de Mordell-Weil para curvas definidas sobre $\mathbb{Q}$) Sea E una curva elíptica definida sobre $\mathbb{Q}$ por*

$$y^2 = x^3 + Ax + B, \text{ con } A, B \in \mathbb{Z}$$

y sean las raíces $e_1, e_2, e_3 \in \mathbb{Q}$ de $p(x) = x^3 + Ax + B$. Entonces

$$E(\mathbb{Q})/2E(\mathbb{Q})$$

es un grupo finito.

Demostración. Como $e_1, e_2, e_3 \in \mathbb{Q}$, haciendo un cambio de variable podemos asumir que $e_1, e_2, e_3 \in \mathbb{Z}$. Del homomorfimo dado en el teorema 3.1 tenemos el homomorfimo inyectivo inducido

$$\begin{array}{rccc} \hat{\phi}: & E(\mathbb{Q})/2E(\mathbb{Q}) & \rightarrow & (\mathbb{Q}^x/\mathbb{Q}^{x^2}) \bigoplus (\mathbb{Q}^x/\mathbb{Q}^{x^2}) \bigoplus (\mathbb{Q}^x/\mathbb{Q}^{x^2}) \\ & \overline{(x,y)} & \rightarrow & \hat{\phi}(\overline{(x,y)}) = \phi((x,y)) \end{array}$$

Por el teorema fundamental de homomorfismo de grupos, tenemos que

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \hat{\phi}(E(\mathbb{Q})/2E(\mathbb{Q})).$$

Para probar que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito es suficiente probar que $\hat{\phi}(E(\mathbb{Q})/2E(\mathbb{Q}))$ es finito, sea $(\overline{a}, \overline{b}, \overline{c}) \in \hat{\phi}(E(\mathbb{Q})/2E(\mathbb{Q}))$, (donde a,b,c son enteros libres de cuadrados), entonces existe $P = (x, y) \in E(\mathbb{Q})$ tal que

$$\hat{\phi}(\overline{(x,y)}) = \phi((x,y)) = (\overline{a}, \overline{b}, \overline{c}).$$

Ahora si $p|a$, entonces $p|abc$, así $p \in S$ con

$$S = \{p \in \mathbb{Z}/p \, es \, primo \, y \, p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

Como S es finito, existe solamente finitos a, b, c módulo cuadrados. Por lo tanto $\hat{\phi}(E(\mathbb{Q})/2E(\mathbb{Q}))$ es finito, lo cual probaría el teorema. □

3.2. Caso general del teorema débil de Mordell

Teorema 3.3. *(Caso general del teorema débil de Mordell-Weil) Sea E una curva elíptica definida sobre $\mathbb{Q}$ por*

$$y^2 = x^3 + Ax + B, \text{ con } A, B \in \mathbb{Z}$$

y sea K el cuerpo de descomposición del polinomio cúbico $p(x) = x^3 + Ax + B$ con raíces $e_1, e_2, e_3 \in K$. Entonces

$$E(\mathbb{Q})/2E(\mathbb{Q})$$

es un grupo finito.

Demostración. Para probar el caso general, la idea es imitar el caso particular reemplazando $\mathbb{Q}$ por K, con lo cual tendremos 3 problemas:

1. Vamos a obtener información de $E(K)/2E(K)$ y nosotros queremos obtener $E(\mathbb{Q})/2E(\mathbb{Q})$, para ello necesitamos hallar una relación entre ellos.

2. Para poder conseguir que $E(\mathbb{Q})/2E(\mathbb{Q})$ sea finito en el teorema anterior usamos el hecho de que el conjunto S definido en la proposición 3.1 sea finito, pero para ello se uso la factorización única en $\mathbb{Z}$. Esto podría fallar en el anillo de enteros algebraicos A_K que reemplazará a $\mathbb{Z}$.

3. Como todo elemento de $\mathbb{Q}^x/\mathbb{Q}^{x^2}$, se representa como ± 1 veces un producto de primos distintos (ver 3.1) y ± 1 representa las unidades en $\mathbb{Z}$, estas unidades necesitan ser controladas en el anillo que reemplaza a $\mathbb{Z}$ en el caso general.

El siguiente teorema nos ayudará a cubrir la parte 1).

Teorema 3.4. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ por*

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

Sea K el cuerpo de descomposición de $p(x) = (x - e_1)(x - e_2)(x - e_3) \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$. Entonces el homomorfismo canónico

$$\begin{array}{rccc} \varphi: & E(\mathbb{Q})/2E(\mathbb{Q}) & \to & E(K)/2E(K) \\ & P + 2E(\mathbb{Q}) & \to & P + 2E(K) \end{array}$$

tiene como número de elementos en su núcleo una cantidad menor ó igual a $2^{2[K:\mathbb{Q}]}$. En consecuencia si $E(K)/2E(K)$ es finito entonces $E(\mathbb{Q})/2E(\mathbb{Q})$ también lo sería.

Demostración. Sea $P \in ker(\varphi)$ entonces $P \in E(\mathbb{Q}) \cap 2E(K)$. Como $P \in 2E(K)$ existe un punto $Q_P \in E(K)$ tal que $P = 2Q_P$. Para cada $P \in ker(\varphi)$, definamos la función

$$\begin{array}{rccc} \lambda_P : & Gal(K/\mathbb{Q}) & \to & E[2] \\ & \sigma & \to & Q_P^\sigma - Q_P \end{array}$$

con

$$E[2] = \{P \in E(K) : 2P = \mathcal{O}\}.$$

Esta función esta bien definida, ya que la imagen de λ_P se encuentra en $E[2]$, veamos

$$2(Q_P^\sigma - Q_P) = 2(Q_P^\sigma) - 2Q_P = P^\sigma - P = \mathcal{O}$$

Veamos que si $\lambda_P = \lambda_{P'}$ entonces $P' \in P + 2E(\mathbb{Q})$.
Como $\lambda_P = \lambda_{P'}$ entonces

$$Q_P^\sigma - Q_P = \lambda_P = \lambda_{P'} = Q_{P'}^\sigma - Q_{P'} \, para \, todo \, \sigma \in Gal(K/\mathbb{Q})$$

de ahí que

$$(Q_{P'} - Q_P)^\sigma = Q_{P'} - Q_P.$$

Por otro lado como K es una extensión normal de $\mathbb{Q}$ entonces $K^{Gal(K/\mathbb{Q})} = \mathbb{Q}$. Por lo tanto $Q_{P'} - Q_P \in E(\mathbb{Q})$. De ahí que

$$P' - P = 2(Q_{P'} - Q_P) \in 2E(\mathbb{Q})$$

Como cada elemento $P \in ker(\varphi)$ podemos asociarlo a λ_P y para cada elemento diferente del núcleo tenemos una función diferente λ_P de $Gal(K/\mathbb{Q})$ a $E[2]$, de ahí que el orden de el núcleo es menor ó igual al número de funciones de $Gal(K, \mathbb{Q})$ a $E[2]$, el cual es

$$4^{|Gal(K,\mathbb{Q})|} = 2^{2[K:\mathbb{Q}]}.$$

□

Ahora veamos como resolver los problemas 2) y 3), empecemos viendo unos ejemplos.

Ejemplo 3.2.1. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por

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

El cuerpo de descomposición es $K = \mathbb{Q}(i)$. El anillo de enteros $A_K = \mathbb{Z}[i]$ es un dominio de factorización única y su grupo de unidades es $\{(i)^k\}_{k=0}^3 \cong \mathbb{Z}_4$

Ejemplo 3.2.2. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por

$$y^2 = x^3 - 2x$$

El cuerpo de descomposición es $K = \mathbb{Q}(\sqrt{2})$. El anillo de enteros $A_K = \mathbb{Z}[\sqrt{2}]$ es un dominio de factorización única, y su grupo de unidades es el grupo infinito $\{\pm(1 \pm \sqrt{2})^k\}_{k=-\infty}^{\infty}$.

Ejemplo 3.2.3. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por

$$y^2 = x^3 + 5x$$

El cuerpo de descomposición es $K = \mathbb{Q}(\sqrt{-5})$. El anillo de enteros algebraicos $A_K = \mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única, ya que $2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ es más estos números son todos primos. El grupo de unidades es $\{\pm 1\} \cong \mathbb{Z}_2$.

En los dos primeros ejemplos $\mathbb{Z}[\sqrt{-1}]$ y $\mathbb{Z}[\sqrt{2}]$ son dominios de factorización única. Así tenemos que

$$\frac{K^x}{K^{x^2}} = \{\overline{U(_K)}\} \oplus \{\overline{p_1^a}\overline{p_2^b} \ldots / a, b, \ldots \in \{0, 1\}\} \tag{3.5}$$

donde $U(_K)$ es el grupo de unidades de A_K y $p_1, p_2, \ldots$ son primos en A_K. En el tercer ejemplo vemos que $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única, sin embargo si hacemos $M = \{1, 2, 2^2, 2^3, \ldots\}$ y definamos

$$R = M^{-1}\mathbb{Z}[\sqrt{-5}]$$

entonces R es un anillo con $\mathbb{Z}[\sqrt{-5}] \subseteq R \subseteq K$, esto hace que R tenga las siguientes propiedades

1. R es un dominio de ideales principales por lo tanto un dominio de factorización única.

2. El grupo de unidades de R es finitamente generado (con 1 y $\frac{1}{2}$ como generadores).

   Como R contiene a $\mathbb{Z}[\sqrt{-5}]$, el cuerpo cociente de R está en K, ya que es el menor cuerpo que contiene a R. Por factorización única (3.5) es válido si nosotros interpretamos las unidades y primos como unidades y primos en R

Teorema 3.5. *Sea $K|\mathbb{Q}$ una extensión finita. Sea A_K el anillo de enteros algebraicos de K sobre $\mathbb{Q}$. Entonces existe un anillo R con $A_K \subseteq R \subseteq K$, tal que:*

1. *R es un dominio de ideales principales, por tanto un dominio de factorización única.*

2. *El grupo de unidades de R es finitamente generado.*

Demostración. Consultar [1, pág 122-129]. □

Ahora veamos veamos la modificación de la proposición 3.1 y teorema 3.1 para el caso general:

Proposición 3.2. *Sea*

$$S = \{p \in R/p\, es\, primo\, y\, p|(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}$$

Si p es primo y $p|abc$, entonces $p \in S$

Demostración. La prueba es similar al de la proposición 3.1. □

Teorema 3.6. *Sea E una curva elíptica dada por $y^2 = (x - e_1)(x - e_2)(x - e_3)$, definida sobre $\mathbb{Q}$, con $e_1, e_2, e_3 \in R$. La función definida por*

$$\begin{array}{rccc} \phi: & E(K) & \to & (K^x/K^{x^2}) \bigoplus (K^x/K^{x^2}) \bigoplus (K^x/K^{x^2}) \\ & (x,y) & \to & (\overline{x-e_1}, \overline{x-e_2}, \overline{x-e_3})\, con\, y \neq 0 \\ & \infty & \to & (\overline{1}, \overline{1}, \overline{1}) \\ & (e_1,0) & \to & (\overline{(e_1-e_2)(e_1-e_3)}, \overline{e_1-e_2}, \overline{e_1-e_3}) \\ & (e_2,0) & \to & (\overline{e_2-e_1}, \overline{(e_2-e_1)(e_2-e_3)}, \overline{e_2-e_3}) \\ & (e_3,0) & \to & (\overline{e_3-e_1}, \overline{e_3-e_2}, \overline{(e_3-e_1)(e_3-e_2)}) \end{array}$$

es un homomorfismo. El nucleo de ϕ es $2E(\mathbb{K})$.

Reemplazando $\mathbb{Q}$ por K en la prueba del teorema 3.2 tenemos, $e_1, e_2, e_3 \in K = frac(R)$, haciendo un cambio de variables podemos asumir que $e_1, e_2, e_3 \in R$. Del homomorfimo dado en el teorema anterior tenemos el homomorfimo inyectivo inducido

$$\begin{array}{rccc} \hat{\phi}: & E(K)/2E(K) & \to & (K^x/K^{x^2}) \bigoplus (K^x/K^{x^2}) \bigoplus (K^x/K^{x^2}) \\ & \overline{(x,y)} & \to & \hat{\phi}(\overline{(x,y)}) = \phi((x,y)) \end{array}$$

Por el teorema de homomorfimo de grupos tenemos que

$$E(K)/2E(K) \cong \hat{\phi}(E(K)/2E(K))$$

Para probar $E(K)/2E(K)$ es finito es suficiente probar que $\hat{\phi}(E(K)/2E(K))$ es finito, sea $(\overline{a}, \overline{b}, \overline{c}) \in \hat{\phi}(E(K)/2E(K))$ (donde a,b,c son enteros libres de cuadrados), entonces existe $P = (x, y) \in E(K)$ tal que

$$\hat{\phi}((\overline{x, y})) = \phi((x, y)) = (\overline{a}, \overline{b}, \overline{c})$$

Por la proposición 3.2 tenemos que los primos de R que dividen a a, b, c también dividen a $(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. Entonces la imagen de ϕ esta contenida en el grupo generado por S y las unidades de R. Como ambos son finitos tenemos que $\hat{\phi}(E(K)/2E(K))$ es finito, lo cuál probaría el teorema. Por el teorema 3.4 tenemos que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. □

3.3. El teorema de Mordell

Hasta el momento hemos probado que $E(\mathbb{Q})/2E(\mathbb{Q})$ es un grupo cociente finito, lo cuál no es suficiente para decir que $E(\mathbb{Q})$ sea finitamente generado, por ejemplo $\mathbb{R}/2\mathbb{R} = \{\overline{0}\}$ es finito, pero $\mathbb{R}$ no es finitamente generado. Veamos la siguiente definición que nos ayudará a conseguir nuestro objetivo.

Definición 3.3.1. *Sea $x = a/b \in \mathbb{Q}$, con $mcd(a, b) = 1$. Definamos*

$$\begin{aligned} \widetilde{H}(x) &= \text{máx}(|a|, |b|) \quad (\textbf{\textit{altura}}\ de\, a/b) \\ \widetilde{h}(x) &= log\widetilde{H}(a/b) \quad (\textbf{\textit{altura logarítmica}}\ de\, a/b). \end{aligned}$$

Definición 3.3.2. *Sea $P = (x, y) \in E(\mathbb{Q})$, con $P \neq \mathcal{O}$. Definamos*

$$\begin{aligned} H(x, y) &= \widetilde{H}(x) \quad (\textbf{\textit{altura}}\ de\, (x, y)) \\ h(x, y) &= \widetilde{h}(x) \quad (\textbf{\textit{altura logarítmica}}\ de\, (x, y)). \end{aligned}$$

Si $P = \mathcal{O}$, entonces $H(P) = 1$

Teorema 3.7. *Existe una constante c_1 tal que*

$$|h(P + Q) + h(P - Q) - 2h(P) - 2h(Q)| \leq c_1$$

para todo $P, Q \in E(\mathbb{Q})$

Demostración. Afirmamos que existen constantes c' y c'' tales que:

$$2h(P) + 2h(Q) - c' \leq h(P+Q) + h(P-Q) \tag{3.6}$$

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c'' \tag{3.7}$$

Empezaremos probando la segunda desigualdad, sea una curva elíptica E dada por $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Sean

$$P = (\frac{a_1}{b_1}, y_1),\ Q = (\frac{a_2}{b_2}, y_2)$$

$$P+Q = (\frac{a_3}{b_3}, y_3),\ P-Q = (\frac{a_4}{b_4}, y_4)$$

con $P, Q \in E(\mathbb{Q})$ y $a_i, b_i \in \mathbb{Z}$ tal que $mcd(a_i, b_i) = 1$, para $i = 1, 2, 3, 4$. Como vimos anteriormente para la adición de dos puntos tenemos:

$$\frac{a_3}{b_3} = m_1^2 - \frac{a_1}{b_1} - \frac{a_2}{b_2} = \ con\ m_1 = \frac{y_2 - y_1}{\frac{a_2}{b_2} - \frac{a_1}{b_1}}$$

$$\frac{a_4}{b_4} = m_2^2 - \frac{a_1}{b_1} - \frac{a_2}{b_2} = \ con\ m_2 = \frac{-y_2 - y_1}{\frac{a_2}{b_2} - \frac{a_1}{b_1}}$$

Sumando y luego multiplicando ambas expresiones obtenemos:

$$\frac{a_3}{b_3} + \frac{a_4}{b_4} = \frac{g_1}{g_3},\ \ \frac{a_3 a_4}{b_3 b_4} = \frac{g_2}{g_3}$$

con

$$\begin{aligned} g_1 &= 2(a_1b_2 + a_2b_1)(Ab_1b_2 + a_1a_2) + 4Bb_1^2b_2^2 \\ g_2 &= (a_1a_2 - Ab_1b_2)^2 - 4B(a_1b_2 + a_2b_1)b_1b_2 \\ g_3 &= (a_1b_2 - a_2b_1) \end{aligned}$$

Para continuar con la prueba veamos antes dos lemas.

Lema 3.1. *Sean $c_1, c_2, d_1, d_2 \in \mathbb{Z}$. Se cumple:*

$$\text{máx}(|c_1|, |d_1|) \leq 2\,\text{máx}(|c_1c_2|, |c_1d_2 + c_2d_1|, |d_1d_2|).$$

Demostración. Supongamos que $|c_1| \leq |d_1|$, si no fuese así cambiamos los lugares. Sea L la parte izquierda de la desigualdad del lema y R la parte derecha. Entonces tendríamos 3 casos:

1. Si $|c_2| \leq |d_2|$, entonces $L = |d_1d_2|$ y $2|d_1d_2| \leq R$, así $L \leq R$.

2. Si $|c_2| \geq |d_2| \geq (1/2)|c_2|$, entonces $L = |d_1c_2|$ y $R \geq 2|d_1d_2| \geq |d_1c_2| \geq L$.

3. Si $|d_2| \leq (1/2)|c_2|$, entonces $L = |d_1 c_2|$ y

$$\begin{aligned} R &\geq 2|c_1 d_2 + c_2 d_1| \\ &\geq 2(|c_2 d_1| - |c_1 d_2|) \\ &\geq 2(|c_2 d_1| - |d_1|(1/2)|c_2|) \\ &= |c_2 d_1| = L \end{aligned}$$

Esto completaría la prueba. □

Lema 3.2. *Sean $c_1, c_2, d_1, d_2 \in \mathbb{Z}$, con $mcd(c_i, d_i) = 1$ para $i = 1, 2$. Se cumple*

$$mcd(c_1 c_2, c_1 d_2 + c_2 d_1, d_1 d_2) = 1$$

Demostración. Sea $d = mcd(c_1 d_2 + c_2 d_1, d_1 d_2)$. Supongamos que p es un primo tal que $p \mid c_1$ y $p \mid d$. Como $mcd(c_1, d_1) = 1$, entonces $p \nmid d_1$ Además $p \nmid d_1 d_2$, entonces $p \nmid d_2$. Por lo tanto $p \nmid c_2$, así tendríamos que $p \mid c_1 d_2$ y $p \nmid c_2 d_1$, así $p \nmid c_1 d_2 + c_2 d_1$. Por lo tanto $p \nmid d$, lo cuál sería una contradicción. De igual manera no existe un primo p que divida a c_2 y d. Por lo tanto no existe un primo p que divida a $c_1 c_2$ y d, lo cuál probaría el lema. □

Continuando con la prueba del teorema por el lema anterior, como $mcd(a_3, b_3) = 1$ y $mcd(a_4, b_4) = 1$, tenemos que

$$mcd(a_3 a_4, a_3 b_4 + a_4 b_3, b_3 b_4) = 1.$$

Por lo tanto existen $x, y, z \in \mathbb{Z}$ tales que

$$a_3 a_4 x + (a_3 b_4 + a_4 b_3) + b_3 b_4 = 1.$$

Como

$$g_3(a_3 b_4 + a_4 b_3) = g_1(b_3 b_4) \, y \, g_3(a_3 a_4) = g_2(b_2 b_4), \tag{3.8}$$

tenemos que

$$\begin{aligned} g_3 &= g_3(a_3 a_4)x + g_3(a_3 b_4 + a_4 b_3)y + g_3(b_3 b_4)z \\ &= g_2(b_3 b_4)x + g_1(b_3 b_4)y + g_3(b_3 b_4)z. \end{aligned}$$

Por lo tanto $b_3 b_4 \mid g_3$, así

$$|b_3 b_4| \leq |g_3|.$$

Similarmente tenemos que

$$|a_3 a_4| \leq |g_2|.$$

De la ecuación (3.8) y como $|b_3 b_4| \leq |g_3|$ tenemos que

$$|a_3 b_4 + a_4 b_3| \leq |g_1|.$$

En función de la altura H tenemos que

$$\begin{aligned} H(P+Q)H(P-Q) &= \text{máx}(|a_3|, |b_3|)\,\text{máx}(|a_4|, |b_4|) \\ &\leq 2\,\text{máx}(|a_3 a_4|, |a_3 b_4 + a_4 b_3|, |b_3 b_4|) \\ &\leq 2\,\text{máx}(|g_2|, |g_1|, |g_3|). \end{aligned}$$

Sean $H_1 = \text{máx}(|a_1|, |b_1|)$ y $H_2 = \text{máx}(|a_2|, |b_2|)$. Entonces

$$\begin{aligned} |g_1| &= |2(a_1 b_2 + a_2 b_1)(A b_1 b_2 + a_1 a_2 + 4B b_1^2 b_2^2)| \\ &\leq 2(H_1 H_2 + H_2 H_1)(|A| H_1 H_2 + H_1 H_2) + 4|B| H_1^2 H_2^2 \\ &\geq 4(|A| + 1 + |B|) H_1^2 H_2^2. \end{aligned}$$

Similarmente

$$|g_2| \leq ((1 + |A|)^2 + 8|B|) H_1^2 H_2^2,\ g_3 \leq 4 H_1^2 H_2^2.$$

Por lo tanto

$$H(P+Q)H(P-Q) \leq C H_1^2 H_2^2 = C H(P)^2 H(Q)^2,$$

tomando logaritmo a la desigualdad

$$log(H(P+Q)H(P-Q)) \leq log(C H_1^2 H_2^2) = log(C H(P)^2 H(Q)^2),$$

tenemos para alguna constante c''

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c''. \tag{3.9}$$

Lo cuál probaría la ecuación (3.7). Ahora probemos la ecuación (3.6), primero veamos un lema que nos ayudará en nuestra prueba. □

Lema 3.3. *Sea $\Delta = 4A^3 + 27B^2$ y sean los polinomios*

$$\begin{aligned} F(x,z) &= x^4 - 2Ax^2 z^2 - 8Bxz^3 + A^2 z^4 \\ G(x,z) &= 4z(x^3 + Axz^2 + Bz^3). \end{aligned}$$

Entonces existen $f_1, f_2, g_1, g_2 \in \mathbb{Z}[x,z]$, polinomios homogéneos de grado 3, tales que

$$F f_1 - G g_1 = 4\Delta z^7 \text{ y } F f_2 + G g_2 = 4\Delta x^7.$$

Demostración. Reemplazando $z = 1$ en $F(x, z)$ y $G(x, z)$, tenemos

$$\begin{aligned} F(x,1) &= x^4 - 2Ax^2 - 8Bx + A^2 \\ G(x,1) &= 4(x^3 + Ax + B). \end{aligned}$$

Dividiendo $F(x, 1)$ entre $G(x, 1)$, tenemos que

$$F(x,1) = G(x,1)(\frac{1}{4}x) + (-3Ax^2 - 9Bx + A^2)$$

despejando $G(x, 1)$ tenemos que

$$G(x,1) = \frac{4}{x}(F(x,1) + 3Ax^2 + 9Bx - A^2), \text{ con } A \neq 0$$

$$= (-3Ax^2 - 9Bx + A^2)(-\frac{4}{3A} + \frac{4B}{A^2}) + (\frac{4\Delta}{3A^2}x), \text{ con } A \neq 0.$$

De ahí que

$$(-3Ax^2 - 9Bx + A^2) = (\frac{4\Delta}{3A^2}x)(-\frac{9A^3}{4\Delta}x) + (-9Bx + A^2)$$

$$(\frac{4\Delta}{3A^2}x) = (-9Bx + A^2)(-\frac{4\Delta}{27BA^2}) + \frac{4\Delta}{27B}, \text{ con } A, B \neq 0$$

Por lo tanto

$$4\Delta = (12x^2 + 16A)F(x,1) + (-3x^3 + 5Ax + 27B)G(x,1). \tag{3.10}$$

Reemplazando x por $\frac{x}{z}$ en (3.10) tenemos

$$4\Delta = (12\frac{x^2}{z^2} + 16A)F(\frac{x}{z}, 1) + (-3\frac{x^3}{z^3} + 5A\frac{x}{z} + 27B)G(\frac{x}{z}, 1). \tag{3.11}$$

Como $F(x, z)$ y $G(x, z)$ son polinomios homogéneos de grado 4, multiplicando a (3.11) por z^7 tenemos

$$4\Delta z^7 = (12x^2z + 16Az^3)F(x,z) + (-3x^3 + 5Axz^2 + 27Bz^3)G(x,z).$$

Haciendo $f_1(x, z) = 12x^2z + 16Az^3$ y $g_1(x, z) = -3x^3 + 5Axz^2 + 27Bz^3$ tenemos el resultado requerido. Similarmente se puede obtener

$$\begin{aligned} f_2 &= 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^2 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3 \\ g_2 &= A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 - 3A^2(A^2 + 8B^2)z^3, \end{aligned}$$

tales que

$$Ff_2 + Gg_2 = 4\Delta x^7.$$

□

Lema 3.4. *Sea $R \in E(\mathbb{Q})$.Existe una constante C_2, independiente de R que cumple*

$$4h(R) \leq h(2R) + C_2.$$

Demostración. Sea

$$R = (\frac{a}{b}, y)$$

con $y \in \mathbb{Q}$ y $a, b \in \mathbb{Z}$, con $mcd(a, b) = 1$. Definamos

$$\begin{aligned} h_1 &= a^4 - 2Aa^2b^2 - 8Bab^3 + A^2b^4 \\ h_2 &= (4b)(a^3 + Aab^2 + Bb^3) \\ \Delta &= 4A^3 + 27B^2. \end{aligned}$$

Por el lema anterior, existen polinomios homogéneos $r_1, r_2, s_1, s_2 \in \mathbb{Z}[a, b]$ de grado 3 tales que

$$4\Delta b^7 = r_1h_1 + r_2h_2 \tag{3.12}$$

$$4\Delta a^7 = s_1h_1 + s_2h_2 \tag{3.13}$$

Para un polinomio homogéneo de grado 3 de la forma

$$p(x, y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3$$

tenemos

$$|p(a, b)| \leq (|c_0| + |c_1| + |c_2| + |c_3|)\,\text{máx}(|a|, |b|)^3.$$

Supongamos que $|b| \geq |a|$, de ahí que

$$\begin{aligned} |4\Delta||b|^7 &\leq |r_1(a, b)||h_1| + |r_2(a, b)||h_2| \\ &\leq c_1|b|^3\,\text{máx}(|h_1|, |h_2|), \end{aligned}$$

para algún c_1 constante. Por lo tanto

$$|4\Delta||b|^4 \leq c_1\,\text{máx}(|h_1|, |h_2|).$$

Sea $d = mcd(h_1, h_2)$. Entonces por (3.12) y (3.13) tenemos que

$$d|4\Delta b^7 \ y \ d|4\Delta a^7.$$

Como $mcd(a, b) = 1$, tenemos que $d|4\Delta$, así $d \leq |4\Delta|$, por otro lado, como

$$H(2R) = \text{máx}(\frac{|h_1|}{d}, \frac{|h_2|}{d}),$$

tenemos que

$$\begin{aligned} |4\Delta|H(R)^4 &= |4\Delta||b|^4 \\ &\leq c_1 \,\text{máx}(|h_1|, |h_2|) \\ &\leq c_1|4\Delta| \,\text{máx}(|h_1|/d, |h_2|/d) \\ &\leq c_1|4\Delta|H(2R). \end{aligned}$$

Dividiendo entre 4Δ tenemos que

$$4h(R) \leq h(2R) + C_2$$

para alguna constante c_2. □

Reemplazando P por $P + Q$ en (4.9) tenemos

$$h(2P) + h(2Q) \leq 2h(P + Q) + 2h(P - Q) + c''.$$

Por el lema anterior

$$4h(P) + 4h(Q) - 2c_2 \leq h(2P) + h(2Q).$$

Por lo tanto

$$2h(P) + 2h(Q) - c' \leq h(P + Q) + h(P - Q)$$

para alguna constante c'. Esto completaría la prueba del teorema 3.7.

Teorema 3.8. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Existe una función*

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$$

con las siguientes propiedades:

1. $\hat{h}(P) \geq 0$ para todo $P \in E(\mathbb{Q})$
2. Existe una constante c_1 tal que $|\frac{1}{2}h(P) - \hat{h}(P)| \leq c_1$ para todo P.
3. Dada una constante c, existe solamente una cantidad finita de puntos $P \in E(\mathbb{Q})$, tales que $\hat{h}(P) \leq c$.
4. $\hat{h}(mP) = m^2\hat{h}(P)$, para todo $m \in \mathbb{Z}$ y todo $P \in E(\mathbb{Q})$.
5. $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$, para todo P, Q.
6. $\hat{h}(P) = 0$ si y sólo sí P es un punto de torsión.

Demostración. (1) Haciendo $Q = P$ en el teorema anterior, obtenemos

$$|h(2P) - 4h(P)| \leq c_1, \textit{ para todo } P \in E(\mathbb{Q}). \tag{3.14}$$

Para cada $P \in E(\mathbb{Q})$, definamos

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

Veamos si esta bien definida, para ello probemos la existencia del límite. Tenemos

$$\lim_{n\to\infty} \frac{1}{4^n} h(2^n P) = h(P) + \sum_{j=1}^{\infty} \frac{1}{4^j}(h(2^j P) - 4h(2^{j-1}P)). \tag{3.15}$$

Por (4.14) tenemos

$$|\frac{1}{4^j}(h(2^j P) - 4h(2^{j-1}P))| \leq \frac{c_1}{4^j}$$

así la suma infinita converge. Por lo tanto $\hat{h}(P)$ esta bien definida, de ahí que

$$\hat{h}(P) \geq 0 \textit{ para todo } P \in E(\mathbb{Q}).$$

(2) De la parte (1) tenemos que

$$\sum_{j=1}^{\infty} \frac{c_1}{4^j} = \frac{c_1}{3}$$

De ahí que $|\hat{h}(P) - \frac{1}{2}h(P)| \leq c_1/6$.

(3) Si $\hat{h}(P) \leq c$, entonces $h(P) \leq 2c + \frac{c_1}{3}$. Por lo tanto existe una cantidad finita de puntos P que satisfacen esta desigualdad.

(5) Esta propiedad es conocida como la **ley del paralelogramo** debido a que es originada por 0 y los vectores $P, Q, P + Q$ (adición ordinaria de dos vectores), estos puntos son los vértices de un paralelogramo. Sabemos que

$$\frac{1}{4^n}|h(2^n P + 2^n Q) - 2h(2^n P) - 2h(2^n Q)| \leq \frac{c_1}{4^n}.$$

haciendo que $n \to \infty$ tenemos el resultado esperado.

(4) Como la altura depende solamente de la primera coordenada, $\hat{h}(-P) = \hat{h}(P)$. Por lo tanto, asumamos que $m \geq 0$. El caso en que $m = 0, 1$ es trivial. Si

$Q = P$ por la parte (5) tenemos el caso en que $m = 2$. Supongamos que conocemos el resultado para $m-1$ y m. Entonces

$$\hat{h}((m+1)P) = -h((m\hat{-}1)P) + 2\hat{h}(mP) + 2\hat{h}(P)(\textit{por la parte}\,(5))$$

$$= (-(m+1)^2 + 2m^2 + 2)\hat{h}(P) = (m+1)^2\hat{h}(P).$$

Por inducción el resultado es verdadero para todo m.

(6) Si $mP = \infty$, entonces $m^2 = \hat{h}(P) = \hat{h}(mP) = \hat{h}(\infty) = 0$, así $\hat{P} = 0$. Por lo contrario, si $\hat{h}(P) = 0$, entonces $\hat{h}(mP) = m^2\hat{h}(P) = 0$, para todo m. Sabemos que existe una cantidad finita grande de puntos de altura 0, el conjunto de múltiplos de P es finita.Por lo tanto P es un punto de torsión. Esto completa la prueba del teorema.

□

Teorema 3.9. *(Mordell) Sea E una curva definida sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.*

Demostración. Sean los puntos $R_1, ..., R_n \in E(\mathbb{Q})$ representantes de las clases del grupo cociente finito $E(\mathbb{Q})/2E(\mathbb{Q})$. Definamos

$$c = \text{máx}\{\hat{h}(R_i)\} \quad \text{con } i = 1, ...n$$

y sean $\{Q_1, ..., Q_m\}$ el conjunto de puntos en $E(\mathbb{Q})$ tal que $\hat{h}(Q_i) \leq c$. Este es un conjunto finito por el teorema anterior. Definamos

$$G = \langle R_1, ..., R_n, Q_1, ...Q_m \rangle$$

el subgrupo de $E(\mathbb{Q})$ generado por $R_1, ..., R_n, Q_1, ...Q_m$.
Afirmamos que $G = E(\mathbb{Q})$, probemos esta afirmación, procedamos por contradicción, supongamos que existe $P \in E(\mathbb{Q}) \setminus G$. Entonces existe una cantidad finita de puntos de altura menor que la de P, podríamos cambiar P por uno de estos, si fuese necesario, y asumamos que P tiene la altura más pequeña entre todos los puntos que pertencen a $E(\mathbb{Q})$, pero que no están en G. Por otro lado, como $\overline{P} \in E(\mathbb{Q})/2E(\mathbb{Q})$, entonces $\overline{P} = \overline{R_i}$, para algún $i = 1, 2, \ldots, n$. De ahí que

$$P - R_i = 2P_1$$

para algún $i = 1, 2, \ldots, n$ y algún $P_1 \in E(\mathbb{Q})$. Por el Teorema anterior:

$$\begin{aligned} 4\hat{h}(P_1) &= \hat{h}(2P_1) \\ &= \hat{h}(P - R_i) \\ &= 2\hat{h}(P) + 2\hat{h}(R_i) - \hat{h}(P + R_i) \\ &\leq 2\hat{h}(P) + 2c \end{aligned}$$

Como $c < \hat{h}(P)$, ya que $P \neq Q_j$ tenemos que

$$\begin{aligned} 4\hat{h}(P_1) &\leq 2\hat{h}(P) + 2c \\ &< 2\hat{h}(P) + 2\hat{h}(P) \\ &= 4\hat{h}(P). \end{aligned}$$

Por lo tanto

$$\hat{h}(P_1) < \hat{h}(P).$$

Como P tiene la altura más pequeña de puntos en $E(\mathbb{Q})$, pero que no están en G, tenemos que $P_1 \in G$. Por lo tanto

$$P = R_i + 2P_1 \in G.$$

Esto sería una contradicción, por lo tanto $E(\mathbb{Q}) = G$. Esto completaría la prueba del teorema de Mordell. □

Capítulo 4

El grupo de torsión de una curva elíptica sobre $\mathbb{Q}(i)$

En este capítulo final, estudiaremos la parte de torsión de una curva elíptica, para ello veremos el teorema de Lutz-Nagell, que nos permitirá calcular el subgrupo de torsión $E(\mathbb{Q})_{tors}$ de una curva elíptica $E(\mathbb{Q})$, con una serie de ejemplos que nos ayudará a entenderlo mejor, para luego enunciar el teorema de Mazur, que nos caracterizará por completo los subgrupos de torsión de las curvas elípticas definidas sobre los $\mathbb{Q}$. Finalmente veremos el teorema de Lutz-Nagell sobre el cuerpo gaussiano esto quiere decir definiendo la curva sobre una extensión finita $\mathbb{Q}(i)$, para luego enunciar el teorema analogo al de Mazur, conocido como el teorema de Kenku-Momose, que nos caracterizará por completo los subgrupos de torsión de las curvas elípticas definidas sobre los $\mathbb{Q}(i)$

4.1. Puntos de torsión

Sea E una curva elíptica definida sobre un cuerpo K. Para cada n entero positivo. Definamos el conjunto de puntos de torsión de orden n como

$$E[n] = \{P \in E(\overline{K})/nP = \mathcal{O}\}$$

donde $\overline{K}$ es la clausura algebraica de K, además $E[n]$ contiene puntos con coordenadas no sólo en K sino en $\overline{K}$.

Cuando la característica de K no es 2, la curva E puede ser escrito como

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

y es más simple de determinar E_2.
Sea

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

con $e_1, e_2, e_3 \in \overline{K}$. Un punto P satisface $2P = \mathcal{O}$ si y solo si la recta tangente en P es vertical. Esto significa que $y = 0$ así:

$$E_2 = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

Este es isomorfo a $Z_2 \bigoplus Z_2$.

La situación en el que el cuerpo K es de característica 2 es más delicado como se vió en las ecuaciones (2.3) y (2.4), la curva elíptica E puede asumir una de las siguientes ecuaciones:

$$y^2 + xy + x^3 + a_2x^2 + a_6 = 0$$

$$y^2 + a_3y + x^3 + a_4x + a_6 = 0$$

En el primer caso $a_6 \neq 0$ y en el segundo caso $a_3 \neq 0$ (sino las curvas podrían ser singulares). Si $P = (x, y)$ es un punto de orden 2, entonces la tangente en P será vertical, lo que significa que la derivada parcial con respecto a y debe ser igual a 0, de ahí que $2y + x = 0$ y como $car(K) = 2$, por lo tanto $x = 0$. Reemplazando $x = 0$, tenemos que $0 = y^2 + a_6 = (y + \sqrt{a_6})^2$. Por lo tanto $(0, \sqrt{6})^2$ es el único punto de orden 2 (las raíces cuadradas son únicas en un cuerpo de característica 2), así

$$E[2] = \{\mathcal{O}, (0, \sqrt{6})\}$$

Este es isomorfo a Z_2.
En el caso segundo caso, la derivada parcial con respecto a y es $2y + a_3$ y como la característica del cuerpo K es 2 tenemos $a_3 \neq 0$. Por lo tanto este no es un punto de orden 2, así

$$E[2] = \{\mathcal{O}\}$$

En resumen tenemos la siguiente:

Proposición 4.1. *Sea E una curva elíptica sobre un cuerpo K. Si la característica de K no es 2 entonces*

$$E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Si la característica de K es 2 entonces

$$E[2] = 0 \quad ó \quad \mathbb{Z}_2$$

Demostración. Consultar [2,pág 78] □

Ahora veamos que sucede en $E[3]$, para eso asumamos primero que la característica de K no es 2 ó 3, así E puede escribirse como $y^2 = x^3 + Ax + B$. Un punto P satisface que $3P = \mathcal{O}$ si y sólo si $2P = -P$. Esto significa que la coordenada x en $2P$ es igual a las coordenada x de P (y como la curva es simétrica la coordenada y varia en signo). Sabemos que

$$m^2 - 2x = x, \, con \, m = \frac{3x^2 + A}{2y}$$

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

$$(3x^2 + A)^2 = 12x(x^3 + Ax + B)$$

Operando tenemos

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0$$

La discriminante de este polinomio es $-6912(4A^3 + 27B^2)^2 \neq 0$. Por lo tanto el polinomio no tiene raíces múltiples, esto quiere decir que x toma 4 valores distintos en $\overline{K}$, y cada x produce 2 valores de y, así tendríamos 8 puntos de orden 3. Además sabemos que el punto $\mathcal{O}$ también esta en $E[3]$, entonces que $E[3]$ es un grupo de orden 9 en que cada elemento es de torsión 3. Esto quiere decir que

$$E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

Veamos ahora el caso en que la caracterísitica de K es 2. Si la característica de K es 2 la curva E puede tomar dos formas pasaremos a analizar una de ellas la otra es similar, tenemos

$$y^2 + xy + x^3 + a_2x^2 + a_6 = 0, \; con \; a_6 \neq 0$$

sabemos que $x = m^2 + m + a_2$ donde $m = (y + x^2)/x$
Reemplazando en E tenemos

$$x^4 + x^3 + a_6 = 0$$

La discriminante de este polinomio es $256a_6^3 - 27a_6^2 \neq 0$. Por lo tanto el polinomio no tiene raíces múltiples, esto quiere decir que x toma 4 valores distintos en $\overline{K}$ y cada x produce 2 valores de y, así tendríamos 8 puntos de orden 3. Además sabemos que el punto $\mathcal{O}$ también esta en $E[3]$, entonces E es un grupo de orden 9 en el que cada elemento es de torsión 3, esto quiere decir que

$$E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

Ahora veamos el caso en que la característica de $K = 3$, entonces E tiene la forma

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

Nosotros queremos que la primera coordenada de $2P$ sea igual a la primera coordenada de P. Sabemos que

$$m^2 - a_2 = 3x = 0, \ con \ m = (2a_2x + a_4)/2y$$

Reemplazando m tenemos

$$a_2x^3 + a_2a_6 - a_4^2 = 0$$

Afirmamos que a_2 y a_4 no pueden ser ambos cero a la vez, ya que tendríamos que $x^3 + a_6 = (x + a_6^{1/3})^3$ tiene raíces múltiples, lo cual no puede ser, entonces al menos uno de ellos es diferente de cero.
Si $a_2 = 0$, entonces $-a_4^2 = 0$, lo cual no puede ocurrir por lo tanto $E[3] = \{\infty\}$ en este caso.
Si $a_2 \neq 0$, entonces $a_2(x^3 + a) = 0$, que tiene una sola raíz triple. Por lo tanto habría un valor de x que produce dos valores de y, entonces tendríamos dos puntos de orden 3 y como ∞ también pertenece a $E[3]$, vemos que $E[3]$ tiene orden 3, así

$$E[3] \cong \mathbb{Z}_3$$

como grupo abstracto.
La generalización , esta dado en el siguiente teorema.

Teorema 4.1. *Sea E una curva elíptica sobre el cuerpo K y sea n un entero positivo. Si la característica de K no divide a n ó es 0, entonces*

$$E[n] = \mathbb{Z}_n \bigoplus \mathbb{Z}_n$$

Si la característica de K es $p > 0$ y $p \mid n$, tenemos $n = p^r n'$. Entonces

$$E[n] \simeq \mathbb{Z}_{n'} \bigoplus \mathbb{Z}_{n'} \quad o \quad \mathbb{Z}_n \bigoplus \mathbb{Z}_{n'}$$

Demostración. Consultar[2,pag 79-80] □

4.2. El teorema de Lutz-Nagell

Denotaremos $a/b \neq 0$ un número racional, donde a, b son primos relativos enteros, de aqui tenemos que $a/b = p^r a_1/b_1$ con $p \nmid a_1 b_1$.

Definición 4.2.1. *Se define la valuación p-ádica de un número racional como:*

a) $v_p(x) = \text{máx}\{n \in \mathbb{Z} : p^n | x, \, si \, x \in \mathbb{Z} \setminus \{0\}\}$

b) $v_p(q) = v_p(a) - v_p(b), si \, q = a/b \in \mathbb{Q}$

Por convención se toma $v_p(0) = \infty$.

Ejemplo 4.2.1. $v_2(7/40) = -3$, $v_5(50/3) = 2$, *y* $v_7(1/2) = 0$.

Esta definición nos ayuda a probar el teorema siguiente que es la versión original del teorema de Lutz-Nagell:

Teorema 4.2. *(El teorema de Lutz-Nagell) Sea E una curva elíptica dada por $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Sea $P = (x, y) \in E(\mathbb{Q})$ se cumple:*

1. *Si P tiene orden finito entonces $x, y \in \mathbb{Z}$.*

2. *Si P tiene orden finito con $y \neq 0$ entonces $y^2 \mid 4A^3 + 27B^2$.*

El teorema de Lutz-Nagell esta definida sobre curvas elípticas definidas sobre $\mathbb{Q}$ esta versión original es el artifice de que nosotros pensemos si este teorema se cumple con ciertas condiciones para curvas elípticas definidas sobre la extensión $\mathbb{Q}(i)$. Antes de ver ello veamos algunos ejemplos de curvas elípticas definidas sobre $\mathbb{Q}$ y mostremos como funciona.

Ejemplo 4.2.2. Sea la curva elíptica dada por

$$y^2 = x^3 + 4$$

Si $y = 0$ entonces $x^3+4 = 0$, pero esta ecuación no posee soluciones racionales, por lo tanto $y \neq 0$. Sea $P = (x, y) \in E(\mathbb{Q})$ con orden finito entonces $y^2 \mid 4A^3+27B^2 = 432$. Los posibles valores para y son:

$$y = \pm 1, \pm 2 \pm 3 \pm 4 \pm 6 \pm 12.$$

Solamente $y = \pm 2$ produce un valor entero para x, así los posibles puntos de torsión son $(0, 2)$ y $(0, -2)$. Un cálculo rápido muestra que $3(0, \pm 2) = \mathcal{O}$. Por lo tanto el subgrupo de torsión es cíclico de orden 3.

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, -2), (0, 2)\}$$

Ejemplo 4.2.3. Sea la curva elíptica dada por

$$y^2 = x^3 + 8$$

Entonces $4A^3 + 27B^2 = 1728$. Si $y = 0$, entonces $x = -2$. El punto $(-2, 0)$ tiene orden 2. Si $y \neq 0$, entonces $y^2 \mid 1728$, que significa que $y \mid 24$. Trabajando todas las posibilidades obtenemos los puntos $(1, \pm 3)$ y $(2, \pm 4)$. Sin embargo

$$2(1, 3) = (-7/4, -13/8)\, y\, 2(2, 4) = (-7/4, 13/8).$$

Como estos puntos no tienen coordenadas enteras, ellos no pueden tener orden finito. Por lo tanto $(1, 3)$ y $(2, 4)$ no pueden tener orden finito, así tenemos que el subgrupo de torsión es cíclico de orden 2.

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (-2, 0)\}$$

Ejemplo 4.2.4. Sea la curva elíptica dada por

$$y^2 = x^3 - 43x + 166$$

Entonces $4A^3 + 27B^2 = 425984$. Si $y = 0$ el x no toma valores enteros. Si $y \neq 0$ entonces $y^2 \mid 2^{15} \cdot 13$ de aquí que $y \mid 128$. Trabajando todas las posibilidades, tenemos como posibles puntos de torsión a $(3, \pm 8), (-5, \pm 16), (11, \pm 32)$. Usando la fórmula de duplicación sobre el punto $(3, 8)$ tenemos:

$$x(P) = 3,\ x(2P) = -5,\ x(4P) = 11,\ x(8P) = 3$$

De aquí tenemos que $8P = \pm P$ lo cual implica que P tiene orden 3,7 ó 9. No puede tener orden 9, ya que a lo más hay 7 posibles puntos de torsión y si tuviera orden 3 tendríamos que $x(2P) = x(-P)$ lo cual es falso. Por lo tanto P tiene orden 7, así tenemos que el subgrupo de torsión es ciclico de orden 7.

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\}.$$

Observación 4.1. Veamos algunas complicaciones al aplicar el teorema de Lutz-Nagell.

1) Supongamos que nosotros usamos el teorema de Lutz-Nagell y obtenemos un punto con coordenadas enteras. ¿Como saber si este es ó no un punto de torsión?, en el ejemplo 4.2.3 calculamos $2P$ y obtuvimos un punto con coordenadas no enteras. Por lo tanto, P no era un punto de torsión. En general, el teorema de Lutz-Nagell nos da una lista finita de posibles puntos de torsión.

2) La dificultad de aplicar el teorema de Lutz Nagell, radica en cuanto la discriminante posea mayor cantidad de divisores cuadrados perfectos, esto extendería los posibles valores enteros de y, haciendo más trabajoso el cálculo de posibles puntos de torsión.

Felizmente Mazur nos dió una caracterización definitiva de los subgrupos de torsión conocido como **el teorema de Mazur**, el cuál trataremos más adelante.

Veamos otra técnica que sirve para determinar el subgrupo de torsión, el cuál trabaja con la reducción módulo primos. Sea una curva elíptica dada por $y^2z = x^3 + Axz^2 + Bz^3$ con $A, B \in \mathbb{Z}$. La ecuación

$$\overline{E} : y^2 = x^3 + \overline{A}xz^2 + \overline{B}z^3 \, con \, \overline{A}, \overline{B} \in \mathbb{F}_p$$

se conoce como la **reducción de E módulo p**.

Teorema 4.3. *Sea una curva elíptica dada por $y^2z = x^3 + Axz^2 + Bz^3$ con $A, B \in \mathbb{Z}$ y sea p es un primo tal que $p \nmid 4A^3 + 27B^2$ entonces existe un homomorfismo $r_p : E(\mathbb{Q}) \to \overline{E}(F_p)$. Si p es impar entonces la restricción $r_p \mid_{E(\mathbb{Q})_{tors}}: E(\mathbb{Q})_{tors} \to \overline{E}(F_p)$ es un homomorfismo inyectivo. En particular $\mathcal{O}$ es el único punto que se reduce a $\mathcal{O}$.*

Como consencuencia del teorema tenemos que $E(\mathbb{Q})_{tors} \cong r_p(E(\mathbb{Q})_{tors})$, además como $r_p(E(\mathbb{Q})_{tors})$ es un subgrupo de $\overline{E}(F_p)$ entonces $|E(\mathbb{Q})_{tors}|$ divide a $|\underline{E}(\mathbb{F}_p)|$.

Ejemplo 4.2.5. Sea la curva elíptica $y^2 = x^3 + 8$, hallemos sus puntos de torsión usando el teorema anterior. Tenemos que $4A^3 + 27B^2 = 1728 = 2^6 \cdot 3^3$, así nosotros no podemos usar los primos $2, 3$.

1) Si aplicamos la reducción módulo 5 tenemos:

$$y^2 \equiv x^3 + 3 \, (mod \, 5)$$

de ahí que

x	$x^3 + 3$	y
0	3	$Ninguno$
1	4	± 2
2	1	± 1
3	3	0
4	2	$Ninguno$

Entonces $E(\mathbb{F}_5) = \{\mathcal{O}, (1, -2), (1, 2), (2, -1), (2, 1), (3, 0)\}$, como $|E(\mathbb{F}_5)| = 6$ tenemos que $|E(\mathbb{Q})_{tors}|$ divide a 6.

2) Si aplicamos la reducción módulo 7,11 y 13 respectivamente tenemos que $|E(\mathbb{F}_7)| = 12$, $|E(\mathbb{F}_{11})| = 12$ y $|E(\mathbb{F}_{13})| = 16$ respectivamente, entonces $|E(\mathbb{Q})_{tors}|$ divide a 12 y 16. Por lo tanto $|E(\mathbb{Q})_{tors}|$ divide a 2. Como $(-2, 0)$ es un punto de orden 2, tenemos que:

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (-2, 0)\}.$$

Del ejemplo anterior, el Teorema de Lutz-Nagell resulto ser más efectivo en el sentido de que fue más rápido conseguir los puntos de torsión que al aplicar el teorema anterior, uno se preguntará si ello siempre ocurre, la respuesta es no, veamos un ejemplo de lo contrario.

Ejemplo 4.2.6. Sea la curva elíptica dada por

$$y^2 = x^3 + 18x + 72$$

Entonces $4A^3 + 27B^2 = 163296 = 2^5 \cdot 3^6 \cdot 7$. El teorema de Lutz-Nagell consiste en encontrar todos los y tales que $y^2 | 163296$, de aquí que $y | 108 = 2^2 \cdot 3^3$. En cambio, $|E(\mathbb{F}_5)| = 5$ y $|E(\mathbb{F}_{11})| = 8$. De aquí que el subgrupo de torsión de $E(\mathbb{Q})$ es trivial.

4.3. El teorema de Lutz-Nagell sobre el cuerpo gaussiano $\mathbb{Q}(i)$

En esta sección nosotros extenderemos el teorema de Lutz-Nagell, que en su versión original nos permite calcular los puntos de torsión en $E(\mathbb{Q})$, ahora lo que haremos es calcular los puntos de torsión en $E(\mathbb{Q}(i))$. Antes de realizar la demostración del Teorema de Lutz-Nagell para curvas definidas sobre $\mathbb{Q}(i)$, empecemos dando las siguientes definiciones:

Definición 4.3.1. *Los enteros gaussianos son de la forma*

$$\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}.$$

Definición 4.3.2. *Sean $z, w \in \mathbb{Z}(i)$ con $w \neq 0$. Decimos que z es divisible por w si existe $u \in \mathbb{Z}(i)$ tal que $z = wu$.*

Por otro lado también tendremos en cuenta las siguientes observaciones:

1. Para cada $z = a + bi \in \mathbb{Z}(i)$ la norma se define como $N(z) = ||z||^2 = a^2 + b^2$.
2. Las unidades de $Z(i)$ son ± 1 y $\pm i$.
3. Un número $p \in \mathbb{Z}(i)$, decimos que es un primo gaussiano si y sólo si p es divisible por $\pm 1, \pm i, \pm p$ y $\pm ip$.
4. Un número primo $p \in \mathbb{Z}$ es también un primo gaussiano si y sólo si $p \equiv 3 (mod\, 4)$.
5. Un número $p \in \mathbb{Z}(i)$ es un primo gaussiano si y sólo si $N(p)$ es un entero primo.
6. Si $x \in \mathbb{Q}(i)$ entonces $x = \frac{g}{h}$ con $g, h \in \mathbb{Z}(i)$ y además g y h son coprimos (no poseen factores comunes a excepción de $\pm 1, \pm i$).

Definición 4.3.3. *Se define la valuación p-ádica gaussiana de un número $q \in \mathbb{Q}(i)$:*

$$g_p(q) = g_p(\frac{a}{b}) = r, \text{ tal que } \frac{a}{b} = p^r \frac{a_1}{b_1}$$

donde $a, b, a_1, b_1 \in \mathbb{Z}(i)$ y $p \nmid a_1 b_1$. Por convención se toma $g_p(0) = \infty$.

Ejemplo 4.3.1. $g_{3i}(7i/45) = -2$, $g_{7i}(49/(3i+1)) = 2$.

Sea E una curva elíptica sobre $\mathbb{Z}(i)$ dado por $y^2 = x^3 + Ax + B$ y sea $r \geq 1$ un número entero. Definamos

$$E_r = \{(x, y) \in E(\mathbb{Q}(i))/g_p(x) \leq -2r, g_p(y) \leq -3r\} \cup \{\mathcal{O}\}$$

Estos son los puntos tales que x tiene al menos p^{2r} en su denominador y y tiene al menos p^{3r} en su denominador. Se puede ver también que:

$$E(\mathbb{Q}(i)) \supseteq E_1 \supseteq E_2 \supseteq \ldots$$

La idea para esta demostración es imitar la versión original del teorema de Lutz-Nagell, para lo cuál necesitaremos de algunos resultados previos:

Lema 4.1. *Sea $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}(i)$. Para todo $(x, y) \in E(\mathbb{Q}(i))$ se cumple $g_p(x) < 0$ si y sólo si $g_p(y) < 0$. Además existe un entero $r \geq 1$ tal que $g_p(x) = -2r$ y $g_p(y) = -3r$ ($(x, y) \in E_r$).*

Demostración. Sea

$$x = \frac{x_1}{p^j x_2},\ y = \frac{y_1}{p^k y_2}$$

con $x_1, x_2, y_1, y_2 \in \mathbb{Z}(i)\, p \nmid x_1 x_2$ y $p \nmid y_1 y_2$. Cómo $g_p(x) < 0$ entonces $j > 0$, reemplazando en la curva tenemos que

$$\frac{y_1^2}{p^{2k} y_2^2} = \left(\frac{x_1}{p^j x_2}\right)^3 + A\left(\frac{x_1}{p^j x_2}\right) + B = \frac{x_1^3 + Ap^{2j} x_1 x_2^2 + Bp^{3j} x_2^3}{p^{3j} x_2^3}.$$

Pero el denominador $x^3 + Ax + B$ es igual al denominador de y^2. Por lo tanto $2k = 3j$, esto quiere decir que existe un r con $j = 2r$ y $k = 3r$. □

Dada una curva $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}(i)$. Si $y \neq 0$ podemos dividir entre y^3:

$$\frac{1}{y} = \left(\frac{x}{y}\right)^3 + A\left(\frac{x}{y}\right)\left(\frac{1}{y}\right)^2 + B\left(\frac{1}{y}\right)^3$$

de ahí que obtenemos una nueva curva en términos de t y s, $E' : s = t^3 + Ats^2 + Bs^3$ con $s = 1/y$ y $t = x/y$. Por lo tanto podemos definir una biyección

$$\begin{array}{rccc} \phi: & E\backslash\{(x,0)\} & \to & E' \\ & (x, y) & \to & (t, s) \\ & \mathcal{O} & \to & (0, 0). \end{array}$$

Recordemos que la curva E es simétrica respecto del eje x ($(x, y) \in E(\mathbb{Q}(i))$ si y sólo si $(x, -y) \in E(\mathbb{Q}(i))$), de igual modo esta nueva curva E' es simétrica respecto del cero ($(t, s) \in E(\mathbb{Q}(i))$ si y sólo si $(-t, -s) \in E(\mathbb{Q}(i))$).

Lema 4.2. *$(x, y) \in E_r$ si y sólo si $p^{3r} \mid s$ y $p^r \mid t$.*

Demostración. Esto se puede deducir del lema 4.1. □

Del mismo modo como definimos una nueva curva E' en términos de t y s, podemos definir una recta siguiendo el mismo proceso, es decir que si tenemos una recta en $ax+by+c=0$ con $y \neq 0$ en el plano xy, dividiendo entre y, obtenemos una recta $at+cs+b=0$ en el plano ts. Es más si queremos sumar en dicha curva E' esto sería del siguiente modo, si $P_1 + P_2 = P_3 = (t_3, s_3)$ con $P_1, P_2 \in E'(\mathbb{Q}(i))$ tenemos que la recta que pasa por P_1 y P_2 intersecta a la curva en el punto $(-t_3, -s_3)$, esto quiere decir que si $(t, s) \in E'$ entonces $-(t, s) = (-t, -s)$. En particular podemos afirmar que si la recta $ax + by + c = 0$ es tangente a la curva E en (x, y) si y sólo si $at + cs + b = 0$ es tangente a la curva E', además si $P \in E$ es de orden finito entonces $\phi(P)$ es de orden finito en E'.

Lema 4.3. *Toda recta $t = k$, con $k \in \mathbb{Q}(i)$ una constante y $k \equiv 0 \,(mod\, p)$, intersecta la curva $s = t^3 + As^2t + Bs^3$ en a lo más un punto (t, s) con $s \equiv 0 \,(mod\, p)$. Además esta recta no es tangente en ese punto de intersección.*

Demostración. Supongamos que la recta $t = k$ con $k \in \mathbb{Q}(i)$ una constante y $k \equiv 0 \,(mod\, p)$ intersecta a la curva en dos puntos (t, s_1) y (t, s_2) con $s_1 \equiv s_2 \equiv 0 \,(mod\, p)$. Entonces $s_1 \equiv s_2 \,(mod\, p^j)$ para algún $j \geq 1$. Hacemos $s_i = ps_i'$ con $i = 1, 2$ entonces $s_1' \equiv s_2' \,(mod\, p^{j-1})$, así $s_1'^2 \equiv s_2'^2 \,(mod\, p^{j-1})$, por lo tanto $s_1^2 = p^2 s_1'^2 \equiv p^2 s_2'^2 \,(\mathrm{mod}\, p^{j+1})$. De igual manera como $s_1'^3 \equiv s_2'^3 \,(\mathrm{mod}\, p^{j-1})$ entonces $s_1^3 \equiv s_2^3 \,(mod\, p^{j+2})$. Por lo tanto

$$s_1 = k^3 + Aks_1^2 + Bs_1^3 \equiv k^3 + Aks_2^2 + Bs_2^3 = s_2 \,(mod\, p^{j+1})$$

Como $s_1 \equiv s_2 \,(mod\, p)$ y si $s_1 \equiv s_2 \,(mod\, p^j)$ entonces $s_1 \equiv s_2 \,(mod\, p^{j+1})$ Por inducción tenemos que $s_1 \equiv s_2 \,(mod\, p^j)$ para todo $k \in \mathbb{N}$. De aquí $s_1 = s_2$, por lo tanto la recta $t = k$ intersecta a la curva en a lo más un punto (t, s) con $s \equiv 0 \,(mod\, p)$.
Hallemos la pendiente de la recta tangente a la curva $s = t^3 + As^2t + Bs^3$ derivando tenemos

$$\frac{ds}{dt} = 3t^2 + 2Ats\frac{ds}{dt} + As^2 + 3s^2B\frac{ds}{dt}$$

de aquí tenemos

$$\frac{ds}{dt} = \frac{3t^2 + As^2}{1 - 2Ats - 3s^2B}$$

Si la recta $t = k$ es tangente a la curva en $(t, s) \Rightarrow 1 - 2Ats - 3Bs^2 = 0$ y es divisible por p, pero $s \equiv t \equiv 0 \,(mod\, p)$ entonces

$$1 - 2Ast - 3Bs^2 \equiv 1 \not\equiv 0 \,(mod\, p).$$

Por lo tanto esta recta no es tangente a la curva. □

Si $c = 0$, entonces la recta tiene la forma del lema anterior. Pero este pasa por los puntos P_1' y P_2', así tenemos $P_1' = P_2'$, entonces $P_1 = P_2$, esto quiere decir que la recta $ax + by + c = 0$ es tangente en (x, y). Esto significa que $at + cs + b = 0$ es tangente en (t, s). Por el lema anterior esto sería una contradicción, por lo tanto $c \neq 0$.
Dividiendo por c, obtenemos la recta:

$$s = \alpha t + \beta$$

con $\alpha, \beta \in \mathbb{Q}(i)$ y P_1', P_2', P_3' puntos de dicha recta.

Lema 4.4.

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + As_2^2}{1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)}$$

Demostración. Analicemos 2 casos:

1. Si $t_1 \neq t_2$:

$$\begin{aligned}
&(s_2 - s_1)(1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)) \\
&= (s_2 - s_1) - A(s_2^2 - s_1^2)t_1 - B(s_2^3 - s_1^3) \\
&= (s_2 - s_1) - A(s_2^2 - s_1^2)t_1 - B(s_2^3 - s_1^3) \\
&= (s_2 - As_2^2 t_2 - Bs_2^3) - (s_1 - As_1^2 t_1 - Bs_1^3) + As_2^2(t_2 - t_1) \\
&= t_2^3 - t_1^3 + As_2^2(t_2 - t_1) \\
&= (t_2 - t_1)(t_2^2 + t_1 t_2 + t_1^2 + As_2^2)
\end{aligned}$$

   Esto prueba que $(s_2 - s_1)/(t_2 - t_1)$ es igual a la expresión en el lema.

2. Si $t_1 = t_2$: como la recta $t = c$ con $c \equiv 0 \,(mod\, p)$ intersecta a la curva $s = t^3 + As^2 t + Bs^3$ en un único punto con $s \equiv 0 \,(mod\, p)$ por el lema anterior tenemos que $(s_1, t_1) = (s_2, t_2)$. La recta $s = \alpha t + \beta$ es por lo tanto la recta tangente en ese punto con pendiente

$$\alpha = \frac{ds}{dt} = 3t^2 + As^2 + 2Ast\frac{ds}{dt} + 3Bs^2\frac{ds}{dt}.$$

   De aquí tenemos $\frac{ds}{dt} = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2}$ que igual a la expresión dada en el lema con $t_1 = t_2 = t$ y $s_1 = s_2 = s$

□

Lema 4.5. *Sean $E'_r = \phi(E_r)$ y $E'(\mathbb{Q}(i)) = \phi(E(\mathbb{Q}(i)))$. Entonces E'_r es un subgrupo de $E'(\mathbb{Q}(i))$.*

Demostración. Recordemos que $\mathcal{O}$ es el neutro de la curva E, podemos decir que $(0,0)$ que es el neutro en la curva E' como vimos anteriormente.

(i) $(0,0) \in E'_r$ por definición.

(ii) Sean $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ puntos en E_r y $P'_1 = \phi(x_1, y_1) = (t_1, s_1)$, $P'_2 = \phi(x_2, y_2) = (t_2, s_2)$, como $P_1, P_2 \in E_r$ entonces por el lema 4.2 p^{3r}/s_i, p^r/t_i con $i = 1, 2$.
Como $s_1 \equiv s_2 \equiv 0\,(mod\,p)$ entonces

$$1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2) \equiv 1\,(mod\,p).$$

Además debido a que $p^r | t_i$ con $i = 1, 2$, entonces

$$t_2^2 + t_1 t_2 + t_1^2 + A s_2^2 \equiv 0\,(mod\,p^{2r}).$$

Por lo tanto por el lema 4.4 tenemos que:

$$\alpha \equiv 0\,(mod\,p^{2r})$$

De igual manera como $p^{3r} | s_i$ con $i = 1, 2$ entonces

$$\beta = s_i - \alpha t_i \equiv 0\,(mod\,p^{3r}).$$

El punto $-P'_3 = P'_1 + P'_2 = (-t_3, -s_3)$ es el tercer punto de intersección de la recta $s = \alpha t + \beta$ con $s = t^3 + As^2 t + Bs^3$. Reemplazando s tenemos

$$\alpha t + \beta = t^3 + A(\alpha t + \beta)^2 t + B(\alpha t + \beta)^3.$$

De aquí que

$$t^3 + \frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2} t^2 + ... = 0$$

Entonces

$$t_1 + t_2 - t_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2} \equiv 0\,(mod\,p^{5r}).$$

Esto debido a que $p^{2r} | \alpha$ y $p^{3r} | \beta$. En particular $t_1 + t_2 - t_3 \equiv 0\,(mod\,p^r)$. Como $t_1 \equiv t_2 \equiv 0\,(mod\,p^r)$, entonces $t_3 \equiv 0\,(mod\,p^r)$, así $s_3 = \alpha t_3 + \beta \equiv 0\,(mod\,p^{3r})$. Por lo tanto p^r/t_3 y p^{3r}/s_3 entonces $P'_3 = (t_3, s_3) \in E'_r$.

iii) Sea $P = (x, y) \in E_r$ y $P' = \phi(x, y) = (t, s)$. Como $P = (x, y) \in E_r \Rightarrow g_p(x) \leq -2r$ y $g_p(y) \leq -3r$. Sea $y = a/b \Rightarrow g_p(a) - g_p(b) \leq -3r$, por otro lado $-y = -a/b \Rightarrow g_p(-a) - g_p(b) \leq -3r$ ya que $g_p(-a) = g_p(a)$.
De aquí que $-P = (x, -y) \in E_r$, por lo tanto $-P' = (-t, -s) \in E'_r$.

Por lo tanto E'_r es un subgrupo de $E'(\mathbb{Q}(i))$. □

Teorema 4.4. *(El teorema de Lutz-Nagell sobre el cuerpo gaussiano $\mathbb{Q}(i)$) Sea E una curva elíptica dada por $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}(i)$. Sea $P = (x, y) \in E(\mathbb{Q}(i))$ se cumple:*

1. Si P tiene orden finito entonces $x, y \in \mathbb{Z}(i)$.
2. Si P tiene orden finito con $y \neq 0$ entonces $y^2 \mid 4A^3 + 27B^2$.

Demostración 1) Supongamos que x ó y no esta en $\mathbb{Z}(i)$. Entonces existe un primo gaussiano p que divide al denominador de uno de ellos, además por el lema 4.1, existe un $r \in \mathbb{Z}^+$ tal que $P \in E_r$. Sea m el orden de P, podemos suponer que $p \nmid m$ (caso contrario tendríamos que $m = p^k n$ para algún $k \in \mathbb{Z}$ y $p \nmid n$ luego tomaríamos el punto $Q = p^k P$ que posee orden n con $p \nmid n$). Escojamos el mayor $j \in \mathbb{Z}^+$ tal que $P \in E_j, P \notin E_{j+1}$.
Como

$$t(mP) = mt(P) = 0 (mod\, p^{5j})$$

tenemos que $p^{5j} \mid t(P)$ entonces $P \in E_{5j}$, esto contradice el j escogido. Por lo tanto $x, y \in \mathbb{Z}(i)$, esto prueba la parte (1) del teorema.

2) Supongamos que $y \neq 0$. Entonces $2P = (x_2, y_2) \neq \mathcal{O}$. Como $2P$ tiene orden finito, $x_2, y_2 \in \mathbb{Z}$. Por el Teorema 4.2.1 tenemos

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}$$

Como $x_2 \in \mathbb{Z}$, entonces

$$y^2 \mid (x^4 - 2Ax^2 - 8Bx + A^2).$$

Operando tenemos:
$(3x^2 + 4A)(x^4 - 2Ax^2 - 8Bx + A^2) - (3x^3 - 5Ax - 27B)(x^3 + Ax + B)$
$= 4A^3 + 27B^2$
Además $y^2 = x^3 + Ax + B$. Por lo tanto $y^2 \mid 4A^3 + 27B^2$ □

Ejemplo 4.3.2. Sea la curva elíptica definida sobre $\mathbb{Q}(i)$ dada por

$$y^2 = x^3 - 8ix$$

Si $y = 0$, entonces $x = -2 - 2i$ ó $x = 2 + 2i$, los puntos $(-2 - 2i, 0)$ y $(2 + 2i, 0)$ tienen orden 2. Si $y \neq 0$ con $y^2 \mid 4A^3 + 27B^2 = 2048i = -(1 + i)^{22}$ entonces y toma los valores de:

$$\mu, (1 + i)\mu, (1 + i)^2\mu, \ldots, (1 + i)^{11}\mu$$

donde $\mu = -1, 1, -i, i$. Ninguno de ellos me da una solución con $x \in Z(i)$. Por lo tanto

$$E(\mathbb{Q}(i))_{tors} = \{\mathcal{O}, (0, 0), (-2 - 2i, 0), (2 + 2i, 0)\}.$$

4.4. Acotación de los subgrupos de torsión

4.4.1. El teorema de Mazur

Sea la curva elíptica E definida sobre $\mathbb{Q}$, dada por la ecuación de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \; con \, a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q} \tag{4.1}$$

para calcular el subgrupo de torsión $E(\mathbb{Q})_{\text{tors}}$ aplicando el teorema de Lutz-Nagell, lo que haremos es expresar E como la ecuación

$$y^2 = x^3 + Ax + B, \; con \, A, B \in \mathbb{Z}. \tag{4.2}$$

Esto es debido a que el subgrupo de torsión $E(\mathbb{Q})_{\text{tors}}$ que obtenemos en (4.2) es isomorfo al de (4.1). El siguiente teorema nos da una caracterización definitiva de los subgrupos de torsión de una curva elíptica definida sobre $\mathbb{Q}$.

Teorema 4.5. *(Teorema de Mazur) Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces el subgrupo de torsión de $E(\mathbb{Q})$ es uno de los siguientes 15 grupos:*

$$\mathbb{Z}_n \, con \, 1 \leq n \leq 10 \; ó \; n = 12$$

$$\mathbb{Z}_2 \bigoplus \mathbb{Z}_{2n} \, con \, 1 \leq n \leq 4$$

Demostración. Consultar [5, pág 33-186]. □

Veamos una tabla que nos muestra 15 curvas elípticas diferentes, que poseen subgrupos de torsión distintas.

Curva elíptica definida sobre$\mathbb{Q}$	Subgrupo de torsión$(E(\mathbb{Q})_{\text{tors}})$	Generadores
$y^2 = x^3 + 2$	0	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 + y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 0)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy - 6y = x^3 - 6x^2$	$\mathbb{Z}/8\mathbb{Z}$	$(0, 6)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 - 7xy - 36y = x^3 - 18x^2$	$\mathbb{Z}/10\mathbb{Z}$	$(6, 72)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(1, 0), (0, 0)$
$y^2 = x^3 + 5x^2 + 4x$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(2, 6), (-1, 0)$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(2, -2), (-3, 18)$
$y^2 = x^3 + 337x^2 + 20736x$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(24, 840), (-81, 0)$

4.4.2. El teorema de Kenku-Momose

El teorema de Kenku-Momose nos da una caracterización definitiva de los subgrupos de torsión sobre el cuerpo gaussiano $\mathbb{Q}(i)$.

Teorema 4.6. *(Teorema de Kenku-Momose) Sea $\mathbb{Q}(i)$ una extensión de $\mathbb{Q}$ con $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ y E una curva elíptica definida sobre $\mathbb{Q}(i)$. Entonces el subgrupo de torsión de $E(\mathbb{Q}(i))$ es isomorfo a uno de los siguientes 26 grupos*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \quad & \textit{para} \quad 1 \leq n \leq 18,\ n \neq 17 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad & \textit{para} \quad 1 \leq n \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z} \quad & \textit{para} \quad n = 1, 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{aligned}$$

4.4.3. Conjetura de acotación uniforme

El teorema de Mazur nos muestra los 15 subgrupos de torsión que se pueden obtener trabajando con curvas elípticas definidas sobre los números racionales y el

teorema de Kenku-Momose 26 subgrupos de torsión que se pueden obtener trabajando con curvas elípticas definidas sobre el cuerpo gaussiano entonces nos hacemos la siguiente pregunta: ¿Es posible que la cantidad de subgrupos de torsión sea finita si trabajamos sobre una extensión finita de los números racionales?; la respuesta es sí. Veamos las consecuencias que se obtuvierón apartir del teorema Mazur.

Conjetura de acotación uniforme Para todo entero $d \geq 1$ con $d = [K : \mathbb{Q}]$, existe un entero $B(d)$, tal que para todo cuerpo K de grado d sobre $\mathbb{Q}$ y para toda curva elíptica E definida sobre K, tenemos que

$$|E(F)_{\text{tors}}| < B(d).$$

Podemos ver que este es un caso general, para $d = 1$ tenemos el teorema de Mazur. Por otro lado, notemos que si $P \in E(\mathbb{Q})_{tors}$ entonces $P \in E(\mathbb{Q}(i))_{tors}$, por tal motivo podemos ver una curva definida sobre los racionales como si estuviese definida sobre el cuerpo gaussiano. Este estudio lo realizó años más tarde en el 2005, Yasutsugu Fujita (1965) y caracterizó al conjunto $E(\mathbb{Q}(i))_{tors}$ para curvas definidas sobre los racionales como isomorfo a uno de los 20 grupos que pasamos a detallar.

Teorema 4.7. *(Fujita) Sea E una curva elíptica sobre $\mathbb{Q}$. Sea $F = \mathbb{Q}(i)$. Entonces el subgrupo de torsión de $E(\mathbb{Q}(i))$ es isomorfo a unos de los siguientes 20 grupos.*

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad & para \quad n = 1, 2, 3, 4, 5, 6, 8, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z} \quad & para \quad n = 1, 2, 3, 4 \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad & para \quad n = 3, 4 \end{aligned}$$

o $\mathcal{O}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$.

Demostración. Consultar [6,pág 124-134]. □

Ejemplo 4.4.1. Sea la curva elíptica dada por

$$y^2 = x^3 - 12987x - 263466$$

Si la curva esta definida sobre $E(\mathbb{Q})$, tenemos que el subgrupo de torsión es isomorfo a $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Por otro lado si consideramos que la curva esta definida sobre $E(\mathbb{Q}(i))$,

tenemos:

Orden	Punto
1	$\mathcal{O}$
2	$(-21,0),(-102,0),(123,0)$
4	$(-57,\pm 540),(-21-108i,\pm(1296+972i)),(33,810i),$
	$(-237,\pm 3240i),(-21+108i,\pm(1296-972i)),(303,\pm 4860)$

4.5. Cálculo efectivo del subgrupo de torsión

Veamos como calcular el subgrupo de torsión usando el programa Pari/Gp para la curva

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

Debemos tener en cuenta los siguientes comandos:

1. elllinit: Inicializa a la curva como un vector, donde las primeras componentes que se obtienen son

   $$a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, c_4, c_6, \Delta, j$$

   donde Δ es la discriminante y j es la $j-invariante$.

2. elltors: Calcula el subgrupo de torsión de una curva elíptica definida sobre $\mathbb{Q}$ y nos da la forma de su estructura como un vector de tres componentes $[t, v_1, v_2]$, donde t es el orden del grupo, v_1 nos da la estructura del grupo de torsión como un producto de grupos ciclicos y v_2 nos da los generadores de estos grupos ciclicos.

Ejemplo 4.5.1. Sea la curva elíptica E dada por $y^2 = x^3 + 4$.

```
(18:02) gp > e1=ellinit([0,0,0,0,4])
%1 = [0, 0, 0, 0, 4, 0, 0, 16, 0, 0, -3456, -6912, 0, [-1.5874010519681994747
05639, 0.79370052598409973737585281960 + 1.3747296369986026263834791960*I, 0.79
052598409973737585281960 - 1.3747296369986026263834791960*I]~, 3.33873802356691
3685999087,-1.669369011783458076842999544+ 0.96381064832999906552284889420*I,-
1.629776896028930120858184886 - 1.818185553 E-29*I, 0.814888448014465060429090
30 - 1.411428194462003290422763710*I, 3.217911259098049157248456148]
```

```
(18:03) gp > elltors(e1)
%2 = [3, [3], [[0, 2]]]
```

Estructura del grupo: $\mathbb{Z}_3$.
Generador: (0, 2).

Ejemplo 4.5.2. Sea la curva elíptica E dada por $y^2 + 7xy - 6y = x^3 - 6x^2$

```
(18:50) gp > e2=ellinit([7,-6,-6,0,0])
%3 = [7, -6, -6, 0, 0, 25, -42, 36, -216, 1633, -61201, 352512,4354703137/3525
2, [2.0000000000000000000000000, 0.513493828819868118549086088O,-8.763493828
19868118549086087]~, 1.479677927794478211580972544, 0.9934818585060132473932999
22*I, -0.701295667202135003252863788O4, -2.594022053248545133794126897*I,1.4700
3177695584689121454373]
```

```
(18:51) gp > elltors(e2)
%4 = [8, [8], [[0, 6]]]
```

Estructura del grupo: $\mathbb{Z}_8$.
Generador: (0, 6).

Ejemplo 4.5.3. Sea la curva elíptica E dada por $y^2 = x^3 - 12987x - 263466$

```
(11:51) gp > e1=ellinit([0,0,0,-12987,-263466])
%1 = [0, 0, 0, -12987, -263466, 0, -25974, -1053864, -168662169, 623376, 2276
605760000, 111284641/50625, [123.000000000000000000000000, -21.0000000000000
, -102.000000000000000000000000]~, 0.233433840388767003863363472O, 0.2660403
14948453*I, -6.915069732821692735920044350,-21.339152704022794328165866920*I,0.
5048691949352063284]
(11:52) gp > elltors(e1)
%2 = [8, [4, 2], [[303, 4860], [-21, 0]]]
```

Estructura del grupo: $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
Generadores: (303, 4860) y (-21, 0).

Conclusiones

- Hemos construido un grupo abeliano no trivial agregandole un punto $\mathcal{O}$ a la curva elíptica, esto resulto ser natural para conseguir una identificación entre estos puntos del plano afín A_K^2 y los puntos finitos del espacio proyectivo P_K^2, además de la identificación de $\mathcal{O}$ con los puntos infinitos de P_K^2.

- Utilizando el espacio proyectivo, estudiamos las curvas en P_k^2, las cuales son descritas por polinomios homogéneos é introducimos un nuevo concepto de orden de intersección. Demostramos tambien la asociatividad de puntos en una curva elíptica.

- Demostramos que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito, tomando dos casos, el primero considerando que el polinomio $p(x) = x^3 + Ax + B$ con $A, B \in \mathbb{Q}$ se descompone sobre $\mathbb{Q}$ (caso particular del teorema débil de Mordell-Weill), segundo que dicho polinomio se descompone en una extensión finita de $\mathbb{Q}$ (caso general del teorema débil de Mordell-Weill).

- Introducimos un nuevo concepto de altura de puntos de una curva elíptica esto junto con que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ sea finito, nos ayudo a demostrar que los puntos racionales de una curva elíptica es finitamente generado (teorema de Mordell-Weil).

- Mostramos como se realiza el cálculo de los subgrupos de torsión de una curva elíptica definida sobre $\mathbb{Q}$, esta se hizó de dos maneras, la primera utilizando el teorema de Lutz-Nagell y la segunda utilizando la reducción módulo primo, dicha curva puede ser calculado sobre un cuerpo finito con ciertas condiciones conseguimos que el $E(\mathbb{Q})_{tors}$ divide al orden $E(\mathbb{F}_p)$. Finalmente mostramos el teorema de Mazur, que nos caracteriza todos los subgrupos de torsión de una curva elíptica definida sobre $\mathbb{Q}$.

- Demostramos el teorema de Lutz-Nagell para curvas definidas sobre $\mathbb{Q}(i)$, donde estudiamos las propiedades algebraicas del anillo de enteros gaussianos $\mathbb{Z}(i)$. Finalmente mostramos un teorema analogo al teorema de Mazur, conocido como el teorema de Kenku-Momose, que nos caracteriza todos los subgrupos de torsión sobre una curva elíptica definida sobrel $\mathbb{Q}$(i).

- Utilizando el sistema de cálculo PARI/GP y el teorema de Lutz-Nagell para curvas definidas sobre $Q(i)$, se corroborá el cálculo de los subgrupos de torsión de una curva elíptica sobre el cuerpo gaussiano.

Bibliografía

[1] Antony W. Knapp, *Elliptic curves*. Princeton University Press, 1992.

[2] J.E. Cremona, *Algorthms for Modular Elliptic Curves, second edition*. Cambridge University Press, 1997.

[3] D. Doud, *A Procedure to Calculate Torsion of Elliptic Curves Over* $\mathbb{Q}$. Manuscripta Mathematica, 1998.

[4] Darrel Hankerson, Alfred Menezes y Scott Vanstone, *Guide to Elliptic curve cryptography*. Springer-Verlag New York, 2004.

[5] Joseph H. Silverman, *The arithmetic of Elliptic curves*. Sringer, 1986.

[6] Joseph H. Silverman, *Advanced Topics in the arithmetic of Elliptic curves*. Sringer Verlag, 1994.

[7] J.S. Milne, *Fields and Galois Theory*. Notes, 2003

[8] J.S. Milne, *Elliptic curves*. BookSurge Publishers, 2006.

[9] Steven H. Weintraub, *Galois Theory*. Lehigh University Press, 2006.

[10] Lawrence C. Washington, *Elliptic curves:number theory and criptography*. Chapnan Hall CRC, Boca Raton, FL, 2008.

[11] Searge Lang, *Elliptic curves: Diophantine Analysis* . Springer-Verlag, Berlin, 1978.

[12] Yasutsugu Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extension of* $\mathbb{Q}$. Mathematical Institute Tohoku University, 2003.