Universidad de Valparaíso
Facultad de Ciencias
Instituto de Matemáticas

Aspectos algorítmicos de las curvas de género 2

Tesis para optar al grado de
Magíster en Matemáticas

Presentada por:
JORGE LUIS GÓMEZ MARÍN

Profesor Guía: Dra. Amalia Pizarro Madariaga

VALPARAÍSO
ABRIL - 2025

Agradecimientos

Quiero expresar mi más profundo agradecimiento a Chile y a la Universidad de Valparaíso por brindarme la oportunidad de continuar con mis estudios y abrir nuevas puertas para mi futuro profesional.

Agradezco especialmente a los profesores Amalia Pizarro, Marcelo Flores y Rodrigo Castro, quienes no solo fueron fundamentales en mi formación académica durante el Magíster, sino que también me brindaron apoyo emocional y moral en diversas circunstancias. Por su guía, paciencia y enseñanzas, les estaré siempre agradecido.

Agradezco también a los profesores Edgardo Riquelme y Roberto Villaflor por su tiempo y dedicación en la revisión de mi tesis, contribuyendo así a la culminación de esta etapa.

A María Fernanda Rosero, por haber estado presente en los momentos más difíciles y por haber creído en mí cuando más lo necesitaba. A mis compañeros y amigos Bladimir Blanco y Claudio Fierro, por su amistad incondicional, su apoyo y por tantas risas compartidas a lo largo de este camino.

A mi madre Perla del Carmen Marín, y a mi hermano Kevin Gómez por ayudarme a convertirme en la persona que soy.

Gracias a todos ustedes y a tantas otras personas que, aunque no estén mencionadas aquí, han sido parte fundamental de este proceso y a quienes también les debo mucho.

Per laborem ad lucem.

Resumen

Las isogenias entre variedades abelianas han sido objeto de estudio en diversas áreas de la matemática, incluyendo geometría algebraica, teoría de números y, más recientemente, criptografía. En particular, las isogenias de Richelot en jacobianos de curvas de género 2 han adquirido gran relevancia en el desarrollo de protocolos criptográficos post-cuánticos, como el esquema G2SIDH, una extensión del SIDH basado en curvas elípticas. En este contexto, el presente trabajo se enfoca en el estudio teórico y computacional de las isogenias de Richelot, proporcionando herramientas fundamentales para su análisis y aplicación en criptografía.

El primer capítulo está dedicado a los preliminares necesarios para comprender el problema en estudio. Se inicia con la teoría básica de curvas hiperelípticas de género 2, estableciendo la relación entre los espacios afín y proyectivo, y la estructura de sus cuerpos de funciones. Posteriormente, se abordan conceptos algebraicos esenciales como los anillos locales, anillos Noetherianos y la valoración en puntos de una curva, los cuales son fundamentales para definir divisores y su correspondiente grupo de clases. Además, se introduce la noción de jacobiano de una curva y su representación mediante la forma de Mumford, así como algoritmos para su aritmética eficiente, como el algoritmo de Cantor. También se estudian los subgrupos de torsión y su relación con la estructura del jacobiano, lo cual es clave para el análisis de isogenias.

El segundo capítulo se enfoca en el estudio de variedades abelianas y su polarización. Se presentan definiciones y propiedades fundamentales de las variedades abelianas, junto con su dualidad y la teoría de isogenias entre ellas. La polarización juega un papel central en la clasificación de las variedades abelianas y en la selección de ciertas isogenias de interés, como aquellas que surgen exclusivamente entre jacobianos de curvas. Asimismo, se introduce el concepto de emparejamientos de Weil, los cuales tienen aplicaciones en criptografía y en la caracterización de isogenias.

Finalmente, el tercer capítulo está dedicado al estudio específico de las isogenias de Richelot. Se inicia con la descomposición cuadrática y la correspondencia de Richelot, proporcionando una base teórica para el cálculo de estas isogenias. Luego, se presentan métodos eficientes para su evaluación y clasificación en función de la estructura del subgrupo núcleo. En particular, se analizan isogenias de tipo $(2^n, 2^n)$ y sus ecuaciones asociadas, lo cual permite una implementación más eficiente en el contexto de la criptografía post-cuántica. Se concluye con una descripción del protocolo

G2SIDH y su relevancia en la seguridad criptográfica frente a la computación cuántica.

En resumen, este trabajo proporciona un estudio detallado de las isogenias de Richelot desde una perspectiva algebraico-geométrica, con un énfasis en su aplicabilidad en criptografía. A través de los diferentes capítulos, se establecen las bases teóricas y computacionales necesarias para comprender la estructura y el cálculo de estas isogenias, contribuyendo así al desarrollo de herramientas matemáticas para la criptografía basada en isogenias.

Índice general

Introducción **2**

1. Preliminares **4**

1.1. Curvas hiperelípticas de género 2 4
1.2. Relación entre el espacio afín y el espacio proyectivo 6
1.3. Cuerpos de funciones 9
1.4. Anillos locales y anillos Noetherianos 10
1.5. Valoración en un punto de una curva 12
1.6. Cuerpo de funciones para género 2 16
1.7. Divisores 18
1.8. Grupo de clases de divisores 27
1.9. Jacobiano 30
1.10. Representación de Mumford 32
1.11. Algoritmo de Cantor 39
1.12. Aritmética Rápida 41
1.13. Subgrupos de Torsión 44
1.14. 2-Torsión del Jacobiano 47
1.15. 3-Torsión 49

2. Isogenias entre variedades abelianas **51**

2.1. Variedades Abelianas 51
2.2. Dual de una variedad abeliana 61
2.3. Isogenias 62
2.4. Polarización 65
2.5. Emparejamientos 68

3. Isogenias de Richelot **73**
3.1. Descomposición cuadrática 74
3.2. Correspondencia de Richelot 79
3.3. Calculo eficiente de Isogenias 83
3.4. Isogenias de Richelot para ecuaciones de tipo 1 84
3.5. Superficie de Kummer 86
3.6. Métodos para evaluar Isogenias de Richelot. 88
3.7. Isogenias $(2^n, 2^n)$ 90
3.8. Subgrupos $(2^n, 2^n)$ y ecuaciones de tipo 2 92
3.9. Algoritmo 95
3.10. (2,2)-isogenias en criptografía 99

Introducción

Las curvas hiperelípticas, una clase fundamental dentro de la teoría algebraica de curvas, han capturado la atención de matemáticos y científicos desde su concepción en el siglo XIX. Estas curvas son el resultado de una intersección entre el álgebra y la geometría, lo que las hace de vital importancia en áreas como la criptografía, la física teórica y la teoría de números. El término "hiperelíptico"proviene de la idea de generalizar el concepto de curvas elípticas, que han sido objeto de estudio durante siglos. Las curvas hiperelípticas, al permitir un grado mayor de flexibilidad en su estructura, presentan una riqueza de propiedades y comportamientos intrigantes que aún están siendo explorados en la actualidad.

El interés en las curvas hiperelípticas surgió en el siglo XIX en el marco del desarrollo de la geometría algebraica. Matemáticos como Niels Henrik Abel y Évariste Galois sentaron las bases para el estudio de las curvas algebraicas, abriendo la puerta a la comprensión profunda de su estructura y propiedades. A medida que los investigadores avanzaban en la teoría, se descubrió que las curvas elípticas eran solo un caso particular de una familia más amplia de curvas, conocidas como hiperelípticas. Esta generalización permitió un tratamiento más amplio de conceptos matemáticos esenciales y condujo a desarrollos significativos en el campo [44].

Las isogenias entre variedades abelianas han sido un tema de gran interés en diversas áreas de la matemática, especialmente en geometría algebraica y teoría de números. En años recientes, su estudio ha cobrado relevancia en el ámbito de la criptografía post-cuántica debido a su aplicación en protocolos resistentes a ataques por computadoras cuánticas. En particular, los sistemas criptográficos basados en isogenias, como el Supersingular Isogeny Diffie-Hellman (SIDH) y su extensión a curvas de género 2, conocido como G2SIDH, han surgido como alternativas prometedoras en este campo. Estos esquemas utilizan la dificultad computacional de encontrar isogenias entre variedades abelianas dadas como base para su seguridad.

El protocolo SIDH, basado en curvas elípticas supersingulares, ha sido ampliamente estudiado por su potencial en criptografía post-cuántica. Sin embargo, las recientes vulnerabilidades descubiertas en SIDH han llevado a la búsqueda de variantes más seguras, entre ellas el protocolo G2SIDH, que utiliza jacobianos de curvas de género 2 en lugar de curvas elípticas. El estudio de estas estructuras matemáticas es fundamental para comprender la seguridad y eficiencia de estos sistemas criptográficos, así como para el desarrollo de nuevas implementaciones que refuercen su resistencia ante ataques adversarios.

El presente trabajo tiene como objetivo realizar un estudio detallado de las isogenias de Richelot en jacobianos de curvas de género 2, desde una perspectiva teórica, proporcionando una base sólida para su aplicación en criptografía. Se inicia con una revisión de los aspectos fundamentales de las curvas hiperelípticas de género 2, su estructura algebraica y su relación con los jacobianos. Posteriormente, se analiza la teoría de variedades abelianas y su polarización, aspectos esenciales para comprender la clasificación de isogenias en este contexto. Finalmente, se estudia en detalle la construcción y evaluación eficiente de isogenias de Richelot, con énfasis en su aplicabilidad a G2SIDH.

Capítulo 1

Preliminares

La teoría de curvas hiperelípticas sobre cuerpos finitos es un fascinante campo matemático que combina la geometría algebraica y la teoría de números. Se centra en el estudio de curvas algebraicas especiales, conocidas como curvas hiperelípticas, definidas sobre cuerpos finitos. Estas curvas tienen aplicaciones clave en criptografía y teoría de códigos. Para comprenderlas, es necesario explorar conceptos como la ecuación de Weierstrass y el género de la curva, mientras que la geometría proyectiva proporciona una valiosa herramienta para visualizar y analizar estas curvas en un marco más amplio. Asumiremos algunos conceptos de las variedades algebraicas que pueden ser consultados en [43, Basic Algebraic Geometry 1].

1.1. Curvas hiperelípticas de género 2

A continuación, definiremos el concepto de curvas hiperelípticas para género arbitrario, sin embargo en esta tesis nos concentraremos en el caso de género 2.

Definición 1.1.1 *Sea $g \geq 1$ un número entero, K un cuerpo y $h(x), f(x) \in K[x]$, tales que $deg(f) = 2g+1$, $deg(h) \leq g$ y f mónico. La curva dada por la ecuación:*

$$\mathcal{C} : y^2 + h(x)y = f(x),$$

será llamada curva hiperelíptica de género g si es no singular, es decir, si no existen $x, y \in K$ tales que $2y + h(x) = f'(x) - y = 0$, siendo f', h' las derivada formales de f y h en $K[x]$.

Observación 1.1.1 *La condición anterior es equivalente a la siguiente, si consideramos*

$\mathcal{C}(x,y) := y^2 + h(x)y - f(x)$, entonces los puntos de la curva hiperelíptica están dados por la variedad afín determinada por los ceros de $\mathcal{C}(x,y)$. En tal caso, se tiene que

$$(x,y) \text{ es singular si y solo si } \frac{\partial \mathcal{C}}{\partial y} = \frac{\partial \mathcal{C}}{\partial x} = 0.$$

Observación 1.1.2 *Si $char(K) \neq 2$, es posible describir a una curva hiperelíptica en la forma $\mathcal{C}: y^2 = f(x)$ con f mónico y $deg(f) = 2g+1$ o $deg(f) = 2g+2$. Además, la no singularidad es equivalente a decir que f no tiene raíces múltiples, o bien $f'(x) \neq 0$.*

Definición 1.1.2 *Sea $\mathcal{C}: y^2 = f(x)$ la ecuación de una curva hiperelíptica de género 2 definida sobre un cuerpo K. Decimos que el punto $(x,y) \in \mathcal{C}$ es un punto racional de la curva $\mathcal{C}$, si $x, y \in K$. Denotaremos por $\mathcal{C}(K)$ al conjunto de todos los puntos racionales de la curva y $\mathcal{C}(\overline{K})$ a los puntos de la curva en la clausura algebraica de K.*

En adelante, consideraremos $g = 2$ y $char(K) \neq 2$, es decir, $\mathcal{C}: y^2 = f(x)$ con $deg(f) = 5$ ó $deg(f) = 6$. Puede ocurrir que existan puntos de la curva fuera del cuerpo base K, así distinguiremos $\mathcal{C}(K)$ de $\mathcal{C}(\overline{K})$ de ser necesario.

Lema 1.1.1 *Sea $\mathcal{C}: y^2 = f(x)$ con $deg(f) = 5$ una curva hiperelíptica definida sobre K y sin puntos singulares en $\overline{K}$. Entonces la variedad algebraica $V(\mathcal{C}(x,y))$, con $\mathcal{C}(x,y) = y^2 - f(x)$, es irreducible sobre $\overline{K}$ y la dimensión de $V(\mathcal{C}(x,y)$ es 1.*

Demostración. Sabemos que $V(\mathcal{C}(x,y))$ es irreducible sobre $\overline{K}$ si y solo si $\mathcal{C}(x,y)$ es irreducible sobre $\overline{K}$ lo que es equivalente a que $\mathcal{C}(x,y)$ se factorice completamente sobre $\overline{K}[x,y]$. Consideremos $\mathcal{C}(x,y) \in (\overline{K}[x])[y]$. Una factorización de $\mathcal{C}(x,y)$ debe ser de la forma

$$\mathcal{C}(x,y) = (y - a(x))(y - b(x)),$$

con $a(x), b(x) \in \overline{K}[x]$. Como $deg(f) = 5$, entonces $deg(a) \neq deg(b)$ y al menos uno de ellos es no constante, luego $a(x) - b(x)$ es no constante. Si $x_p \in \overline{K}$ es una raíz de $a(x) - b(x)$ e $y_p = a(x_p) = b(x_p)$ entonces $(x_p, y_p) \in \mathcal{C}(\overline{K})$. Es fácil notar que ambas derivadas parciales de $\mathcal{C}(x,y)$ se anulan en (x_p, y_p), lo cual contradice el hecho de que $\mathcal{C}$ no tiene puntos singulares. Concluimos entonces que $\mathcal{C}(x,y)$ es irreducible sobre $\overline{K}$, así mismo su variedad afín $V(\mathcal{C}(x,y))$.
Por otro lado sea $X = V(\mathcal{C}(x,y))$. Sabemos que la dimensión de una variedad algebraica mide el número de parámetros algebraicamente independientes necesarios para describir los puntos en la variedad. Siendo así basta notar que $K(x,y)$ es algebraico sobre

$K(x)$, pues $y^2 = f(x)$, o lo mismo $\mathcal{C}(x,y) = 0$. Luego el grado de trascendencia es 1, por tanto $dim(X) = 1$. ■

Modelo proyectivo de curvas hiperelípticas El espacio proyectivo es un concepto fundamental en la geometría algebraica y la geometría proyectiva. Proporciona una manera elegante de tratar con puntos en el infinito y de estudiar geometría de manera más uniforme, especialmente en contextos en los que se trata con coordenadas homogéneas.

Homogeneizar una curva es un proceso en geometría algebraica que consiste en convertir una ecuación de una curva en el espacio afín en una ecuación homogénea en el espacio proyectivo correspondiente. Este proceso es útil para extender el estudio de la curva al espacio proyectivo y para incluir puntos en el infinito en la descripción de la curva.

1.2. Relación entre el espacio afín y el espacio proyectivo

Definición 1.2.1 *Un polinomio $F(x_0, x_1, \ldots, x_n)$ en $n+1$ variables con coeficiente en K es homogéneo de grado d si todos sus términos tienen la forma $ax_0^{k_0}x_1^{k_1}\ldots x_n^{k_n}$, donde $k_0 + k_1 + \ldots + k_n = d$ y a es una constante en K.*

Definición 1.2.2 *Sea $F \in K[x_0, x_1, \ldots, x_n]$ un polinomio homogéneo de grado d. La deshomogeneización de F con respecto a x_i, denotada por F_i es un polinomio en una variable menos, donde reemplazamos $x_i = 1$, es decir $F_i = F(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in K[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.*

Definición 1.2.3 *Sea $f \in K[x_0, \ldots, x_{i-1}, x_{i+1} \ldots, x_n]$ con grado total d. Definimos la homogeneización respecto a x_i como $f_i = x_i^d f(x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)$.*

Observación 1.2.1 *Sea $U_i = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n : u_i \neq 0\}$ un abierto, podemos enviar a U_i al espacio afín $\mathbb{A}^n$ y viceversa por:*

$$\begin{array}{rccc} \phi_i : & \mathbb{A}^n & \longrightarrow & U_i \\ & (x_1 \ldots, x_n) & \mapsto & (x_1 : \ldots : x_i : 1 : x_{i+1} : \ldots : x_n), \end{array}$$

$$\begin{array}{rccc} \phi_i^{-1} : & U_i \subseteq \mathbb{P}^n & \longrightarrow & \mathbb{A}^n \\ & (x_0 : \ldots : x_n) & \mapsto & \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right). \end{array}$$

Si consideremos la homogeneización del polinomio $\mathcal{C}(x,y) = Y^2 - f(X)$ definido por la curva $\mathcal{C} : Y^2 = f(X)$, en la variable Z, con $deg(f) = 6$, f mónico y $f(X) = \sum_{i=0}^{6} f_i X^i$, $f_i \in K$, obtenemos el polinomio

$$\mathcal{C}(X,Y,Z) = Y^2 Z^4 - \sum_{i=0}^{6} f_i X^i Z^{6-i}.$$

Para efectos prácticos lo anterior puede verse simplemente como realizar los cambios de variable $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$ al polinomio $\mathcal{C}(x,y)$, lo que nos da una versión homogénea de la ecuación de la curva hiperelíptica.

El modelo proyectivo es importante al trabajar con curvas hiperelípticas porque simplifica las ecuaciones, permite la inclusión de puntos en el infinito, y facilita las operaciones algebraicas y geométricas. Además, es esencial en aplicaciones criptográficas para realizar cálculos de manera eficiente y segura.

Otra forma de homogeneizar es utilizar los espacios proyectivos ponderados o con pesos.

Definición 1.2.4 *Espacio proyectivo con pesos. Sean $i_0, \ldots, i_n \in \mathbb{N}$ y sea K un cuerpo. Definimos en K^{n+1} la relación de equivalencia,*

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n) \text{ si y solo si } b_o = \lambda^{i_0} a_0, b_1 = \lambda^{i_1} a_1, \ldots, b_n = \lambda^{i_n} a_n, \lambda \in K^*.$$

Denotamos por $(a_0 : a_1, \ldots : a_n)$ a la clase de equivalencia del elemento $(a_0, \ldots, a_n)$. Definimos el espacio proyectivo de peso $(i_0, i_1, \ldots, i_n)$ como conjunto de clases de equivalencia y será denotado por $\mathbb{P}^n(i_0, i_1, \ldots, i_n)$. El espacio proyectivo usual, corresponde al espacio de peso $(1,1,\ldots,1)$, es decir, $\mathbb{P}^n = \mathbb{P}^n(1,1,\ldots,1)$.

En particular, para el caso de curvas hiperelípticas consideraremos el espacio $\mathbb{P}^2(1,3,1)$, donde $(X : Y : Z) \sim (\lambda X : \lambda^3 Y : \lambda Z)$, $\lambda \in K^*$. De aquí, considerando los cambios

$$x = \frac{X}{Z}, y = \frac{Y}{Z^3},$$

obtenemos la siguiente versión proyectiva

$$Y^2 = f_6 X^6 + f_5 X^5 Z + f_4 x^4 Z^2 + f_3 X^3 Z^3 + f_2 x^2 Z^4 + f_1 X Z^5 + f_0 Z^6.$$

Observación 1.2.2 *Puntos* (x, y) *asociados a la ecuación afín corresponden a puntos* $(X : Y : 1)$ *en el espacio proyectivo con pesos. Más aún, si la ecuación afín es no singular entonces el modelo proyectivo con pesos es también no singular.*

Definición 1.2.5 *Definimos la involución hiperelíptica como la función* $i : \mathcal{C} \to \mathcal{C}$ *tal que* $i(x, y) = (x, -y)$. *Mas aun, en la versión proyectiva tenemos que* $i(X : Y : Z) = (X : -Y : Z)$ *y los puntos tales que* $Z = 0$ *corresponden a los puntos al infinito.*

Lema 1.2.1 *Dada la ecuación de la curva hiperelíptica en su versión proyectiva*

$$Y^2 = f_6X^6 + f_5X^5Z + f_4x^4Z^2 + f_3X^3Z^3 + f_2X^2Z^4 + f_1XZ^5 + f_0Z^6.$$

Los puntos al infinito son de la forma $(1 : \alpha : 0)$, *donde* $\alpha \in K$ *tal que* $\alpha^2 - f_6 = 0$, *más aún, dichos puntos son no singulares.*

Demostración. Sea $Z = 0$. Si $X = 0$ entonces $Y = 0$, pero $(0, 0, 0)$ no determina ninguna clase en el espacio proyectivo. Por otro lado si $X \neq 0$ podemos suponer que $X = 1$, de donde $Y^2 = f_6$, y asi considerar los puntos $(1 : \alpha : 0)$ y $(1 : -\alpha : 0)$ con $\alpha^2 = f_6$.
Ahora bien dichos puntos hacen parte de la geometría de la curva determinada por la ecuación en el modelo proyectivo, para ello veamos que los puntos determinados por α son no singulares. Para $X = 1$, tenemos la curva y sus derivadas parciales

$$\tilde{\mathcal{C}}(Y, Z) = Y^2 - f_6 - f_5Z - f_4Z^2 - f_3z^3 - f_2Z^4 - f_1Z^5 - f_0Z^6,$$
$$\frac{\partial\tilde{\mathcal{C}}}{\partial Y} = 2Y, \ \frac{\partial\tilde{\mathcal{C}}}{\partial Z} = -f_5 - 2f_4Z - 3f_3Z^2 - 4f_2Z^3 - 5f_1Z^4 - 6f_0Z^5,$$

con lo cual, $\frac{\partial\tilde{C}(\alpha,0)}{\partial Y} = 2\alpha$, $\frac{\partial\tilde{C}(\alpha,0)}{\partial Z} = -f_5$. Si el punto $(1 : \alpha : 0)$ fuese singular, tendríamos $\alpha = f_5 = 0$. Pero, en este caso, si $\alpha = 0 = f_5$ y dado que $\alpha^2 = f_6$, hecho que contradice el grado de f $deg(f) = 6$, así los puntos $(1 : \alpha : 0)$ y $(1 : -\alpha : 0)$ son no singulares. ■

Corolario 1.2.1 *Si* $char(K) \neq 2$, *entonces la curva hiperelíptica* $\mathcal{C} : y^2 = f(x)$ *con* $deg(f) = 5$ *tiene un único punto al infinito* $(1 : 0 : 0)$.

Definición 1.2.6 *Sea* $\mathcal{C} : y^2 = f(x)$ *con* $def(f) = 5$ *ó* 6 *una curva hiperelíptica de género 2. Denotamos los puntos al infinito por* $\infty^+ := (1 : \alpha^+ : 0)$ *y* $\infty := (1 : \alpha^- : 0)$, *(con* α^+ *y* α^- *raíces de* $\alpha^2 - f_6 = 0$*), cuando hay un solo punto en el infinito, lo denotamos por* $\infty = \infty^+ = \infty^- = (1 : \alpha : 0)$.

- *Si el punto al infinito es único, entonces la curva $\mathcal{C}$ es llamada un modelo ramificado de una curva hiperelíptica, o bien modelo real.*
- *Si hay dos puntos diferentes al infinito ∞^+, ∞^- con $\alpha^+, \alpha^- \in K$, $\mathcal{C}$ es llamada un modelo de descomposición de una curva hiperelíptica, o también modelo imaginario.*
- *Si $\alpha^+, \alpha^- \in \overline{K}$ entonces $\mathcal{C}$ es llamada un modelo inerte de una curva hiperelíptica.*

1.3. Cuerpos de funciones

Definición 1.3.1 *Para cualquier conjunto $X \subseteq \mathbb{P}^n(\overline{K})$ definimos:*

$$I_K(X) = \langle \{ f \in K[x_0, \ldots, x_n] \colon f \text{ es homogeneo y } f(P) = 0 \text{ para todo } P \in X \} \rangle.$$

Si X es una variedad definida sobre K entonces $I_K(X)$ es un ideal primo, luego el anillo de coordenadas es un dominio de integridad. Si X es afine podemos dar una interpretación como las funciones de X en K. Por otro lado si X es proyectivo el cociente f/g de polinomios no queda bien definido, sin embargo basta tomar f y g homogéneos del mismo grado.

Definición 1.3.2 *El ideal sobre K de un conjunto $X \subseteq \mathbb{A}^n(\overline{K})$ es*

$$I_K(X) = \left\{ f \in K[x_1, \ldots, x_n] \colon f(P) = 0, \text{para todo } P \in X(\overline{K}) \right\}.$$

Definición 1.3.3 *Sea X una variedad afín sobre K. El cuerpo de funciones denotado por $K(X)$ está dado por:*

$$K(X) = \left\{ \frac{f_1}{f_2} \colon f_1, f_2 \in K[X], f_2 \notin I_K(X) \right\},$$

donde $K[X] = K[x_1, \ldots, x_n]/I_K(X)$ es el anillo coordenado afín de X y bajo la relación de equivalencia, $\frac{f_1}{f_2} \sim \frac{f_3}{f_4}$ si y solo si $f_1 f_4 - f_3 f_2 \in I_K(X)$.

1.4. Anillos locales y anillos Noetherianos

Asociaremos ahora un anillo de funciones a una curva de género dos, con la intención de definir por un subgrupo del grupo abeliano libre formado por los puntos de la curva, o bien su base, que combina las valuaciones o valoraciones de una función en un punto de la curva hiperelíptica y así poder definir un grupo llamado el grupo de Picard.

Definición 1.4.1 *Un anillo local R es un anillo con un único ideal maximal; si $\mathfrak{m}$ es dicho ideal, entonces $R-\mathfrak{m}$ es el conjunto de las unidades de R.*

Definición 1.4.2 *Un anillo Noetheriano R es un anillo en el cual todo ideal es finitamente generado.*

Teorema 1.4.1 *Sea R un anillo conmutativo con unidad. Los siguientes enunciados son equivalentes:*

1. *R es Noetheriano.*
2. *Toda Familia no vacía de ideales de R tiene un elemento maximal.*
3. *R Satisface la condición de la cadena ascendente (C.C.A), esto es, toda cadena ascendente de ideales de R, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots \subseteq \cdots$ se estabiliza, es decir, existe $N \in \mathbb{N}$ tal que $I_{N+j} = I_N$ para todo $j \geq 0$.*

Demostración. 1) $\Rightarrow$ 2) Sea $\mathcal{F}$ una familia no vacía de ideales de R. Consideremos el poset $(\mathcal{F}, \subseteq)$; ahora sea $\{I_\alpha\}_{\alpha \in A}$ una cadena de $\mathcal{F}$, es decir un subconjunto totalmente ordenado. Como dichos ideales están encajados, entonces $J = \cup_{\alpha \in A} I_\alpha$. Como R es Noetheriano, entonces J es finitamente generado, luego existen $r_1, r_2, \ldots, r_k \in J$ tales que $J = (r_1, r_2, \ldots, r_k)$. Para cada $r_i \in J$ se tiene que $r_i \in I_{\alpha_i}$ con $i = 1, 2, \ldots, k$. Podemos suponer sin perdida de generalidad que $I_{\alpha_1} \subseteq I_{\alpha_2} \subseteq \cdots \subseteq I\alpha_k$, Pues bastaría permutar los índices y rendirá, siendo así, $r_1, r_2, \ldots, r_k \in I_{\alpha_k}$. Note que J es el menor ideal que contiene a $r_1, r_2, \ldots, r_k$, por ser el generado, luego $J \subseteq I_{\alpha_k}$ y claramente $I_{\alpha_k} \subseteq J$ así $J = I_{\alpha_k}$. Por tanto $J \in \mathcal{F}$, mas aun J es cota superior de $\{I_\alpha\}_{\alpha \in A}$ Luego del Lema de Zorn, concluimos que $\mathcal{F}$ tiene un elemento maximal.
2) $\Rightarrow$ 3) Supongamos que tenemos la cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ y consideremos la familia $\mathcal{F} = \{I_k\}_{k \in \mathbb{N}}$. Por hipótesis $\mathcal{F}$ tiene un elemento maximal,

sea I_N dicho elemento, luego por construcción $I_N \subseteq I_{N+j}$ para todo $j \geq 0$, y como I_N es maximal, entonces para todo $j \geq 0$, $I_N = I_{N+j}$, es decir, la cadena se estabiliza.
3) $\Rightarrow$ 1) Por reducción al absurdo, supongamos que existe $I \subseteq R$ que no es finitamente generado. Sea $x_1 \in I$, como I no es finitamente generado, entonces $(x_1) \subsetneq I$, luego existe $x_2 \in I$ tal que $x_2 \notin (x_1)$ por tanto $(x_1) \subsetneq (x_1, x_2) \subsetneq I$ repitiendo este razonamiento obtenemos $x_1, x_2, \ldots, x_n, \ldots \in I$ tales que $(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, x_2, \ldots, x_n) \subsetneq \cdots$ es una cadena de ideales que no se estabiliza, absurdo. ■

Definición 1.4.3 *Sea $\mathcal{C}$ una curva hiperlíptica de género 2 definida sobre K. Definimos el anillo local sobre K de $\mathcal{C}$ en un punto $P \in \mathcal{C}(K)$ como*

$$\mathcal{O}_{P,K}(\mathcal{C}) := \left\{ f \in K(\mathcal{C}) \colon f \text{ es regular en } P \right\}.$$

Lema 1.4.1 *Consideremos $\mathfrak{m}_{P,K}(\mathcal{C}) := \left\{ f \in K(\mathcal{C}) \colon f(P) = 0 \right\}$. Las siguiente afirmaciones son verdaderas:*

1. *$\mathcal{O}_{P,K}(\mathcal{C})$ es un anillo.*
2. *$\mathfrak{m}_{P,K}(\mathcal{C})$ es un $\mathcal{O}_{P,K}(\mathcal{C})$ ideal.*
3. *$\mathfrak{m}_{P,K}(\mathcal{C})$ es maximal.*
4. *$\mathcal{O}_{P,K}(\mathcal{C})$ es un anillo local.*

Demostración. Probemos que $\mathcal{O}_{P,K}(\mathcal{C})$ es Noetheriano. Sea $I \subseteq \mathcal{O}_{P,K}(\mathcal{C})$ un ideal, y definamos $J = I \cap K[\mathcal{C}]$. Es claro que J es un ideal de $K[\mathcal{C}]$. Del teorema de la base de Hilbert y del hecho de que si R es un anillo Noetheriano y M es un ideal de R, entonces R/M es Noetheriano se concluye que $K[\mathcal{C}] = K[x_1, \ldots, x_n]/I_K(\mathcal{C})$ es Noetheriano. De lo anterior, J es finitamente generado, digamos $J = (f_1, \ldots, f_m)$, entendiendo que los f_i pueden ser vistos en $K[\mathcal{C}]$, o también su clase en $K(\mathcal{C})$ según corresponda.

Afirmación: $f_1, \ldots, f_m$ generan a I.

Sea $g \in I \subseteq \mathcal{O}_{P,K}(\mathcal{C})$, como g esta definida en P, existen $g_1, g_2 \in K[C]$, tales que $g = g_1/g_2$ y $g_2(P) \neq 0$ luego que $g_2 \cdot g \in J$.
Se sigue que $g_2 \cdot g = r_1 f_1 + \cdots + r_m f_m$, con $r_i \in K[\mathcal{C}]$, así $g = \left(\sum_i r_i f_i\right)/b = \sum_i (r_i/b) f_i$, donde $r_i/b \in \mathcal{O}_{P,K}(\mathcal{C})$, pues $b(P) \neq 0$. Por tanto $I \subseteq (f_1, \ldots, f_m)$, por otro lado, cada $f_i \in I$, por como se definió J, concluimos que $J = (f_1, \cdots, f_m)$ en $\mathcal{O}_{P,K}(\mathcal{C})$.

Por otro lado veamos que $\mathfrak{m}_{P,K}(\mathcal{C})$ es maximal. Sea $g \in \mathcal{O}_{P,K}(\mathcal{C})$, como g es regular en P entonces $g(P) \in K$, así definimos la aplicación $\varphi_P(g) = g(P)$ que es fácil de verificar es un homomorfismo sobreyectivo, más aún, $Ker(\varphi_P) = \mathfrak{m}_{P,K}(\mathcal{C})$. Luego del primer teorema de isomorfismo

$$\mathcal{O}_{P,K}(\mathcal{C})/\mathfrak{m}_{P,K}(\mathcal{C}) \cong K.$$

Concluimos que $\mathfrak{m}_{P,K}(\mathcal{C})$ es maximal.

Ahora bien, cualquier función regular que no está en $\mathfrak{m}_{P,K}(\mathcal{C})$ no puede ser cero en P, lo que implica que pertenece a la unidad del anillo $\mathcal{O}_{P,K}(\mathcal{C})$. Así, todos los ideales maximales deben coincidir, y por lo tanto, $\mathcal{O}_{P,K}(\mathcal{C})$ es un anillo local. ■

Lema 1.4.2 *Sea $\mathcal{C}$ una curva hiperelíptica de género 2 y $P \in \mathcal{C}(K)$. Entonces $\mathfrak{m}_{P,K}(\mathcal{C})$ es un ideal principal.*

Definición 1.4.4 *Un uniformizador de P es un elemento $t_P \in \mathcal{O}_{P,K}(\mathcal{C})$ tal que $\mathfrak{m}_{P,K}(\mathcal{C}) = (t_P)$. Análogamente se define en $\mathcal{O}_{P,\overline{K}}(\mathcal{C})$.*

1.5. Valoración en un punto de una curva

En teoría de variedades algebraicas, las valoraciones juegan un papel fundamental en la definición de los divisores de Weil. Intuitivamente, una valoración mide el orden de anulación o de polos de funciones racionales en un punto específico de una variedad. Esto permite conectar el comportamiento local de funciones en la variedad con objetos algebraicos globales como los divisores.

Definición 1.5.1 *Sea K un cuerpo. Una valoración discreta en K es una función $v : K \to \mathbb{Z} \cup \{\infty\}$ tal que:*

1. *$v(fg) = v(f) + v(g)$, para todo $f, g \in K^*$.*
2. *Para todo $f, g \in K^*$ tal que $f + g \neq 0$, se tiene que $v(f+g) \geq min\{v(f), v(g)\}$.*
3. *$v(f) = \infty$ si y solo si $f = 0$.*

Ejemplo 1.5.1 ▪ *Sea K es un cuerpo, la función $v : K \to \{0, \infty\}$ con $v(0) = \infty$ y $v(x) = 0$ para todo $x \neq 0$ define una valoración.*

- *Sea $K=\mathbb{Q}$ y p un número primo, podemos escribir cualquier $x\in\mathbb{Q}^\times$ en una única forma como $p^v\frac{c}{d}$ con $c,d\in\mathbb{Z}$ y $mcd(c,d)=1$, tal que $p\nmid c,d$. Así, tomando $v_p(x)=v$ obtenemos una valoración llamada la valoración p-ádica.*

Lema 1.5.1 *Sea K un cuerpo y v una valuacíon discreta en K, entonces:*

1. $v(1)=0$.
2. *Si $f\in K^*$, entonces $v(1/f)=-v(f)$.*
3. $R_v:=\{f\in K^*:\ v(f)\geq 0\}\cup\{0\}$ *es un anillo (anillo de valoración).*
4. $\mathfrak{m}_v:=\{f\in K^*:\ v(f)>0\}$ *es un ideal maximal en R_v.*
5. *Si $f\in K^*$ es tal que $f\notin R_v$ entonces $1/f\in\mathfrak{m}_v$.*
6. R_v *es un anillo local.*

Demostración. Ver [15, Lem. 7.4.2] ■

Lema 1.5.2 *Sea $\mathcal{C}$ una curva de género 2 y $P\in\mathcal{C}(K)$. Para toda función no nula $f\in\mathcal{O}_{P,K}(\mathcal{C})$ existe $m\in\mathbb{N}$ tal que $f\notin\mathfrak{m}_{P,K}^m=\mathfrak{m}_{P,K}\cdots\mathfrak{m}_{P,K}$.*

Veamos que toda curva de género 2 es hiperelíptica, siendo así hablaremos de ahora en mas de curvas de género 2.

Proposición 1.5.1 *Sea K un cuerpo de característica 0 y $\mathcal{C}$ una curva proyectiva no singular definida sobre K de género mayor que 1. las siguientes condiciones son equivalentes:*

(i) Existe un $K-$morfismo $\pi:\mathcal{C}\to\mathbb{P}^1_K$ de grado 2.

(ii) Existe una $K-$ involución $w:\mathcal{C}\to\mathcal{C}$ tal que $\mathcal{C}/\langle w\rangle$ es $K-$isomorfa a $\mathbb{P}^1_K$.

Diremos que $\mathcal{C}$ es hiperelíptica si satisface alguna de estas condiciones.
Demostración. Veamos que (i) implica (ii). Debido a que la extensión $K(\mathcal{C})/\pi^*K(\mathbb{P}^1_K)$ tiene grado 2 y a que toda extensión de grado 2 en característica cero es de Galois, tenemos que el grupo de Galois de la extensión $K(\mathcal{C})/\pi^*K(\mathbb{P}^1_K)$ esta generado por un único elemento $\widehat{w}$ de orden 2. Esta automorfismo del grupo de Galois induce un automorfismo de $\mathcal{C}$, $w:\mathcal{C}\to\mathcal{C}$, de orden 2. Como $\widehat{w}$ deja fijo a $\pi^*K(\mathbb{P}^1_K)$, se tiene que $\pi\circ w=\pi$, así (i) implica (ii). La implicación de (ii) a (i) se sigue del hecho de que la proyección dada por $\pi:\mathcal{C}\to\mathcal{C}/\langle w\rangle$ tiene grado 2 y de que $\mathcal{C}/\langle w\rangle$ es isomorfo a $\mathbb{P}^1_K$. ■

Observación 1.5.1 *Obsérvese que π no está determinado de forma única, ya que podemos componerlo con un automorfismo de $\mathbb{P}^1_K$. Sin embargo, La involución w sí es canónica de la curva.*

Proposición 1.5.2 *Toda curva de género 2 es hiperelíptica.*

Demostración. Ver capitulo 7, [35, Prop. 1.10]. ■

Definición 1.5.2 *Sea $\mathcal{C}$ una curva de género 2, $P \in \mathcal{C}$ y sea $\mathfrak{m}_P := \mathfrak{m}_{P,K}(\mathcal{C})$. Fijamos $\mathfrak{m}_P^0 = \mathcal{O}_{P,K}(\mathcal{C})$. Sea $f \in \mathcal{O}_{P,K}(\mathcal{C})$ tal que $f \neq 0$. Definimos el orden de f en P como:*

$$v_P(f) := max\{m \in \mathbb{N}_0 \colon f \notin \mathfrak{m}_P^m\}.$$

Si $v(f) = 1$, diremos que f tiene un cero simple en P.

Lema 1.5.3 *Sea $\mathcal{C}$ una curva de género 2, $P \in \mathcal{C}(\overline{K})$, $t_p \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})$ un uniformizador en P, $f \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})$ con $f \neq 0$, entonces*

$$v_P(f) = \left\{n \in \mathbb{N}_0 \colon f/t_P^n \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})\right\}.$$

Así, $f = t_P^{v_p(f)}u$, con $u \in (\mathcal{O}_{P\overline{K}}(\mathcal{C}))^*$.

Observación 1.5.2 *Notemos que lo descrito anteriormente es la versión discreta del siguiente resultado clásico de funciones analíticas.*

Teorema 1.5.1 *Suponga que f es una función analítica no constante en un dominio D. Si $z_0 \in D$ es un cero de f, entonces z_0 tiene un orden finito $m \geq 1$ y existe una función analítica g en D tal que $g(z_0) \neq 0$ y*

$$f(z) = (z - z_0)^m g(z) \quad \textit{para todo } z \in D.$$

Esta similitud de las funciones analíticas o meromorfa con las funciones racionales se da pues históricamente la geometría algebraica clásica sobre $\mathbb{C}$ y trabajos posteriores se hicieron sobre cuerpos finitos.

Lema 1.5.4 *Sea $\mathcal{C}$ una curva de género 2, $P \in \mathcal{C}(\overline{K})$ y $f \in K(C)$. Entonces f puede ser escrita como f_1/f_2 donde $f_1, f_2 \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})$.*

Definición 1.5.3 *Sea $\mathcal{C}$ una curva de género 2, $f \in K(\mathcal{C})$. Un punto $P \in \mathcal{C}(\overline{K})$ es llamada un polo de f si $f \notin \mathcal{O}P,\overline{K}(\mathcal{C})$.*

Si $f = f_1/f_2$, con $f_1, f_2 \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})$ entonces podemos definir

$$v_p(f) := v_p(f_1) - v_p(f_2).$$

Lema 1.5.5 *Sea $\mathcal{C}$ una curva de género 2 y $f \in K(\mathcal{C})$. Si $P \in \mathcal{C}(\overline{K})$ es un polo de f entonces $v_p(f) < 0$ y P es un cero de $1/f$.*

Demostración. Sea $f \in K(\mathcal{C})$ y consideremos $f \equiv f_1/f_2$, con $f_1, f_2 \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})$. Como $P \in \mathcal{C}(\overline{K})$ es un polo de f, entonces $f \notin \mathcal{O}_{P,\overline{K}}(\mathcal{C})$, en particular $f_2(P) = 0$.
Siendo así $\left(\frac{1}{f}\right)(P) = \frac{f_2(P)}{f_1(P)} = 0$, también notemos que si $m = v_P(f_1)$ y $n = v_P(f_2)$ existen $u_1, u_2 \in (\mathcal{O}_{P,\overline{K}}(\mathcal{C}))^*$ tales que

$$f \equiv \frac{f_1}{f_2} = \frac{t_p^m u_1}{t_p^n u_2} = t_p^{m-n} u.$$

Si $m > n$ entonces $f(P) = 0$ pero por hipótesis sabemos que P es un polo de f, luego $m < n$,

$$\frac{1}{f} \equiv \frac{f_2}{f_1} = \frac{t_p^n u_2}{t_p^m u_1} = t_p^{n-m} u.$$

Se sigue que P es un cero de $\frac{1}{f}$ y $v_P(f) = m - n < 0$. ■

Teorema 1.5.2 *Sea $\mathcal{C}$ una curva de género 2 y $P \in \mathcal{C}(\overline{K})$. Entonces, v_p es una valoración discreta en $K(\mathcal{C})$; más aún se tiene las siguientes propiedades:*

1. *Si $f \in \overline{K}(\mathcal{C})^*$ y $f \in \overline{K}^*$, entonces $v_p(f) = 0$.*
2. *Sean $c \in \overline{K}$ y $f \in K(\mathcal{C})$. Si $v_P(f) < 0$, entonces $v_P(f + c) = v_P(f)$.*
3. *Sean $f_1, f_2 \in K(\mathcal{C})^*$ tales que $v_P(f_1) \neq v_P(f_2)$, entonces $v_P(f_1 + f_2) = min\{v_P(f_1), v_P(f_2)\}$.*

Demostración. Ver [19, Cor. I.6.6] y [31, Thm. VI9.1]. ■

1.6. Cuerpo de funciones para género 2

Sea $\mathcal{C} : y^2 = f(x)$ una curva de género 2, recordemos la construcción del cuerpo de funciones de una variedad algebraica 1.3.3. Fijemos $\mathcal{C}(x,y) = y^2 - f(x)$ y consideremos $X = V(\mathcal{C}(x,y))$ la variedad afín. Definimos el anillo de coordenadas $K[C] = K[x,y]/I_K(X)$, donde $I_K = (\mathcal{C}(x,y))$, además suponemos $deg(f) = 5$ para tener un único punto al infinito.

Observación 1.6.1 *Notemos que cada $g(x,y) \in K[\mathcal{C}]$ puede ser escrito como $g(x,y) = a(x) - b(x)y$, con $a(x), b(x) \in K[x]$, además esta representación es única.*

Demostración. Sea $g(x,y) \in K[\mathcal{C}]$ y consideremos los monomios de la forma $m_{ij}x^i y^j$ con $m_{ij} \in K$. Si j es par

$$m_{ij}x^i y^j = m_{ij}x^i y^{2s} = m_{ij}x^i (y^2)^s = m_{ij}x^i f(x)^s \in K[x].$$

Si j es impar realizamos el mismo razonamiento y obtenemos que $m_{ij}x^i y^j = m_{ij}x^i y^{2s+1} = m_{ij}x^i f(x)^s y \in yK[x]$.

Así, tras algunos reordenamientos

$$g(x,y) = \sum_{ij} m_{ij}x^i y^j = \sum_t m_t x^t - \sum_q (-m_q)x^q f(x)^q y = a(x) - b(x)y.$$

Dicha escritura es única, es decir dados $a(x), a'(x), b(x), b'(x) \in K[x]$, donde $g(x,y) = a(x) - b(x)y = a'(x) - b'(x)y$, entonces $a(x) = a'(x)$ y $b(x) = b'(x)$. Supongamos que las expresiones que representan a $g(x,y)$ son iguales, basta tener presente que dicha ecuación esta vista en $K[x,y]$. Luego tenemos que $(b(x) - b'(x))y = a(x) - a'(x) \in K[x]$, lo cual solo es posible si $b(x) = b'(x)$ y por tanto $a(x) = a'(x)$. ■

Definición 1.6.1 *Dado $g(x,y) = a(x) - b(x)y \in K[\mathcal{C}]$, consideremos $\overline{g}(x,y) = a(x) + b(x)y$. Definimos $N(g) = g\overline{g} = a^2(x) - b^2(x)f(x) \in K[x]$.*

Observación 1.6.2 *Sea $P = (\tilde{x}, \tilde{y}) \in \mathcal{C}$. Suponga que $g(x,y) = a(x) - b(x)y \in \overline{K}[\mathcal{C}]^*$ tiene un cero en P y que $\tilde{x}$ no es raíz de ambos $a(x)$ y $b(x)$. Entonces $\overline{g}(P) = 0$ si y solo si $\tilde{y} = 0$.*

Demostración. Supongamos que $\overline{g}(P) = 0$. Por hipótesis P es cero de g entonces obte-

nemos las siguientes dos ecuaciones

$$a(\tilde{x}) + b(\tilde{x})\tilde{y} = 0,$$
$$a(\tilde{x}) - b(\tilde{x})\tilde{y} = 0.$$

Sumando y restando ambas ecuaciones obtenemos respectivamente que $2a(\tilde{x}) = 0$ y $2b(\tilde{x})\tilde{y} = 0$ como $char(K) \neq 2$, obtenemos así que $a(\tilde{x}) = b(\tilde{x})\tilde{y} = 0$. Sabemos que $\tilde{x}$ no puede ser raíz de a y b simultáneamente, es decir, $b(\tilde{x}) \neq 0$, por tanto concluimos que $\tilde{y} = 0$. Recíprocamente, supongamos que $\tilde{y} = 0$. Como $g(\tilde{x}, \tilde{y}) = 0$, se sigue que $a(\tilde{x}) = b(\tilde{x})\tilde{y} = 0$, con lo cual $P = (\tilde{x}, \tilde{y})$ es cero de $\overline{g}$. ■

Lema 1.6.1 *Sea $P = (\tilde{x}, \tilde{y}) \in \mathcal{C}$ con $\tilde{y} \neq 0$ y $g(x, y) = a(x) - b(x)y \in \overline{K}[\mathcal{C}]^*$. Suponga que $g(P) = 0$ y que $\tilde{x}$ no es raíz $a(x)$ y $b(x)$ simultáneamente. Entonces $g(x, y) = (x - \tilde{x})^s l(x, y)$, donde s es la mayor potencia de $(x - \tilde{x})$ que divide a $N(g)$ y tal que $l(x, y) \in \overline{K}(\mathcal{C})$ no tiene polos ni ceros en P.*

Demostración. Podemos escribir

$$g = g \cdot \frac{\overline{g}}{\overline{g}} = \frac{N(g)}{\overline{g}} = \frac{a^2 - b^2 f}{a + by}.$$

Sea s la mayor potencia de $x - \tilde{x}$ que divide a $N(g)$, luego $N(g) = (x - \tilde{x})^s d(x)$ con $d(\tilde{x}) \neq 0$. De la observación anterior, se sigue que $\overline{g}(P) \neq 0$, con lo cual basta definir $l(x, y) = \dfrac{d(x)}{\overline{g}}$ de donde $g = (x - \tilde{x})^s l(x, y)$ con $l(P) \neq 0, \infty$. ■

Lema 1.6.2 *Sea $P = (\tilde{x}, 0) \in \mathcal{C}$. Entonces $x - \tilde{x} = y^2 s(x, y)$, donde $s(x, y) \in \overline{K}(\mathcal{C})$ no tiene ni polos ni ceros en P.*

Demostración. Basta definir $s(x, y) := \dfrac{x - \tilde{x}}{y^2}$ y notar que como $P = (\tilde{x}, 0)$ no es singular, entonces $f'(\tilde{x}) \neq 0$ y $f(\tilde{x}) = 0$. Como $\dfrac{1}{s(x, y)} = \dfrac{f(x)}{x - \tilde{x}}$, sabemos que $x - \tilde{x}$ divide a $f(x)$, pero como $f'(\tilde{x}) \neq 0$, entonces $(x - \tilde{x})^2$ no divide a f. Así, $s(P) \neq 0, \infty$, y por lo anterior, tenemos que

$$s(x, y) = \frac{x - \tilde{x}}{f(x)} = \frac{x - \tilde{x}}{(x - \tilde{x})\tilde{f}(x)} = \frac{1}{\tilde{f}(x)},$$

con $\tilde{f}(\tilde{x}) \neq 0$. ■

Uniformizador en género 2 Sea $\mathcal{C} : y^2 = f(x)$ una curva de género 2, $P \in \mathcal{C}$ y t_P un uniformizador en P. Tenemos que $t_p(P) = 0$ y para cada $f \in K(\mathcal{C})$ (o bien $\mathcal{O}_{p,\overline{K}}(\mathcal{C})^*$), existe un $d \in \mathbb{Z}$ y $u \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})^*$, $(u(P \neq 0, \infty))$, tal que $f = t_p^d u$ con $d = v_p(f)$.

Observación 1.6.3 *De los lemas anteriores, podemos obtener formas explícitas de los uniformizadores, a saber:*

- *Si* $P = \infty$, *entonces* $t_P = \frac{x^2}{y}$.
- *Si* $P = (\tilde{x}.\tilde{y})$, $\tilde{y} \neq 0$ *entonces* $t_P = x - \tilde{x}$.
- *Si* $P = (\tilde{x}, 0)$, *entonces* $t_P = y$.

Definición 1.6.2 *Si* $f = t_p^d u$ *con* $u(P) \neq 0$ *y* $u(P) \neq \infty$*:*

- *Si* $d > 0$ *decimos que* f *tiene un cero de orden* $d = v_P(f)$.
- *Si* $d < 0$, *decimos que* f *tiene un polo de orden* $|d|$ *en* P.

1.7. Divisores

Queremos ahora definir una ley de suma para los puntos de nuestra curva hiperelíptica haciendo de $\mathcal{C}$ un grupo. Cabe resaltar que el método de la cuerda y la tangente utilizado para las curvas elípticas no puede ser empleado en este caso. Daremos el desarrollo teórico para construir el grupo, sin embargo veamos la idea intuitiva y geométrica que describe la situación.

Curvas elípticas

Una curva elíptica definida sobre un cuerpo K tiene una ecuación $\mathcal{C} : y^2 = f(x)$, donde $deg(f) = 3$ ó $4, char(K) \neq 2$.

Si $f(x)$ es un polinomio de grado 3, es decir, $f(x) = ax^3 + bx^2 + cx + d$, entonces la ecuación $y^2 = f(x)$ define una curva elíptica si y solo si el discriminante

$$\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$$

es no nulo.

Así mismo, si $f(x)$ es de grado 4, es decir, $f(x) = ax^4 + bx^3 + cx^2 + dx + e$, entonces $y^2 = f(x)$ define una curva elíptica si y solo si el discriminante

$$\Delta = 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e - 27a^2d^4$$

$$+144ab^2ce^2 - 6ab^2d^2e - 80abc^2de + 18abcd^3 + 16ac^4e - 4ac^3d^2$$

$$-27b^4e^2 + 18b^3de - 4b^3c^2e - 4b^2c^3d + b^2c^4$$

es no nulo.

Este discriminante mide si $f(x)$ tiene raíces múltiples. Si $\Delta = 0$, la curva tiene una singularidad y no es una curva elíptica.

Si tomamos $\mathcal{O} = \infty$. Podemos entonces definir un grupo de la siguiente manera:

- Dados $P, Q \in \mathcal{C}$, construimos la recta l que pasa por P y Q.
- l intercepta a $\mathcal{C}$ en un tercer punto R. Tomamos $P \bigoplus Q$ como el punto simétrico a R respecto el eje x.

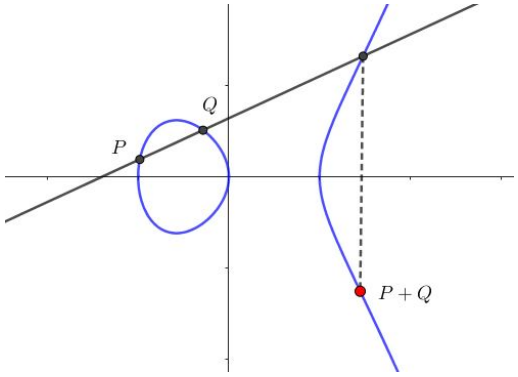


Figura 1.1: Suma en la curva elíptica

Una curva de género 1 con estructura de grupo es llamada **curva elíptica**.

género 2

Sea $\mathcal{C}$ una curva de género 2 como en 1.1.1, el infinito es un punto de Weierstrass en $\mathcal{C}$. A la curva $\mathcal{C}$ no podemos dotarla de estructura de grupo por si sola, sin embargo puede ser inyectada en un grupo llamado el $Jacobiano$ de $\mathcal{C}$:

$$\mathcal{C} \hookrightarrow \mathcal{J}(\mathcal{C}) \hookrightarrow \mathcal{C} \times \mathcal{C}.$$

Podemos entonces identificar los elementos de $J(\mathcal{C})$ como "parejas ordenadas" $(P_1, P_2) \in \mathcal{C} \times \mathcal{C}$, sobre cierta relación de equivalencia.

Consideremos entonces $D_1, D_2 \in \mathcal{J}(\mathcal{C})$ tales que $D_1 = (P_1, P_2), D_2 = (P_3, P_4)$, con $P_1, P_2, P_3, P_4 \in C$.

Para definir $D_1 \bigoplus D_2$ determinamos por interpolación de Lagrange una curva $\mathcal{C}'$: $y = g(x)$, con $deg(x) = 3$, tal que pasa por los puntos $P_1, P_2, P_3 y P_4 \in C$. Más aún, por el teorema de Bezout, la cubica intercepta a $\mathcal{C}$ en exactamente 6 puntos.

Obtenemos entonces puntos $P_5, P_6 \in \mathcal{C} \cap \mathcal{C}'$, con lo cual podemos definir $D_1 \bigoplus D_2 := (P_5', P_6')$ donde P_5' y P_6' son los puntos simétricos respecto al eje y de P_5 y P_6 respectivamente.

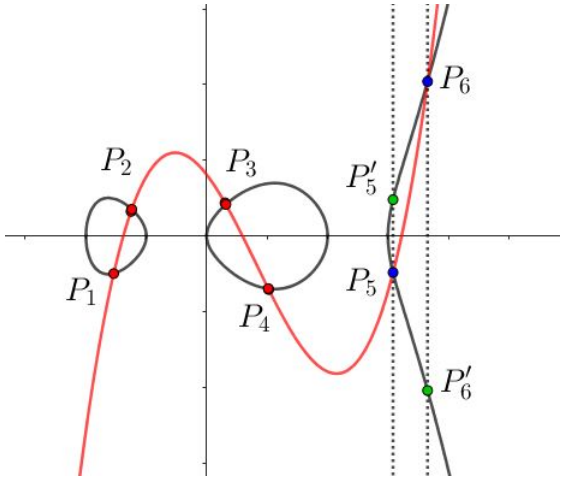


Figura 1.2: Suma en J(C)

Definición 1.7.1 *Sea $\mathcal{C}$ una curva de género 2 definida sobre un cuerpo K. Un divisor en $\mathcal{C}$ es una suma formal*

$$D = \sum_{P \in C(\overline{K})} n_p \cdot P,$$

con $n_p \in \mathbb{Z}$ y solo finitos n_p siendo no nulos. Si todos los $n_p = 0$, escribimos $D = 0$.

El soporte de D esta dado por $supp(D) = \{P \in C(\overline{K}) : n_P \neq 0\}$.

Definición 1.7.2 *Denotamos por $Div_{\overline{K}}(\mathcal{C})$ al conjunto de todos los divisores en $\mathcal{C}$.*

Definición 1.7.3 *Si $\tilde{D} = \sum_{P \in C(\overline{K})} n_p' \cdot P$, definimos $D - \tilde{D} := \sum_{P \in C(\overline{K})} (n_P - n_p') \cdot P$*

Diremos que $D \geq 0$ si $n_P \geq 0$ para todo $P \in supp(D)$. En tal caso, diremos que D es un divisor efectivo.

Definición 1.7.4 *Definimos el grado de un divisor $D = \sum_{P \in C(\overline{K})} n_p \cdot P$ como el entero $\sum_{P \in C(\overline{K})} n_p$, el que denotaremos como deg (D). Definimos el conjunto*

$$Div^0_{\overline{K}}(\mathcal{C}) := \left\{ D \in Div_{\overline{K}}(\mathcal{C}) \colon deg(D) = 0 \right\}.$$

Teorema 1.7.1 *$Div_{\overline{K}}(\mathcal{C})$ es un grupo aditivo y $Div^0_{\overline{K}}(\mathcal{C})$ es un subgrupo de $Div_{\overline{K}}(\mathcal{C})$.*

Demostración. $Div_{\overline{K}}(\mathcal{C})$ es un grupo abeliano libre generado por los puntos de $\mathcal{C}$. ■

Definición 1.7.5 *Sea $D = \sum_{P \in C(\overline{K})} n_p \cdot P \in Div_{\overline{K}}(\mathcal{C})$. Para $\sigma \in Gal(\overline{K}/K)$ definimos*

$$\sigma(D) = \sum_{P \in C(\overline{K})} n_p \cdot \sigma(P) \in Div_{\overline{K}}(\mathcal{C}),$$

donde $\sigma(P) = (\sigma(x), \sigma(y))$, si $P = (x, y)$. Si para todo $\sigma \in Gal(\overline{K}/K)$, $\sigma(D) = D$, decimos que D esta definido sobre K. Denotaremos por $Div_K(\mathcal{C})$ al conjunto de los divisores definidos sobre K.

Observación 1.7.1 *Sea K'/K la extensión finita generada por todas las coordenadas de todos los $P \in sup(D)$ y denotemos por K'' a la clausura de Galois de K'. Para verificar la definición anterior, bastaría considerar cualquier $\sigma \in gal(\overline{K}/K)$ tal que $\sigma(K'') = K''$. De esta forma, basta estudiar estudiar la acción de $\sigma \in Gal(K''/K)$.*

Definición 1.7.6 *Sean $P(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ y $Q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$, polinomios con coeficientes en un cuerpo. Definimos el resultante entre P*

y Q, denotado por Res(P,Q), como el determinante de la matriz de Sylvester:

$$S(f,g)=\begin{pmatrix} a_m & a_{m-1} & a_{m-2} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & 0 & a_m & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ b_n & b_{n-1} & b_{n-2} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & 0 & b_n & \cdots & b_2 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_n & b_{n-1} & \cdots & b_1 & b_0 \end{pmatrix}.$$

Observación 1.7.2 *Existe además una variación a dicha matriz, la cual es la matriz de* $(n+m)\times(m+n)$ *dada por,*

$$S(f,g)=\begin{pmatrix} a_m & & & b_n & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_m & \vdots & & \ddots & \\ \vdots & & \vdots & b_0 & & & b_n \\ a_0 & & \vdots & & \ddots & & \vdots \\ & \ddots & \vdots & & & \ddots & \vdots \\ & & a_0 & & & & b_0 \end{pmatrix}.$$

Ejemplo 1.7.1

1. *Sean* $f(x)=x-a$ *y* $g(x)=x-b$, *entonces*

$$Res(f,g)=det\begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix}=a-b.$$

2. *Sean* $f(x)=x-a$ *y* $g(x)=b_nx^n+\cdots+b_1x+b_0$, *entonces*

$$Res(f,g)=det\begin{pmatrix} 1 & & & b_n \\ -a & \ddots & & b_{n-1} \\ & \ddots & 1 & \vdots \\ & & -a & b_0 \end{pmatrix}=g(a).$$

Observación 1.7.3 *Notemos que en estos ejemplos se cumple que* $Res(f,g) = 0$ *si y solo si a es raíz de* g*, es decir* f *y* g *comparten una raíz. El siguiente teorema resalta lo anterior y da la importancia al resultante de dos polinomios.*

Teorema 1.7.2 *Sea* $f, g \in K[x]$*. Las siguientes afirmaciones son equivalentes:*

1. $Res(f,g) = 0$.
2. $deg(mcd(f,g)) \geq 1$.
3. *Existe* $a \in \overline{K}$*, tal que* $f(a) = g(a) = 0$.

Demostración. Ver [24, Thm. 1.3]. ■

Observación 1.7.4 *Sean* $f, g \in K[x]$*, tales que los términos independientes de* f *y* g *son no nulos. Entonces* $Res(f,g) = 0$*, si y solo si,* f *y* g *tienen un cero común en* $\overline{K}$.

Teorema 1.7.3 *Sea* $\mathcal{C}$ *una curva de género 2 sobre* K *y* $f \in K(\mathcal{C})^*$*, entonces* f *tiene finitos polos y ceros.*

Demostración. Sea $f = \frac{f_1(x,y)}{f_2(x,y)} \in K(\mathcal{C})^*$, con $f_1, f_2 \in K[\mathcal{C}]$. Los polos de f están contenidos en $\mathcal{C} \cap V(f_2)$, como el resultante $Res_x(f_2(x,y), \mathcal{C}(x,y))$ es un polinomio en la variable y con una cantidad finita de raíces, entonces $\mathcal{C} \cap V(f_2)$ es finito, por tanto hay un numero finto de polos.

Los ceros de f están contenidos en $\mathcal{C} \cap (V(f_1) \cup V(f_2))$ y se sigue del mismo razonamiento anterior que f tiene finitos ceros. ■

Definición 1.7.7 *Sea* $f \in \overline{K}(\mathcal{C})^*$*, definimos el divisor de* f *por*

$$div(f) = \sum_{P \in \mathcal{C}(\overline{K})} v_P(f) \cdot P,$$

para v_p *definido por 1.5.3. Los divisores de funciones son llamados divisores principales y los denotamos por*

$$Prin_{\overline{K}}(\mathcal{C}) = \left\{ div(f) \colon f \in \overline{K}(\mathcal{C})^* \right\}.$$

Teorema 1.7.4 *Sea* $\mathcal{C}$ *una curva de género 2 sobre* K *y* $f \in K(\mathcal{C})$ *entonces* $deg(div(f)) = 0$*. Más precisamente,* f *tiene el mismo numero de polos que de ceros.*

Demostración. Ver [19, Ch.2, Cor. 6.10], [44, Prop. 3.1]. ■

Lema 1.7.1 *Sea $\mathcal{C}$ una curva de género 2 sobre K y $f \in K(\mathcal{C})^*$, entonces :*

1. $div(ff') = div(f) + div(f')$.
2. $div(1/f) = -div(f)$.
3. $div(f+f') \geq \sum_P min\{v_P(f), v_P(f')\}(P)\}$.
4. $div(f^n) = n \cdot div(f)$, *para todo* $n \in \mathbb{Z}$.

Demostración. Sean $f, f' \in K(\mathcal{C})^*$

1. Notemos primero que si $g \in K(\mathcal{C})^*$, entonces existe un $m \in \mathbb{Z}$, tal que $g = t_p^m u$ donde $u \in \mathcal{O}_{p,\overline{K}}(\mathcal{C})$ y $t_p \in \mathcal{O}_{P,\overline{K}}(\mathcal{C})$ un uniformizador.

   Asi, $f = t_p^m u_1$, $f' = t_p^n u_2$, con $u_1, u_2 \in \mathcal{O}_{p,\overline{K}}(\mathcal{C})^*$, luego $u_1 u_2 \in \mathcal{O}_{p,\overline{K}}(\mathcal{C})^*$, y

   $$v_p(ff') = v_p(t_p^m u_1 t_p^n u_2) = v_p(t_p^{m+n} u_1 u_2) = m+n = v_p(f) + v_p(f')$$

   con lo cual,

   $$\begin{aligned} div(ff') &= \sum_{P \in \mathcal{C}(\overline{K})} v_p(ff') \cdot P, \\ &= \sum_{P \in \mathcal{C}(\overline{K})} (v_p(f) + v_p(f')) \cdot P, \\ &= \sum_{P \in \mathcal{C}(\overline{K})} v_p(f) \cdot P + \sum_{P \in C(\overline{K})} v_p(f') \cdot P, \\ &= div(f) + div(f'). \end{aligned}$$

2. Sea $f \in K(\mathcal{C})^*$, utilizando la propiedad anterior aplicada a f y $1/f$ obtenemos, $\mathbf{0} = div(1) = div(f/f) = div(f) + div(1/f)$, de donde $div(1/f) = -div(f)$.

3. Recordemos que si $f, g \in K(\mathcal{C})^*$ con $f \neq g$ no nulas, entonces

   $$v_p(f+g) \geq min\{v_p(f), v_p(g)\}.$$

En efecto, supongamos sin pérdida de generalidad que $v_p(f) = n \geq m = v_p(g)$, entonces podemos escribir $f = t_p^n u, g = t_p^m u'$, como en i), luego

$$v_p(f+g) = v_p\left(t_p^m u'\left(\frac{u}{u'}t_p^{n-m}+1\right)\right) \geq v_p(t_p^m u') + v_p(\frac{u}{u'}t_p^{n-m}+1) \geq v_p(t_p^m u') = m,$$

pues $\frac{u}{u'}t_p^{n-m}+1 \in \mathcal{O}_{p,\overline{K}}(\mathcal{C})$, entonces $v_p(\frac{u}{u'}t_p^{n-m}+1) \geq 0$. Por tanto,

$$\begin{aligned} div(f+f') &= \sum_p v_P(f+f')\cdot P, \\ &\geq \sum_p min\{v_p(f), v_p(f')\}\cdot P. \end{aligned}$$

4. Sea $f \in K(\mathcal{C})^*$ y $n \in \mathbb{N}$. Por inducción, si $n = 0$ entonces $div(f^0) = div(1) = \mathbf{0} = 0 \cdot div(f)$. Supongamos que la afirmación vale tiene para n, veamos el resultado para $n+1$. Se tiene que:

$$div(f^{n+1}) = div(f^n f) = div(f^n) + div(f) = n \cdot div(f) + div(f) = (n+1)div(f).$$

Sea $n < 0$, luego $-n \in \mathbb{N}$. Por lo anterior tenemos que $div(f^{-n}) = -n \cdot div(f)$, o bien $n \cdot div(f) = -div(f^{-n})$ y de 2), $div(1/g) = -div(g)$, de donde

$$n \cdot div(f) = -div(f^{-n}) = -div(1/f^n) = div(f^n).$$

■

Observación 1.7.5 (Divisores de Weil y divisores de Cartier) *A continuación, hacemos un comentario respecto a dos clases fundamentales de divisores que se utilizan en geometría algebraica: los* ***divisores de Weil*** *y los* ***divisores de Cartier****. Ambas nociones son herramientas esenciales para describir divisores en variedades algebraicas, y aunque tienen definiciones diferentes, están relacionadas en varios contextos. Presentamos sus definiciones, una comparación y un breve contexto histórico:*

- ***Divisores de Weil:*** *Un* divisor de Weil *D en una variedad irreducible X es una combinación formal de subvariedades irreducibles de codimensión 1:*

$$D = \sum_Z n_Z [Z],$$

donde:

- *Z es una subvariedad irreducible de codimensión 1.*
- *$n_Z \in \mathbb{Z}$ es un coeficiente entero, que refleja el orden de anulación o de polo en Z.*

- ***Divisores de Cartier:*** *Un* divisor de Cartier *D en una variedad X es un conjunto de datos locales $\{(U_i, f_i)\}$, donde:*

  - *$\{U_i\}$ es un recubrimiento abierto de X.*
  - *$f_i \in K^*$ son funciones racionales no nulas definidas en U_i.*
  - *En las intersecciones $U_i \cap U_j$, los cocientes f_i / f_j satisfacen:*

$$f_i / f_j \in \mathcal{O}_X^*(U_i \cap U_j),$$

  es decir, son funciones regulares y no nulas.

  Los divisores de Cartier están asociados a secciones globales del haz invertible $\mathcal{O}(D)$, reflejando su naturaleza algebraica.

Comparación:

Aspecto	***Divisores de Weil***	***Divisores de Cartier***
Definición	*Combinaciones formales de subvariedades irreducibles.*	*Asociados a haces invertibles $\mathcal{O}(D)$.*
Naturaleza	*Geométrica (centrada en subvariedades).*	*Algebraica (centrada en funciones y haces).*
Contexto	*Usados en cuerpos finitos o variedades no suaves.*	*Usados en $\mathbb{C}$ o $\mathbb{R}$, y variedades suaves.*
Requisitos	*Pueden definirse en variedades singulares.*	*Requieren suavidad para coincidir con los de Weil.*
Relación	*En variedades suaves, son equivalentes.*	*En variedades singulares, pueden diferir.*

Relación: *En variedades* suaves*, los divisores de Weil y de Cartier son equivalentes: todo divisor de Weil puede ser asociado a un divisor de Cartier y viceversa. Sin embargo, en variedades* singulares*, los divisores de Weil son más generales, ya que pueden existir divisores de Weil que no sean de Cartier.*

Contexto histórico:

- ***Divisores de Cartier:*** *Surgieron primero, en el contexto de la geometría algebraica clásica sobre $\mathbb{C}$.*

- *En el siglo XIX, los trabajos de Riemann y Dedekind exploraron el vínculo entre funciones racionales y divisores en curvas algebraicas. Esto culminó en el teorema de Riemann-Roch.*
- *En los años 1950, Cartier y Serre formalizaron el concepto usando haces invertibles y secciones globales, consolidando su enfoque algebraico.*

- ***Divisores de Weil:*** *Fueron introducidos por André Weil en los años 1940 como parte de su enfoque algebraico para estudiar variedades definidas sobre cuerpos finitos. Su generalidad los hace adecuados para trabajar con variedades singulares o sobre cuerpos arbitrarios.*

Este desarrollo histórico refleja la evolución de la geometría algebraica, desde el análisis clásico en $\mathbb{C}$ hasta el enfoque moderno basado en cuerpos arbitrarios y esquemas.

1.8. Grupo de clases de divisores

El grupo de clases de divisores definidos sobre cuerpos finitos es fundamental debido a su relevancia en la teoría de números, la criptografía de curva elíptica y la conexión entre la teoría de números y la geometría algebraica. Proporciona herramientas esenciales para abordar problemas de seguridad y eficiencia en aplicaciones criptográficas sobre cuerpos finitos.

Observación 1.8.1 *De ahora en adelante, consideraremos K un cuerpo finito.*

Definición 1.8.1 *El grupo de divisores de clase de una curva $\mathcal{C}$ sobre K es*

$$Pic_K^0(\mathcal{C}) := Div_K^0(\mathcal{C})/Prin_K(\mathcal{C}).$$

y es llamado también el grupo de Picard de $\mathcal{C}$. Los divisores $D_1, D_2 \in Div_K^0(\mathcal{C})$ son linealmente equivalentes si $D_1 - D_2 \in Prin_K(\mathcal{C})$ y escribimos $D_1 \equiv D_2 mod Prin_K^0(\mathcal{C})$. La clase de divisor de un divisor $D \in Div_K^0(\mathcal{C})$ es denotada por $[D]$.

Divisores afines efectivos

Definición 1.8.2 *Sea $\mathcal{C}$ una curva de género 2 y denotemos por $\mathcal{C} \cap \mathbb{A}^2$ la curva afín. Un divisor efectivo en $\mathcal{C}$, es un divisor D tal que:*

$$D = \sum_{P \in (\mathcal{C} \cap \mathbb{A}^2)(\overline{K})} n_p \cdot P, \ \ n \geq 0.$$

Definición 1.8.3 *Un divisor D es semi reducido si:*

1. *D es efectivo.*
2. *Si $P = i(P)$ para $P = (x, y)$, e i la involución definida en 1.2.5, entonces $n_p = 1$.*
3. *Si $P \neq i(P)$, tal que $n_P > 0$, entonces $n_{i(P)} = 0$.*

Observación 1.8.2 *Notemos que si $P = i(P)$, con $P = (x, y)$, entonces $y = 0$, así la segunda condición pude formularse como: Si $P = (x, 0)$ entonces $n_p = 1$.*

En esencia un divisor es semi reducido si cualquier punto igual a su involución tiene una ocurrencia de 1 y en caso contrario, alguna de las ocurrencias de P o $i(P)$ es nula.

Observación 1.8.3 *Es posible probar que si $D_1, D_2 \in Div^0_{\overline{K}}(\mathcal{C})$, entonces existe $f \in \overline{K}(\mathcal{C})$ tal que $D_1 = D_2 + div(f)$.*

Observación 1.8.4 *Sea $g(x) = \prod_j (x - a_j)^{c_j} \in K[x]$, entonces*

$$div(g) = \sum_j c_j (P_j + i(P_j) - 2 \cdot \infty),$$

donde $P = \left(a_j, \sqrt{f(a_j)}\right)$ y $i(P) = \left(a_j, -\sqrt{f(a_j)}\right)$.

Lema 1.8.1 *Cada divisor en $\mathcal{C}$ es equivalente a un divisor semi reducido.*

Demostración. Ver [15, Lem. 10.3.3]. ■

Ejemplo 1.8.1 *Sea $\mathcal{C}$ una curva de género 2 y $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in \mathcal{C}$, con $x_1 \neq x_2$. Consideremos el divisor $D = -1 \cdot P_1 + 2 \cdot P_2 + 1 \cdot i(P_2)$ el cual no es semi reducido. Primero, para que sea efectivo consideremos $div(x - x_1) = 1 \cdot P_1 + 1 \cdot i(P_1) - 2\infty$, así*

$$\begin{aligned} D + div(x - x_1) &= -1 \cdot P_1 + 2 \cdot P_2 + 1 \cdot i(P_2) + 1 \cdot P_1 + 1 \cdot P_1 - 2 \cdot \infty, \\ &= 1 \cdot i(P_1) + 2 \cdot P_2 + 1 \cdot i(P_2) - 2 \cdot \infty. \end{aligned}$$

Ahora bien para anular la ocurrencia simultanea de P_2 y $i(P_2)$ consideremos

$$\begin{aligned} D + div(x - x_1) - div(x - x_2) &= 1 \cdot i(P_1) + 2 \cdot P_2 + 1 \cdot i(P_2) - 2 \cdot \infty - (1 \cdot P_2 + 1 \cdot i(P_2) - 2\infty), \\ &= 1 \cdot i(P_1) + 1 \cdot P_2. \end{aligned}$$

Finalmente tenemos que,

$$\begin{aligned} D' &= D + div(x - x_1) - div(x - x_2), \\ &= D + div\left(\frac{x - x_1}{x - x_2}\right). \end{aligned}$$

es semi reducido.

Proposición 1.8.1 *Sean $\mathcal{C} : y^2 = f(x)$, $v(x) \in K[X]$ tales que $f(x) - v(x)^2 = \prod_j (x - a_j)^{d_j}$. Entonces*

$$div(y - v(x)) = \sum_j d_j \cdot ((a_j, b_j) - \infty),$$

donde $b_j = v(a_j)$. Si además, $b_j = 0$ entonces $d_j = 1$.

Demostración. Consideremos la función $y - v(x)$, analicemos que pasa con su ceros, de tenerlos. Sea $P = (a, b)$ un punto de la curva $\mathcal{C}$, donde $b \neq 0$, y supongamos que $y - v(x)$ se anula en P, así tenemos que $v(a) = b$. De lo anterior, notar que $y + v(x)$ no puede tener un cero en P, pues $v(a) - b \neq 0$. Como

$$(y + v(x))(y - v(x)) = y^2 - v(x)^2 = f(x) - v(x)^2.$$

Así, el orden de los ceros de P de $y - v(x)$ es el mismo que el de $f(x) - v(x)^2$. Por tanto, si $b \neq 0$ y $v(a) = 0$, entonces al calcular $div(y - v(x))$ el coeficiente de P es el mismo que la multiplicidad de $x - a$ en la factorización de $f(x) - v(x)^2$. Por otro lado, supongamos que tenemos un punto en $\mathcal{C}$ de la forma $(a, 0)$ que es raíz de $y - v(x)$. Esto es $f(a) = 0$ y $v(a) = 0$, notar que

$$x - a = y^2 \frac{x - a}{f(x)}.$$

Como $f(x)$ no tiene raíces múltiples, entonces $(x - a)/f(x)$ no tiene ceros ni polos en $(a, 0)$, con lo cual $x - a$ tiene un cero doble en $(a, 0)$. La función $v(x)$ tiene al menos un cero doble en $(a, 0)$, pero $y - v(x)$ tiene un cero simple en $(a, 0)$.

Supongamos que $(x - a)^2$ es factor del polinomio $f(x) - v(x)^2$, como $(x - a)^2$ es un

factor de $v(x)^2$, entonces también lo seria de $f(x)$, lo que no puede ser por que $f(x)$ no tiene raíces múltiples. Concluimos entonces que el polinomio $f(x) - v(x)^2$ tiene a $x-a$ como factor de multiplicidad 1, o bien dicho en términos de divisores; si $v(a) = 0$ y $(a,0)$ esta en la curva $\mathcal{C}$ entonces $[(a,0)]$ aparece con coeficiente 1 en $div(y - v(x))$ y que el polinomio $f(x) - v(x)^2$ tiene a $x-a$ como raíz simple.

Lo anterior nos dice que cada cero de $y - v(x)$ es un cero de $f(x) - v(x)^2$. Ahora bien veamos que $f(x) - v(x^2)$ no tiene otros ceros. En efecto, escribimos

$$div(y - V(x)) = \sum_j d_j([(a_j, b_j)] - [\infty]).$$

Entonces

$$div(y + v(x)) = \sum_j d_j([(a_j, -b_j)] - [\infty]) = \sum_j d_j([i(a_j, b_j)] - [\infty]).$$

Además, por 1.7.1

$$div(f(x) - v(x)^2) = div(y - v(x)) + div(y + v(x)) = \sum_j d_j([(a_j, b_j)] + [(a_j, -b_j)] - 2[\infty]).$$

Se sigue de 1.8.4 que todas las raíces de $f(x) - v(x)^2$ aparecen en $div(y - v(x))$. ■

Cuando no haya lugar a confusión, escribiremos P en vez de $1 \cdot P$.

Definición 1.8.4 *Sea $D = \sum_P n_P \cdot P$ un divisor. Definimos la involución en D de forma natural como $i(D) := \sum_P n_p \cdot i(P)$.*

Proposición 1.8.2 *Sea $D \in Div_K^0(\mathcal{C})$. El divisor $D + i(D)$ es principal.*

Demostración. Sea $D = \sum_{P \neq \infty} n_P(1 \cdot P - 1 \cdot \infty)$, entonces

$$D + i(D) = \sum_{P, i(P) \neq \infty} n_P(P + i(P) - 2\infty) = div\left(\prod_P (x - x_p)^{n_P}\right).$$

Esta ultima igualdad dada por 1.8.4. ■

1.9. Jacobiano

Consideremos el cuerpo finito F_q, donde q es una potencia de un número primo p. Recordemos que la ecuación de la curva hiperelíptica de género g definida sobre F_q

está dada por $\mathcal{C} : y^2 = f(x)$ donde $f(x) \in \mathbb{F}_q[x]$ con $deg(f) = 2g+2$.

Denotaremos el jacobiano de la curva como $\mathcal{J}_K(\mathcal{C})$ o simplemente $\mathcal{J}(\mathcal{C})$ si no hay ambigüedad en el cuerpo que se este utilizando. Se verifica que $\mathcal{J}(\mathcal{C})$ es un grupo abeliano finito que se construye a partir de los puntos racionales en la curva. Los puntos en el jacobiano corresponden a ciertas clases de divisores en la curva, y la operación de grupo se define mediante la suma de estos divisores.

El jacobiano de una curva hiperelíptica sobre un cuerpo finito tiene propiedades interesantes y es relevante en la teoría de números. Por ejemplo, se utiliza en la construcción de protocolos criptográficos y en la resolución de ecuaciones diofánticas. Además, el número de puntos racionales en el jacobiano de una curva hiperelíptica sobre un cuerpo finito también está relacionado con el teorema de Hasse-Weil, que proporciona una estimación del número de puntos racionales en la curva hiperelíptica.

Variedades abelianas. Una variedad abeliana es una variedad algebraica que tiene una estructura de grupo abeliano. Esto significa que la variedad es un espacio algebraico que admite una operación de grupo conmutativo, lo que incluye propiedades como la inversión y la suma de puntos.

La relación entre el jacobiano de una curva hiperelíptica sobre un cuerpo finito y las variedades abelianas se establece de la siguiente manera:

A través de la correspondencia de Torelli, que es un resultado profundo en la teoría de curvas algebraicas, se puede demostrar que el jacobiano de una curva hiperelíptica sobre un cuerpo finito es isomorfo (en términos de variedades abelianas) a un subgrupo de un jacobiano de una curva suave más general. En otras palabras, el jacobiano de una curva hiperelíptica se puede ver como una subvariedad abeliana de un jacobiano más grande.

Esta relación entre el jacobiano de una curva hiperelíptica y las variedades abelianas tiene aplicaciones importantes en la teoría de números, particularmente en la construcción de sistemas criptográficos basados en curvas elípticas sobre cuerpos finitos.

La discusión anterior nos permite hacer referencia tanto al grupo de Picard, como al jacobiano como el objeto algebraico donde están bien definidas las operaciones de grupo de manera indistinta, cabe aclarar que en algunos textos se omite tal discusión y se toma el Picard y el jacobiano de manera indistinta.

Se realizan algunos comentarios adicionales sobre este tema en el Capítulo 2.

1.10. Representación de Mumford

Dado que ya tenemos bien caracterizado nuestro objeto algebraico, nos interesa tener una buena representación de cada clase de equivalencia, es decir, obtener otros objetos mas simples y conocidos los cuales nos etiqueten y nos guarden la información de los representantes de cada clase. Para este propósito, introduciremos las representaciones de Mumford, que se basan en la caracterización de un divisor mediante una pareja de polinomios y que con ayuda de algoritmos podemos realizar ciertas operaciones entre divisores de forma mas explicita.

Definición 1.10.1 *Sean $D_1 = \sum_P m_p \cdot P$ y $D_2 = \sum_P n_p \cdot P$ dos divisores en una curva $\mathcal{C}$ de género 2. Definimos el máximo común divisor entre D_1 y D_2 como*

$$mcd(D_1, D_2) := \sum_P min\{m_P, n_P\} \cdot P - \sum_P min\{m_P, n_P\} \cdot \infty.$$

Proposición 1.10.1 *Sea $\mathcal{C}$ una curva de género 2 y consideremos $D = \sum_j c_j(P_j - \infty)$ un divisor semi reducido, con $P_j = (a_j, b_j) \in \mathcal{C}$. Sean $u(x) = \prod_j (x - a_j)^{c_j}$ y $v(x) \in K[x]$ tal que para todo j, $v(a_j) = b_j$. Entonces*

$$D := mcd\left(div(u(x)), div(y - v(x))\right),$$

si y solo si, $f(x) - v(x)^2$ es un múltiplo de $u(x)$.

Demostración. En la notación de la proposición 1.8.1. Sea $\alpha_j \geq c_j$ para todo j, lo que es equivalente a que $f(x) - v(x)^2$ sea un múltiplo de $u(x)$. Además D es el mcd solo si los $\alpha_j \geq c_j$, para todo j.

Por ultimo notemos que para los puntos de la forma (a_j, b_j) con $b_j = 0$ en D, al D ser semi reducido, $c_j = 1$. Y dado que $div(x - a_j)$ tiene dos copias de $[P_j]$, pero $div(y - v(x))$ solo tiene una, entonces el mcd solo puede tener una, lo anterior por 1.8.1. ■

Teorema 1.10.1 *Existe una correspondencia uno a uno entre los divisores semi reducidos $D = \sum_j c_j \cdot (P_j - \infty)$ y las parejas de polinomios $(u(x), v(x))$ que satisfacen que:*

1. *$u(x)$ es mónico.*
2. *$deg(u(x)) = \sum_j c_j$ y $deg(v(x)) < deg(u)$.*
3. *$v(x)^2 - f(x)$ es un múltiplo de $u(x)$.*

Bajo esta correspondencia tenemos que $D = mcd\left(div(u(x)), div(y - v(x))\right)$.

Demostración. Sean $(u(x), v(x))$, que satisfacen 1,2 y 3 anteriores, tomemos

$$D = mcd(div(u(x)), div(y - v(x))).$$

Si $f(x) - v(x)^2 = \prod_j (x - a_j)^{d_j}$, entonces $div(y - v(x)) = \sum_j d_j((P_j) - (\infty))$, donde $b_j = v(a_j)$, y si $b_j = 0$, entonces $d_j = 1$, así $deg(u(x)) = \sum_j c_j$ y $d_j \geq c_j$. Como $div(y - v(x))$ es semi reducido, entonces D es semi reducido.

Recíprocamente, sea D un divisor semi reducido, y sea $P_j = (a_j, b_j) \in supp(D)$, es decir $D = \sum_j c_j(P_j - \infty)$ Se debe construir una tupla $(u(x), v(x))$, elegimos $u(x)$ de manera natural como $u(x) = \prod_j (x - a_j)_j^c$ y debemos encontrar $v(x)$ tal que $v(a_j) = b_j$ para todo j y $v^2 - f(x)$ sea un múltiplo de $u(x)$.

Supongamos que para cada j tenemos un polinomio $v_j(x)$ tal que $v_j(a_j) = b_j$ y

$$v_j(x)^2 \equiv f(x) mod (x - a_j)^{c_j}.$$

Consideremos el sistema de congruencias

$$\begin{aligned} t &\equiv v_1(x) \mod (x - a_1)^{c_1}, \\ t &\equiv v_2(x) \mod (x - a_2)^{c_2}, \\ &\vdots \\ t &\equiv v_l(x) \mod (x - a_l)^{c_l}. \end{aligned}$$

Como los $(x - a_i)$ son coprimos dos a dos, entonces del teorema chino del resto existe $v(x) \in K[x]$ tal que $v(x) \equiv v_j(x) mod (x - a_j^{c_j})$, para todo j.

Basta entonces solucionar congruencias de la forma $w^2(x) \equiv f(x) mod (x - a)^c$ donde $w(a) = b$ y $b^2 = f(a)$.

Para esto se usa el método de Newton para encontrar soluciones usando aproximación numérica, ver [7, Thm. 13.4]. ■

Definición 1.10.2 *Sea D un divisor semi reducido. Los polinomios $(u(x), v(x))$ del teorema anterior son llamados la representación de Mumford de D.*

Definición 1.10.3 *Sea $\mathcal{C}$ una curva hiperelíptica de género g definida sobre un cuerpo K, y sea $D = \sum_j c_j \cdot (P_j - \infty)$ un divisor semi reducido. Decimos que D es un* divisor

reducido *si* $\sum_j c_j \leq g$, *es decir, si su grado es menor o igual que el género de la curva. En particular, cuando* $g = 2$, *un divisor semi reducido es reducido si su grado es menor o igual que* 2.

Definición 1.10.4 *Sea D un divisor, definimos*

$$\mathscr{L}(D) := \{f \in K(\mathcal{C}) : div(f) + D \geq 0\} \cap \{0\}.$$

$\mathscr{L}(D)$ *es un espacio vectorial sobre* $\overline{K}$ *y definimos* $\ell(D) := dim_{\overline{K}} \mathscr{L}(D)$.

Ejemplo 1.10.1 *Si* $D = 3[P_1] - 2[Q_2]$. *Una función* $f \in \mathscr{L}(D)$ *puede tener a lo mas un triple polo en* P_1 *y como mínimo un doble cero en* P_2, *también notar que* f *no puede tener otros ningún otro polo, pero puede tener ceros diferentes a* P_2.

Proposición 1.10.2 *Sea* $\mathcal{C}$ *una curva algebraica definida sobre K, y sean* D, D_1 *y* D_2 *divisores en* $\mathcal{C}$, *entonces:*

1. *Si* $deg(D) < 0$, *entonces* $\mathscr{L}(D) = \{0\}$.
2. *Si* $D_1 \sim D_2$ *entonces* $\mathscr{L}(D_1) \cong \mathscr{L}(D_2)$.
3. $\mathscr{L}(\boldsymbol{0}) = \overline{K}$.
4. $\ell(D) < \infty$.
5. *Si* $deg(D) = 0$ *entonces* $\ell(D) = 0$ *o* 1.

Demostración. Ver [7, Prop. 11.14]. ■

Teorema 1.10.2 *(Riemann-Roch) Dada una curva algebraica* $\mathcal{C}$, *existe un entero g, llamado el género de* $\mathcal{C}$ *y un divisor* $\mathscr{K}$, *llamado divisor canónico, tal que*

$$\ell(D) - \ell(\mathscr{K} - D) = deg(D) - g + 1.$$

para todo divisor D.

Demostración. Ver [19, Ch. 4, Thm. 1.3] ■

Corolario 1.10.1 $deg(\mathscr{K}) = 2g - 2$.

Demostración. Consideremos los divisores $D = 0$ y $D = \mathcal{K}$, por el teorema de Riemann-Roch, y por 1.10.2 usando (3), tenemos que $\ell(\mathcal{K}) = g$ y $\ell(\mathcal{K}) = deg(\mathcal{K}) - g + 2$, por tanto, $deg(\mathcal{K}) = 2g - 2$. ■

Proposición 1.10.3 *Sea D un divisor de grado 0 sobre una curva algebraica $\mathcal{C}$. Existe un único divisor reducido D_1, tal que $D - D_1$ es un divisor principal.*

Demostración. Consideremos el teorema de Riemann-Roch para el divisor $D + g[\infty]$,

$$\ell(D + g[\infty]) = \ell(\mathcal{K} - D - g[\infty]) + 1 \geq 1,$$

Pues $\ell(\mathcal{K} - D - g[\infty]) \geq 0$. Existe entonces una función no nula F de manera que

$$div(F) + D + g[\infty] \geq 0.$$

Sea $D_1 = div(F) + D$, como D_1, D están en la misma clase de divisores entonces $D_1 + g[\infty] \geq 0$ y $deg(D_1) = 0$. De lo anterior deducimos que si $D_1 = \sum_j c_j([P_j])$, entonces los únicos puntos en D_1 con coeficientes negativos son $[\infty]$ y que como mucho hay otros g puntos el la suma. Por otro lado, por el lema 1.8.1 podemos asumir D_1 reducido.

Veamos que D_1 es único. Supongamos que $D - D_1 = div(F)$ y que $D - D_2 = div(G)$ con $D - 1$ y D_2 reducidos. Entonces

$$D_1 + i(D_2) = D + i(D) - div(F) - i(div(G)).$$

Dicho divisor es principal, pues $D + i(D)$ lo es 1.8.2, y la involución de un divisor principal es un divisor principal.

Entonces existe H tal que $D_1 + i(D_2) = div(H)$, por tanto

$$div(H) + 2g[\infty] = (D_1 + g[\infty]) + i(D_2 + g[\infty]) \geq 0.$$

Así, por definición de $\mathcal{L}(2g[\infty])$ 1.10.4, $H \in \mathcal{L}(2g[\infty])$.

Por Riemann-Roch tenemos que

$$\ell(2g[\infty]) - \ell(\mathcal{K} - 2g[\infty]) = 2g - g + 1 = g + 1.$$

Por 1.10.1, $deg(\mathcal{K} - 2g[\infty]) = -2 < 0$, por tanto $\ell(\mathcal{K} - 2g[\infty]) = 0$, esto ultimo por 1.10.2.

Concluimos entonces que $\ell(2g[\infty]) = g+1$. Notemos que $x^j \in \mathscr{L}(2j[\infty])$, siendo así el conjunto de funciones $\{1, x, x^2, \ldots, x^g\}$ forman un conjunto linealmente independiente en el espacio $\mathscr{L}(2g[\infty])$.

En resumen, H es un polinomio de grado a lo mas g, dicho de otro modo, para algunos puntos P_j y enteros c_j, se sigue que

$$D_1 + i(D_2) = \sum_j c_j([P_j] + [i(P_j)] - 2\infty).$$

Finalmente, como D_1 y $i(D_2)$ son reducidos,sin perdida de generalidad, supongamos que la ocurrencia de $[P_j]$ ocurre en D_1 y la de $[i(P_j)]$ ocurre en $i(D_2)$ o mas precisamente

$$D_1 = \sum_j ([P_j] - [\infty]) \quad y \quad i(D_2) = \sum_j ([i(P_j)] - \infty).$$

Con lo cual $D_1 = D_2$. ■

El siguiente teorema este teorema permite caracterizar de forma única clases de divisores en el jacobiano 1.10.1.

Teorema 1.10.3 *Existe una correspondencia uno a uno entre las clases de divisores de grado* 0 *y las parejas de polinomios* $(u(x), v(x)) \in K[x]^2$ *tales que:*

1. $u(x)$ *es mónico.*
2. $deg(v(x)) < deg(u(x)) \leq 2$.
3. $v(x)^2 - f(x)$ *es un múltiplo de* $u(x)$.

Observación 1.10.1 *Así, existe una cierta representación polinomial de la clase de un divisor de tal forma que*

$$[D] = [x^2 + ax + b, cx + d], \ [D] \in \mathcal{J}(\mathcal{C}).$$

Observación 1.10.2 *En algunos textos se utiliza la notación,* $\mathcal{J}(u, v)$*, para indicar que estamos en* $\mathcal{J}(\mathcal{C})$.

Queremos ahora un algoritmo para obtener la representación de Mumford de una forma explicita.

Teorema 1.10.4 *Sea* $(u(x), v(x))$ *la representación de Mumford de un divisor semi reducido* D *de grado* 0. *El siguiente algoritmo se utiliza para encontrar la representación del divisor reducido en* $[D] \in Prin_K(\mathcal{C})$.

Algoritmo de reducción

1. *Sea* $\tilde{u}(x) := \frac{f(x)-v(x)^2}{u(x)}$.
2. *Sea* $\tilde{v}(x) := -v(x) \ (mod \tilde{u}(x))$, *con* $deg(\tilde{v}(x)) < deg(\tilde{u}(x))$.
3. *Fijamos* $u(x) = \tilde{u}(x)$ *y* $v(x) = \tilde{v}(x)$.
4. *Hacemos* $u(x)$ *mónico multiplicando por escalar.*
5. *Si* $deg(u(x)) > 2$ *regresamos al paso 1.*
6. *Obtenemos* $(u(x), v(x))$.

Ejemplo 1.10.2 *Sea* $(u(x), v(x))$ *la representación de Mumford del divisor semi-reducido* D. *Si* i *es la involución hiperelíptica,* $(u, -v)$ *es la representación de* $i(D)$.
Demostración. *Sea* $D = \sum_j c_j((P_j) - (\infty))$ *un divisor semi reducido con* $P_j = (a_j, b_j)$ *y representación de Mumford* $(u(x), v(x))$. *Se cumple que:*

1. $u(x)$ *es mónico.*
2. $deg(u) = \sum_j c_j$ *con* $deg(v) < deg(u)$.
3. $v(x)^2 - f(x)$ *es múltiplo de* $u(x)$, *con* $v(a_j) = b_j$.

Basta notar que para el divisor semi-reducido $i(D) = \sum_j c_j(i(P_j) - (\infty))$ *se tiene que* $deg(-v(x)) = deg(v(x)) < deg(u(x))$. *Además* $(-v(x))^2 - f(x) = v(x)^2 - f(x)$ *es un múltiplo de* $u(x)$ *y* $-v(a_j) = -b_j$, *donde* $i(P_j) = (a_j, b_j)$. *Así* $(u(x), -v(x))$ *es la representación de Mumford de* $i(D)$. ■

Ejemplo 1.10.3 *Sea* $\mathcal{C} : y^2 = x^5 - 5x^3 + 4x + 1$, *calculemos* $div(y-1)$, $div(x)$ *y encontremos un representante de Mumford para el divisor* $[(-1,1)] + [(-1,-1)] + [(1,1)] + [(2,1)] + [(0,1)] - 5[\infty]$.

a) *Veamos que* $div(y-1) = [(-1,1)] + [(-2,1)] + [(1,1)] + [(2,1)] + [(0,1)] - 5[\infty]$.

Sea $v(x)$ *un polinomio, de la proposición 1.8.1, si* $f(x) - v(x)^2 = \prod_j (x-a_j)^{d_j}$, *entonces* $div(y - v(x)) = \sum_j d_j((a_j, b_j) - (\infty))$ *donde* $v(a_j) = b_j$. *Para* $v(x) = 1$ *basta notar que de la ecuación que define a la curva se tiene que:*

$$\begin{aligned} y^2 - 1 &= x^5 - 5x^3 + 4x, \\ &= x(x^4 - 5x^2 + 4), \\ &= x(x^2 - 4)(x^2 - 1), \\ &= x(x-2)(x+2)(x-1)(x+1). \end{aligned}$$

Así como todas las multiplicidades de las raíces son 1, $d_j = 1$, *y como* v *es constante* $v(a_j) = 1$, *luego*

$$\begin{aligned} div(y-1) &= \sum_j d_j((a_j, b_j) - (\infty)), \\ &= [(0,1)] + [(2,1)] + [(-2,1)] + [(-1,1)] + [(1,1)] - 5[\infty]. \end{aligned}$$

b) *Afirmamos que* $div(x) = [(0,1)] + [(0,-1)] - 2[\infty]$.

Por definición tenemos que: $div(x) = \sum_{P \in \mathcal{C}} v_P(x) \cdot P$, *o bien basta analizar los ceros o polos de* x, *si* $x = 0$, *entonces* $y^2 = 1$ *o bien* $y = 1$ *ó* $y = -1$, *es decir, los únicos puntos que aparecen en el divisor son* $(0,1)$ *y* $(0,-1)$ *y como son raíces simples, entonces* $div(x) = [(0,1)] + [(0,-1)] - 2[\infty]$.

c) *Calculemos* $(u(x), v(x))$, *representante de Mumford de* $[(-1,1)] + [(-1,-1)] + [(1,1)] + [(2,1)] + [(0,1)] - 5[\infty]$.

Sabemos que dado un punto $P = (x_p, y_p)$ *en la curva tenemos que*

$$div(x - x_p) = [(x_p, y_p)] + [(x_p, -y_p)] - 2[\infty].$$

Notemos que el divisor anterior no es semi-reducido, pues aparece un punto y su involución hiperelíptica, luego debemos buscar un D' *tal que* $D = D' + div(f)$ *con* $f \in K(\mathcal{C})$, *tomando* $div(x+1) = [(-1,1)] + [(-1,-1)] - 2[\infty]$, $D = D' + div(x+1)$, *más aún, dado que* $D' = [(1,1)] + [(2,1)] + [(0,1)] - 3[\infty]$ *es semi reducido, y por inspección en la correspondencia entre divisores y pares de polinomios* $(u(x), v(x))$,

tenemos que $u(x) = (x-1)(x-2)(x-0) = x(x-1)(x-2)$*, por otro lado,* $v(0) = v(2) = v(1) = 1$*, y para que* $deg(v(x)) < deg(u(x)) = 3$*, se debe tener que* $v(x) = 1$*.*

Verificamos que $v(x)^2 - f(x)$ *sea un múltiplo de* $u(x)$

$$\begin{aligned} v(x)^2 - f(x) &= 1 - (x^5 - 5x^3 + 4x + 1), \\ &= -x^5 + 5x^3 - 4x, \\ &= -x(x-2)(x+2)(x-1)(x+1), \\ &= -(x+2)(x+1)u. \end{aligned}$$

Luego tenemos el par $(u(x), v(x)) = (x(x-1)(x-2), 1)$ *y lo reducimos,*

$\tilde{u}(x) = \dfrac{f(x) - v(x)^2}{u(x)} = \dfrac{(x+2)(x+1)u(x)}{u(x)} = (x+2)(x+1)$ *y* $\tilde{v}(x) \equiv -1 mod(\tilde{u}(x))$*,*

obtenemos que $D \sim D'$ *entonces* $[D]$ *esta representada por* $((x+2)(x+1), -1)$*.*

Observación 1.10.3 *El algoritmo de reducción descrito anteriormente se presenta de forma iterativa, aplicando sucesivos pasos hasta obtener una representación de Mumford reducida. Sin embargo, en el artículo original de Cantor [4], se propone una versión más general del algoritmo que permite realizar la reducción en un solo paso. Esta versión explota el hecho de que, dado un divisor semi-reducido representado por* $(a(x), b(x))$*, se puede construir directamente un nuevo par* $(a'(x), b'(x))$ *que representa el mismo divisor en su forma reducida mediante la fórmula:*

$$a'(x) = \frac{f(x) - b(x)^2}{a(x)}, \quad b'(x) \equiv -b(x) \mod a'(x), \quad \deg b'(x) < \deg a'(x).$$

Esta forma es computacionalmente más eficiente y evita la necesidad de pasos iterativos.

1.11. Algoritmo de Cantor

Dado que tenemos una operación de grupo en el conjunto de clases de divisores, queremos poder asociar a la suma de dos divisores reducidos, su representación de Mumford a partir de las representaciones de Mumford de cada sumando. Una herramienta que nos permitirá hacer esto de forma efectiva será el algoritmo de Cantor y

veamos a su vez como se relaciona con la geometría de la curva; para ello retomemos las ideas sobre como podríamos sumar "puntos"de la curva 1.7.

La representación de Mumford de un divisor en una curva algebraica se basa en el uso de polinomios que permiten describir el divisor de manera efectiva.

Para calcular el representante de Mumford, utilizamos la interpolación de Lagrange. Dado un conjunto de g puntos $P_i = (x_i, y_i)$, el polinomio de interpolación $v(x)$ se puede expresar como:

$$v(x) = \sum_{i=g}^{t} \Big(y_i \prod_{\substack{j=1 \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \Big).$$

Este polinomio tiene la propiedad de que $v(x_i) = y_i$, lo cual garantiza que captura la información del divisor D adecuadamente. En la práctica, el cálculo de $v(x)$ mediante la fórmula de Lagrange permite obtener un representante que describe el comportamiento del divisor a lo largo de la curva.

Teorema 1.11.1 *Sean $\mathcal{C} : y^2 = f(x)$ una curva de género 2, $D_1, D_2 \in Div_K^0(\mathcal{C})$ divisores reducidos con $(u_1(x), v_1(x)), (u_2(x), v_2(x))$ las respectivas representaciones de Mumford. El siguiente procedimiento permite obtener la representación de Mumford de la clase $[D_1 + D_2]$.*

1. *Consideramos $d = mcd\,(u_1, u_2, v_1 + v_2)$. Determinar $H_1, h_2, h_3 \in K[x]$, tales que*

$$d = u_1, h_1 + u_2 h_2 + (v_1 + v_2) h_3.$$

2. *Definimos $v_0 = \dfrac{u_1 v_2 h_1 + u_2 v_1 h_2 + (v_1 + v_2) h_3}{d}$.*

3. *Calculamos $u = \dfrac{u_1 u_2}{d^2}$ y $v \equiv v_0 (mod\ u)$, con $deg(v) < deg(u)$.*

4. *Reducimos $\tilde{u} := \dfrac{f - v^2}{u}$ y $\tilde{v} \equiv -v (mod\ \tilde{u})$ con $deg(\tilde{v}) < deg(\tilde{u})$.*

5. *Fijamos $u = \tilde{u}$ y $v = \tilde{v}$.*

6. *Hacemos u mónico.*

7. *Si $deg(u) \geq 2$, regresar al paso 4. En otro caso, continuamos.*

8. *Obtenemos $(u(x), v(x))$.*

Ejemplo 1.11.1 *Sean* $(u(x), v(x))$ *la representación de un divisor semi-reducido.*

a) $(1,0)$ *es el neutro de la operación, es decir,* $(u(x), v(x)) + (1,0) = (u(x), v(x))$.

Del algoritmo de Cantor, $u_1 = u, v_1 = v, u_2 = 1, v_2 = 0$, *luego*

1. $d = mcd(u_1, 1, v_1) = 1$, *luego* $u_1(x)\cdot 0 + 1\cdot 1 + 0\cdot v_1(x) = 1$, $h_1 = 0, h_2 = 1, h_3 = 0$.
2. $v_0 = \dfrac{u_1(x)\cdot 0\cdot 0 + 1\cdot v_1(x)\cdot 1 + (v_1(x)\cdot 0 + f(x))\cdot 0}{1} = v$.
3. $u(x) = \frac{u_1(x)\cdot 1}{1} = u_1(x)$ *y* $v(x) = v_0$.

Como v *ya esta reducido módulo* u, *y* (u, v) *ya es una representación, entonces* (u, v) *es la representación deseada.*

b) *El inverso de un representante de Mumford* $(u(x), v(x))$, *es de la forma* $(u(x), -v(x))$, *es decir,* $(u(x), v(x)) + (u(x), -v(x)) = (1,0)$.

Del algoritmo de Cantor tomamos $u_1 = u, v_1 = v, u_2 = u$ *y* $v_2 = -v$, *luego*

1. $d = mcd(u, u, 0) = mcd(u, 0) = u$, *luego* $u = u(2^{-1}) + u(2^{-1}) + 0\cdot 0$.
2. $v_0 = \dfrac{u\cdot(-v)2^{-1} + u\cdot(v)2^{-1} + (0+f)\cdot 0}{u} = 0$.
3. $u = \frac{u\cdot u}{u^2} = 1$, $v = v_0$.

Con lo cual obtenemos la representación $(1,0)$ *como se quería.*

1.12. Aritmética Rápida

Notemos que, aunque la adición en representaciones de Mumford se vuelve un procedimiento algorítmico que ocurre en $K[x]$, se necesitan calcular ciertos polinomios que pueden hacer el el proceso mas lento. Aquí algunos algoritmos para acelerar dicho proceso.

Adición en el caso mas común

En este caso las dos clases de divisores a sumar consisten en cuatro puntos, dos cada uno, diferentes a su involución. Los resultados en el algoritmo de composición

1.11.1 son $u = u_1 u_2$ y un polinomio v de grado ≤ 3 que satisfacen $u|v^2 + vh - f$. Empezamos con $u_i|v_i^2 + v_i h - f$ y como en el teorema, podemos obtener v usando el teorema Chino de los restos:

$$v \equiv v_1 \ mod \ u_1,$$
$$v \equiv v_2 \ mod \ u_2.$$

Luego se calcula el primer polinomio u' haciendo $\dfrac{f - vh - v^2}{u_1 u_2}$ mónico y tomando $v' = (-h - v \ mod \ u')$.

Ahora bien, para optimizar no desarrollamos completamente lo anterior. Listamos las siguientes sub-expresiones necesarias y mostraremos que nos dan el mismo resultado, tomamos:

$$\begin{aligned} k &= (f - v_2 h - v_2^2)/u_2, \\ s &= (v_1 - v_2)/u_2 \ mod \ u_1, \\ l &= s u_2, \\ u &= (k - s(l + h + 2v_2))/u_1, \\ u' &= u \ \textit{mónico}, \\ v' &\equiv -h - (l + v_2) \ mod \ u'. \end{aligned}$$

Notemos que $v = s u_2 + v_2 = l + v_2$ cumplen las congruencias anteriores, es claro para la segunda congruencia. Para la primera notemos que

$$v \equiv s u_2 + v_2 \equiv ((v_1 - v_2)/u_2) u_2 + v_2 \equiv v_1 \ mod \ u_1.$$

La división para crear a k es exacta de la definición de u_2 *y* v_2, para u, notemos que

$$u_1 u_2 u = u_2(k - s(l + h + 2v_2)) = f - v_2 h - v_2^2 - l(l + h) - 2l v_2 = \cdots = f - vh - v^2.$$

Por otro lado notemos que como $deg(f) = 5$, $deg(h) \leq 2$, $deg(v_2) = 1$, u_2 es mónico de grado 2, entonces $k = x^3 + (f_4 - u_{21})x^2 + cx + c'$ donde c y c' son constantes. Es decir esto muestra que se necesitan menos operaciones involucradas si se mira el algoritmo de esta forma, luego en u se realiza una división de k de grado 3, con un u_1 de grado 1 por tanto solo se necesita una parte de k para efectos de cómputo, ver 4.3.1. [29, 4.3.2

Addition in Most Common Case].

Duplicación

Además de sumar clases de divisores utilizando la representación de Mumdford, también nos interesa la duplicación, o encontrar n veces dicha clase, dicho proceso puede hacerse tanto en el jacobiano, como dentro de otros conjuntos donde si bien no hay estructura de grupo, permiten encontrar de forma rápida los múltiplos enteros de una representación.

Sea $u(x) = x^2 + u_1 x + u_0,\ v(x) = v_1 x + v_0$ la representación de Mumford de un divisor de peso 2, queremos $2[u, v] = [u_{new}, v_{new}]$, donde del algoritmo de Cantor, se tiene que

$$\begin{aligned} u_{new} &= u^2, \\ v_{new} &= v \ mod\ u, \\ u_{new} &| v_{new}^2 + v_{new} h - f. \end{aligned}$$

Asi, esta clase es reducida para obtener $[u', v']$. Usamos las siguientes expresiones:

$$\begin{aligned} k &= (f - hv - v^2)/u, \\ s &\equiv k/(h + 2v)\ mod\ u, \\ l &= su, \\ \widetilde{u} &= s^2 - ((k + 2v)s - k)/u, \\ u' &= \widetilde{u}\ (hecho\ mónico), \\ v' &\equiv -h - (l + v)\ mod\ u'. \end{aligned}$$

Notemos que no calculamos el divisor semi-reducido explícitamente, aquí $v_{new} = l + v = su + v$. Así, es claro que se da la congruencia, para ver la divisibilidad, consideramos que

$$v_{new}^2 + v_{new} h - f = l^2 + 2lv + v^2 + hl + hv - f = s^2 u^2 + u(s(h + 2v) - k),$$

$$(h + 2v)s - k \equiv (h + 2v)k/(h + 2v - k) \equiv 0\ mod\ u.$$

Finalmente,

$$\frac{v_{new}^2 + v_{new} h - f}{u_{new}} = \frac{s^2 u^2 + (h2v)su - ku}{u^2}.$$

Para una discusión más detallada, véase [29, Doubling 4.3.3].

1.13. Subgrupos de Torsión

Dado un grupo G, sus subgrupos de torsión están compuesto por aquellos elementos g tales que $g^n = e$, para algún n natural y donde e es el elemento neutro del grupo. Estos subgrupos son relevantes no solo en teoría de grupos, sino también en aplicaciones prácticas, como la criptografía. En particular, algoritmos de intercambio de claves basados en isogenias, donde el orden de los elementos juega un papel crucial en la seguridad del protocolo.

Definición 1.13.1 *Sea $\mathcal{C}$ una curva de género 2 sobre $\mathbb{F}_q$, con $q = p^r$ y p primo. Para $[D] \in \mathcal{J}_{\mathbb{F}_q}(\mathcal{C})$, definimos para $n \in \mathbb{N}$*

$$[n][D] := [D] + \cdots + [D],$$

donde D es un divisor reducido. Definimos el n-ésimo subgrupo de torsión de $\mathcal{J}_{\mathbb{F}_q}(C)$ como

$$\mathcal{J}_{\overline{\mathbb{F}}_q}(\mathcal{C})[n] := \left\{ [D] \in \mathcal{J}_{\overline{\mathbb{F}}_q}(\mathcal{C}) \colon [n][D] = [0] \right\}.$$

Dado que $\mathcal{J}_{\overline{\mathbb{F}}_q}(\mathcal{C})$ es un grupo abeliano finitamente generado, una pregunta natural es que tan grande puede ser su rango.

Teorema 1.13.1 *Sea $\mathcal{C}$ una curva de género g sobre $\mathbb{F}_q$, con $q = p^r$, y p primo. Si $mcd(p, n) = 1$, entonces*

$$\mathcal{J}(\mathcal{C})[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Demostración. Ver [30, Thm 10.3] y [30, Thm 10.5] ■

Teorema 1.13.2 *Sea $\mathcal{C}$ una curva de género 2 sobre $\mathbb{F}_q$, $q = p^r$, p primo. Existen polinomios $L(t) \in \mathbb{Z}[t]$ de $deg(L) = 4$ con las siguientes propiedades:*

1. $L(1) = |Pic_{\mathbb{F}_q}(\mathcal{C})|$.
2. $L(t) = \prod_{i=1}^{4}(1 - \alpha_i t)$, *con* $\alpha_i \in \mathbb{C}$, $\alpha_{2+i} = \overline{\alpha_i}$, $|\alpha_i| = \sqrt{q}$, $i \in \{1, 2\}$.
3. $L(t) = q^2 t^4 L\left(\frac{1}{qt}\right)$.
4. *Dado $n \in \mathbb{N}$, definimos $L_n(t) = \prod_{i=1}^{4}(1 - \alpha_i^n t)$, entonces $L_n(1) = |Pic_{\mathbb{F}_q}(\mathcal{C})|$.*

Demostración. Ver [40, Thm 3.9], [15, Thm 10.7.1]. ■

Teorema 1.13.3 *Sea α_i con las condiciones del teorema anterior, $n \in \mathbb{N}$, entonces*

$$\left|\mathcal{C}(\mathbb{F}_{q^n})\right| = q^n + 1 - \sum_{i=1}^{4} \alpha_i^n.$$

Sea $\mathcal{J}$ un jacobiano de una curva hiperelíptica de género 2, y $D = \sum_i c_i(P_i - \infty)$, un divisor reducido, es decir $\sum_i c_i \leq 2$. Queremos calcular $[n][D]$. Para eso, recordemos primero el caso de género 1, es decir, en curvas elípticas.

Polinomios de división Consideremos la curva elíptica dada por

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

con $3A^3 + 27B^2 \neq 0$, siendo la condición de no singularidad, ver [23, Teorema 3.2] y [23, Corolario 3.4].

Definición 1.13.2 *Definimos los polinomios de división $\psi_M \in \mathbb{Z}[x, y, A, B]$, dados por la relación de recurrencia:*

- $\psi_0 = 0, \psi_1 = 1, \psi_2 = 2y, \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$.
- $\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5Ax^2 - 4ABX - 8B^2 - A^3)$.
- $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$, *para* $m \geq 2$.
- $\psi_{2m} = (2y)^{-1}\psi_m\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right)$, *para* $m \geq 3$.

Lema 1.13.1 *$\psi_n \in \mathbb{Z}[x, y^2, A, B]$ si n es impar y $\psi_n \in 2y\mathbb{Z}[x, y^2, A, B]$ si n es par.*

Definición 1.13.3 *Definimos los polinomios*

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \quad \omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

Lema 1.13.2 *Para las expresiones anteriores se cumple que:*

- $\phi_m \in \mathbb{Z}[x, y^2, A, B]$ *para todo* $m \in \mathbb{N}$.
- *Si m es impar, entonces* $\omega_m \in y\mathbb{Z}[x, y^2, A, B]$.
- *Si m es par, entonces* $\omega_m \in \mathbb{Z}[x, y^2, A, B]$

Ahora bien, dada la ecuación de la curva $y^2 = x^3 + Ax + B$, consideramos los anteriores polinomios en $\mathbb{Z}[x, A, B]$, además fijando A y B, podemos considerar los polinomios anteriores en una sola variable, así tenemos el siguiente lema.

Lema 1.13.3 *Sean A y B fijos, $y^2 = x^3 + Ax + B$, la ecuación de una curva elíptica, entonces*

- $\phi_n(x) = x^{n^2}$ + (terminos de menor grado).
- $\psi_n^2(x) = n^2 x^{n^2-1}$ + (terminos de menor grado).

Finalmente de lo anterior podemos caracterizar los puntos de la curva elíptica $[n]P$ como sigue.

Teorema 1.13.4 *Sea $E : y^2 = x^3 + Ax + B$ una curva elíptica sobre un cuerpo finito, $P = (x, y)$ un punto de la curva y $n \in \mathbb{N}$, entonces:*

$$[n]P = \left(\frac{\phi_n(x)}{\psi_{n^2}(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right).$$

Además, si consideremos el endomorfismo de grupos

$$\begin{array}{rccc} [n]: & E & \longrightarrow & E \\ & P & \longmapsto & [n]P, \end{array}$$

tenemos el siguiente resultado

Corolario 1.13.1 *El subgrupo de n-torsión de una curva elíptica $E : y^2 = x^3 + Ax + B$, $ker[n] = \{P \in E : [n]P = \infty\}$, es tal que $|ker[n]| = n^2$.*

Por otro lado, existen polinomios que tienen la misma función de los polinomios de división.

Polinomios de división de Cantor

Definición 1.13.4 *Sea $[D]$ un divisor con representación de Mumford $(u(x), v(x))$. El peso de D es el grado de $u(x)$.*

Definición 1.13.5 ***Polinomios de división de cantor*** ℓ*,[10, Def. 5.1].*

Sea $\mathcal{C} : y^2 = f(x)$ *curva hiperelíptica de género* g *sobre el cuerpo finito* K*, con* $\ell > g$ *un entero coprimo a la característica de* K*.*

Sea $P \in \mathcal{C}(K)$*. Para un punto genérico* $Q = (x, y) \in \mathcal{C}$*, la representación de Mumford del elemento* $\ell[Q - P]$ *en el jacobiano de* $\mathcal{C}$ *puede escribirse como sigue*

$$\ell[Q-P] = \left(X^g + \sum_{i=1}^{g-1} \frac{d_i(x)}{d_g(x)} X^i, y \sum_{i=1}^{g-1} \frac{e_i(x)}{e_g(x)} X^i \right),$$

donde los numeradores $d_0, \ldots, d_{g-1}, e_0, \ldots, e_{g-1} \in K[x]$ *y los denominadores* $d_g, e_g K[x]$ *son mónicos. Con lo cual* $\left(\frac{d_0}{d_g}, \cdots, \frac{d_{g-1}}{d_g}, \frac{e_0}{e_g}, \cdots, \frac{e_{g-1}}{e_g} \right)$ *es la representación racional de la multiplicación por* ℓ*.*

Observación 1.13.1 *Para nuestro caso:*

Los polinomios de división de Cantor son polinomios en $\mathbb{F}_q$ *denotados por* $d_0, d_1, d_2, e_0, e_1, e_2$ *tales que para todo divisor de peso 1,* $P = (x - p, y_p)$*,* $[D] = [P - \infty]$*, la representación de Mumford esta dada por:*

$$[\ell][P] = \left(x^2 + \frac{d_1(x_p)}{d_2(x_p)} x + \frac{d_0(x_p)}{d_2(x_p)}, y_p \left(\frac{e_0(x_p)}{e_2(x_p)} x + \frac{e_0(x_p)}{e_2(x_p)} \right) \right).$$

Donde los grados los los polinomios son $2\ell^2 - 1, 2\ell^2 - 2, 2\ell^2 - 3, 3\ell^2 - 2, 3\ell^2$ y $3\ell^2 - 2$ *respectivamente.*

Discutamos la 2 y 3- torsión para darnos un panorama de dichos cálculos.

1.14. 2-Torsión del Jacobiano

Sea $\mathcal{C}$ una curva de género 2 y $\mathcal{J}(\mathcal{C})$ su jacobiano con cuerpo base $\mathbb{F}_q$. Por definición,

$$\mathcal{J}(\mathcal{C})[2] = \left\{ [D] \in \mathcal{J}_{\overline{\mathbb{F}}_q}(\mathcal{C}) \colon [2][D] = [0] \right\},$$

además, por el teorema 1.13.1 sabemos que

$$\mathcal{J}(\mathcal{C})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

Definición 1.14.1 *Los puntos de Weierstrass de la curva* $\mathcal{C} : y^2 = f(x)$ $deg(f) = 5$ *son los puntos invariantes por la involución hiperelíptica,* $i(x, y) = (x, -y)$*, es decirlos puntos*

$(\alpha_i, 0) \in \mathcal{C}(\overline{\mathbb{F}}_q)$, *donde los* α_i *son las raíces de* f, *luego hay* 6 *puntos contando el* ∞.

Teorema 1.14.1 *Cada elemento no nulo de* $\mathcal{J}(\mathcal{C})[2]$ *esta únicamente determinados por un par de puntos de Weierstrass distintos en* $\mathcal{C}$.

Demostración. Sean $\{(\alpha_i, 0)\}_i$ los puntos de Weierstrass de la curva $\mathcal{C}$ y sean $[P_{ij}] = [(\alpha_i, 0) - (\alpha_j, 0)]$. Notemos que $[P_{ij}]$ no es el divisor de una función, es decir, $[P] \neq [0]$ en $\mathcal{J}(\mathcal{C})$, notemos además que de $2[P_{ij}] = 2[(\alpha_i, 0)] - 2[(\alpha_j, 0)]$, de la observación 1.8.4

$$div\left(\frac{x-\alpha_i}{x-\alpha_j}\right) = div(x-\alpha_i) - div(x-\alpha_j) = 2[(\alpha_i, 0)] - 2[(\alpha_j, 0)] = 2[P_{ij}],$$

así $2[P_{ij}] = [0]$ en $\mathcal{J}(\mathcal{C})$, por tanto, $[P_{ij}] \in \mathcal{J}(\mathcal{C})[2]$, luego, $[P_{ij}] = -[P_{ij}] = [P_{ji}]$ por lo tanto $[P_{ij}]$ queda totalmente determinado por $\{i, j\}$, más aún

$$[P_{ij}] + [P_{kl}] \text{ es principal si y solo si } \{i, j\} = \{k, l\}.$$

Con lo cual cada $\{i, j\}$ determina únicamente un elemento en $\mathcal{J}(\mathcal{C})[2]$, pues $|\mathcal{J}(\mathcal{C})[2]| = 2^4 = 16$, que corresponden a las $\binom{6}{2}$ parejas con distintos puntos de Weierstrass en $\mathcal{C}$ mas el punto en el infinito. ■

Observación 1.14.1 *Cada elemento no nulo de* $\mathcal{J}(\mathcal{C})[2]$ *puede ser representado por el par* $\{i, j\}$ *y cada* $(x-\alpha_i)(x-\alpha_j)$ *determina un elemento* $[P_{ij}]$ *en* $\mathcal{J}(\mathcal{C})[2]$.

Proposición 1.14.1 *Sea* $\mathcal{J}(\mathcal{C})[2](\mathbb{F}_q) = \{[D] \in \mathcal{J}(\mathcal{C})[2] : [D]$ *está definido sobre* $\mathbb{F}_q\}$, *el* 2*-rango de* $\mathcal{J}(\mathcal{C})[2](\mathbb{F}_q)$ *depende de la factorización de* f *en* $\mathbb{F}_q$,

Factorización	*2-rango*
(1,4), (2,3)	*1*
(1,1,3), (1,2,2)	*2*
(1,1,1,2)	*3*
(1,1,1,1,1)	*4*

donde cada entrada de una tupla indica el grado de un factor de f.

Demostración. Si $[D]$ es un divisor con representación de Mumford $(u(x), v(x))$, entonces $-[D]$ tiene representación $(u(x), -v(x))$. Si $[D] \in \mathcal{J}(\mathcal{C})[2]$, entonces $[D] = -[D]$ y por la unicidad en la representación de Mumford tenemos que $v \equiv 0$. Por otro lado del algoritmo de Cantor, como $v^2 - f$ divide a u, entonces u divide a f

- Si $u(x) = (x-\alpha)(x-\beta)$, $v(x) = 0$, entonces de la proposición anterior $[D] = [P_1 + P_2 - 2\infty]$ con $P_1 = (\alpha, 0), P_2 = (\beta, 0)$.

- Si $u(x) = x - \alpha$, $D = [P_1 - \infty]$, con $P_1 = (\alpha, 0)$, de donde $[2D] = [2(\alpha, 0) - 2\infty] = div(x-\alpha)$, así $[D] \in \mathcal{J}(\mathcal{C})[2]$.

Concluimos entonces que los divisores $[D]$ con representación de Mumford $(u, 0)$ generan a $\mathcal{J}(\mathcal{C})[2]$ Así el 2-rango de $\mathcal{J}(\mathcal{C})[2](\mathbb{F}_q)$ es $m-1$, donde m es el numero de factores irreducibles de f en $\mathbb{F}_q$.

Ejemplo 1.14.1 *Sea $\mathcal{C} : y^2 = x^5 + 1$, calculemos $\mathcal{J}(\mathcal{C})[2](\mathbb{F}_q)$ para $p = 3, 5, 11$. Basta entonces recuperar una factorización de f en los diferentes cuerpos.*

- *Para $p = 3$, $y^2 = (x+1)(x^4 + 2x^3 + x^2 + 2x + 1)$, luego $u(x) = x + 1$ y $J(C)[2] = \langle [D] \rangle$, con representación de Mumford $(-1, 0)$.*

- *Para $p = 5$, la curva es singular.*

- *Para $p = 11$, $x^5+1 = (x+1)(x+3)(x+4)(x+5)(x+9)$, luego tomando $[D_1] = [(-1,0) - \infty], [D_2] = [(-3,0) - \infty], [D_3] = [(-4,0) - \infty]$ y $[D_4] = [(-5,0) - \infty]$, tenemos que $\mathcal{J}(\mathcal{C})[2] = (\mathbb{Z}/2\mathbb{Z})^4 \cong \langle [D_1] \rangle \times \langle [D_2] \rangle \times \langle [D_3] \rangle \times \langle [D_4] \rangle$.*

1.15. 3-Torsión

La técnica que usamos para calcular divisores de orden 3 es analizar los divisores que satisfacen la ecuación $[2D] = -[D]$, con la representación de Mumford de D dada por $(u(x), v(x))$. Usando la parte de composición del algoritmo de Cantor obtenemos divisores de la forma $(u^2(x); \tilde{v}(x))$ para $[2D]$. Por otro lado $-[D]$, con representación $(u(x), -v(x))$, luego de-reduciendo de la segunda coordenada de la forma $v + ku$ con $k = k_1 x + k_0$ obtenemos

$$u^2 = \frac{f - (v + uk)^2}{k_1^2 u}.$$

Observación 1.15.1 *Cabe destacar que, en la proposición 1.15.1, la aplicación del algoritmo de reducción en un único paso 1.10.3, justifica la presencia de a_0 en la expresión, a diferencia de los coeficientes k_0 o k_1.*

Proposición 1.15.1 *[39, Trisection for genus 2 curves in odd characteristic]*
Sea $\mathcal{C}$ una curva de género 2. $D_3 = [x^2 + u_1 x + u_0; v_1 x + v_0] \in J(C)[3]$ si y solo si $M(u_1) = 0$ donde M es el polinomio $3 - modular$

$$\begin{aligned} u_0 &= 2a_0 v_1 + \tfrac{1}{4}u_1^2 + \tfrac{5}{2}a_0^2 u_1 + \tfrac{1}{4}a_0^4, \\ v_0 &= \tfrac{5}{4}a_0 u_1^2 + \tfrac{1}{2}u_1 v_1 - \tfrac{5}{2}u_1 a_0^3 + \tfrac{1}{2}a_0 f_3 - \tfrac{5}{2}a_0^2 v_1 - \tfrac{1}{4}a_0^5, \\ v_1 &= 160a_0^6 u_1 - 32a_0^2 u_1 f_3 + 48a_0^2 f_2 + 450a_0^4 u_1^2 - 5u_1^4 - 16f_1, \\ &\quad +16u_1 f_2 - 12u_1^2 f_3 + 40a_0^2 u_1^3 + 11a_0^8 - 20a_0^4 f_3 / (24a_0(5u_1^2 + 5a_0^4 + 2f_3 + 20a_0^2 u_1)). \end{aligned}$$

y a_0 raíz de $mcm(p_1(a_0, u_1, p_2(a_0, u_1))$ donde p_1, p_2 son de grados 7 y 8 en a_0^2.

Ejemplo 1.15.1 *Consideremos $p = 2^{20} + 33$ y la curva definida por $y^2 = x^5 + x$ sobre $\mathbb{F}_p$.*

$$\begin{aligned} M(x) &= x^{40} + 183488x^{36} + 528540x^{32} + 565275x^{28} + 255328x^{24} + 882029x^{20} \\ &\quad +507685x^16 + 652433x^{12} + 58622x^8 + 150436x^4 + 718609. \end{aligned}$$

Nosotros obtenemos 3-rango 4 sobre $\mathbb{F}_p$. Sean

$$\begin{gathered} (x^2 + 622217x + 1048608, 597387x + 247526), \\ (x^2 + 560973x + 1048608, 214773x + 788568), \\ (x^2 + 587479x + 985970, 945347x + 349582), \\ (x^2 + 748357x + 62639, 857088x + 135670). \end{gathered}$$

Luego los divisores asociados a las representaciones de Mumford anteriores son una base del grupo de 3-torsión.

Notamos así la complejidad para caracterizar los diferentes ordenes de los divisores.

Capítulo 2

Isogenias entre variedades abelianas

El objetivo central de este capítulo, es el estudio de las isogenias entre variedades abelianas. Si bien reconocemos la rica diversidad de estas estructuras, no entraremos en un análisis exhaustivo de todas las variedades abelianas.

Un punto crucial en esta discusión es la polarización de las variedades abelianas, que jugará un papel determinante en nuestras consideraciones. En particular, nos restringiremos a aquellas variedades abelianas que presentan una polarización principal. La polarización no solo proporciona un marco para entender la geometría de estas variedades, sino que también es fundamental para asegurar que los morfismos que consideramos preserven la rica estructura inherente a los jacobianos.

De este modo, nuestro estudio se desarrollará en un contexto bien definido, donde la polarización principal actuará como un criterio necesario para las isogenias que nos proponemos estudiar. En particular, nos centraremos en isogenias que preservan la polarización.

2.1. Variedades Abelianas

Aunque en este capítulo no se profundizará en el estudio detallado de los grupos algebraicos y las variedades abelianas, se presentarán las nociones fundamentales necesarias para establecer el marco teórico de los resultados expuestos. Estas nociones básicas, si bien no pretenden ser exhaustivas, proporcionan los conceptos esenciales que se utilizarán a lo largo del texto.

Grupos algebraicos

Definición 2.1.1 *Un grupo algebraico G absolutamente irreducible sobre un cuerpo K es una variedad sobre K (afín o proyectiva) absolutamente irreducible, dotado de las siguientes aplicaciones:*

- *Un morfismo $m : G \times G \to G$, que será llamado adición.*
- *Un morfismo morfismo $i : G \to G$, que será llamado inverso.*
- *Un punto $K-$racional $\mathbf{0} \in G$, llamado neutro.*

verificando lo siguiente:

- $m \circ (Id_G \times m) = m \circ (m \times Id_G)$ *(asociatividad).*
- $m|_{\{0\}\times G} = P_2$*, donde P_2 es la proyección de $G \times G$, en el segundo argumento.*
- $m \circ (i \times Id_G) \circ \delta_G = c_o$*, donde δ_G es la función diagonal de $G \to G \times G$ y c_0 envía a G en* 0.

Sea L una extensión de K. Sea $G(L)$ el conjunto de los puntos $L-$racionales de G. El conjunto $G(L)$ es un grupo en el cual la suma y los inversos se calcula evaluando en morfismos que son definidos sobre K, que no dependen de L, en los cuales el elemento neutro es el punto $\mathbf{0}$.

Un hecho sorprendente es que si G es una variedad proyectiva, la ley de grupo m es necesariamente conmutativa.

Ejemplo 2.1.1 ***Grupo multiplicativo.*** *Sea G_m la variedad afín determinada por la ecuación $xy = 1$*

$$(V(xy-1)) = \{(a, a^{-1}) : \ a \in K \setminus \{0\}\}.$$

en $\mathbb{A}^2$. Las funciones $m((x,y),(x',y')) \mapsto (xx', yy')$ e $i(x,y) = (x^{-1}, y^{-1})$ son regulares en G_m. Se tiene que G_m junto con estas funciones satisfacen la definición anterior con neutro $(1,1)$. Además, como grupo multiplicativo se tiene que $G_m \cong K \setminus \{0\}$, con $(x, x^{-1}) \mapsto x$.

Una **variedad abeliana** es un objeto fundamental en geometría algebraica, que combina las estructuras algebraicas de un grupo con las propiedades geométricas de una variedad. Formalmente, definimos una variedad abeliana como sigue:

Definición 2.1.2 *Una **variedad abeliana** es una variedad algebraica A que es también un grupo, tal que la operación de grupo es regular (morfismo de variedades algebraicas) y la inversión también es regular, es decir:*

- *Existe una operación de grupo $+ : A \times A \to A$.*
- *La operación $+$ es asociativa, tiene un elemento neutro $0 \in A$, y cada elemento tiene un inverso.*
- *La operación de inversión $- : A \to A$ está dada por $-a$ para cada $a \in A$.*

Las variedades abelianas pueden tener distintas dimensiones y poseen una estructura de grupo algebraico compatible con su geometría. Se caracterizan por ser proyectivas y completas, lo que significa que pueden ser incrustadas en un espacio proyectivo mediante ecuaciones polinómicas y que toda secuencia de puntos dentro de la variedad cuya imagen en un espacio proyectivo posee un punto de acumulación en la variedad. En particular, la completitud garantiza que la operación de grupo esté bien definida en todo el dominio, sin singularidades o puntos en el infinito, lo que las distingue dentro de la teoría de variedades algebraicas.

Ejemplo 2.1.2

1. ***Curvas elípticas:** Estas son variedades abelianas de dimensión uno y pueden ser definidas como la solución de ecuaciones de la forma*

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

   donde a y b son constantes, ver 1.7. Tienen una rica estructura algebraica y son fundamentales en la teoría de números.

2. ***Variedades de Jacobiano:** Dada una curva algebraica de género g, su variedad de jacobiano es una variedad abeliana de dimensión g. Esta construcción permite estudiar las propiedades de la curva a través de su jacobiano, que encapsula información sobre las funciones meromorfas y los ciclos sobre la curva.*

3. ***Variedades abelianas de dimensión superior:** Existen diversas variedades abelianas de dimensión superior que no provienen directamente de una curva algebraica. Un ejemplo importante son las variedades de Prym, que surgen a partir de un cubrimiento finito de curvas, ver [21]. Dado un cubrimiento doble $\pi : \widetilde{C} \to C$*

de una curva $\mathcal{C}$, la variedad de Prym asociada a este cubrimiento se define como el núcleo de la norma del jacobiano de $\widetilde{\mathcal{C}}$ sobre el jacobiano de $\mathcal{C}$, es decir, $Prym(\pi) = \ker(Nm : \mathcal{J}(\widetilde{\mathcal{C}}) \to \mathcal{J}(\mathcal{C}))$, y tiene dimensión $g-1$, donde g es el género de $\widetilde{\mathcal{C}}$. Otra clase de variedades abelianas de dimensión superior son las variedades de Albanese, ver[41]. Dada una variedad proyectiva y lisa X, la variedad de Albanese $Alb(X)$ es la variedad abeliana que parametriza todos los morfismos de X hacia una variedad abeliana. Una variedad se dice lisa si es suave, es decir, no tiene puntos singulares, lo cual significa que su espacio tangente está bien definido en todos los puntos. En particular, el jacobiano de una curva es su variedad de Albanese, pero en dimensiones mayores el Albanese puede ser una variedad abeliana sin ser un jacobiano. Además, el producto de dos jacobianos de curvas distintas, como $\mathcal{J}(\mathcal{C}_1) \times \mathcal{J}(\mathcal{C}_2)$, es una variedad abeliana de dimensión $g_1 + g_2$, pero no necesariamente es un jacobiano, pues se trata de una variedad abeliana que no proviene de una sola curva. Estas construcciones son fundamentales en geometría algebraica, ya que permiten estudiar propiedades de variedades de dimensión superior sin recurrir exclusivamente a la noción de jacobiano.

4. ***Grupos de puntos racionales de variedades abelianas:*** *Si A es una variedad abeliana definida sobre un cuerpo K, entonces los puntos de A que son racionales sobre K forman un grupo abeliano.*

5. ***Producto de curvas elípticas:*** *Dada una colección de curvas elípticas, su producto forma una variedad abeliana. Por ejemplo, el producto de dos curvas elípticas es una variedad abeliana de dimensión dos.*

6. ***Variedades abelianas sobre cuerpos de números:*** *Estas variedades, que se encuentran en la teoría de números, incluyen ejemplos como las variedades de K3 y ciertas variedades de Fano [12].*

A continuación veremos que el jacobiano de una curva es una variedad abeliana que es "*naturalmente*" isomorfa a $Pic^0_K(\mathcal{C})$. Este isomorfismo natural dota a al jacobiano con una estructura de grupo.

Definición 2.1.3 *Sea $\mathcal{C}$ una curva de género 2 y K un cuerpo tal que $\mathcal{C}(K) \neq \emptyset$. Para un*

punto arbitrario en $P \in \mathcal{C}(\overline{K})$ *definimos*

$$\begin{aligned} l : \mathcal{C}(K) &\to Pic^0_K(\mathcal{C}) \\ Q &\mapsto [Q - P]. \end{aligned}$$

Esta función es inducida por el morfismo inyectivo $\tilde{l} : \mathcal{C} \hookrightarrow J$ para alguna variedad que tiene la siguiente propiedad universal.

Teorema 2.1.1 *Si* A *es una variedad abeliana y* $\psi : \mathcal{C} \to A$ *es un morfismo que envía* P *a la identidad de* A*, entonces existe un único homomorfismo* $\varphi : \mathcal{J} \to A$ *de variedades abelianas tales que* $\psi = \varphi \circ \tilde{l}$*,*

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\tilde{l}} & \mathcal{J} \\ {\scriptstyle\psi}\downarrow & \swarrow_{\varphi} & \\ A & & \end{array}$$

Siendo así, si podemos incluir los punto de la curva $\mathcal{C}$ en una variedad abeliana, dicha variedad es única.

El siguiente teorema asegura que el $Pic^0(\mathcal{C})$ es una variedad, y dada la unicidad anterior, es la única variedad abeliana con dicha propiedad.

Teorema 2.1.2 *[34, Thm 1.1](Variedad Jacobiana) Existe una variedad abeliana* $\mathcal{J}$ *sobre* K*, y un morfismo de funtores,* $i : Pic(\mathcal{C})^0 \to \mathcal{J}$*, tal que* $i : Pic(\mathcal{C})^0(T) \to \mathcal{J}(T)$ *es un isomorfismo de grupos donde* T *es un esquema conexo sobre* K*.*

Observación 2.1.1 *En matemáticas, un esquema es una estructura matemática que relaja la definición de variedad algebraica para incluir, entre otras cosas, multiplicidades (ej. las ecuaciones* $x = 0$ *y* $x^2 = 0$ *definen la misma variedad algebraica pero distintos esquemas) y "variedades"definidas sobre anillos (ej. las curvas de Fermat están definidas sobre el anillo de los números enteros).*

Los esquemas consideran ideas de tipo geométrico, algebraico y de teoría de números. La noción de esquema se remonta a los años 1960, cuando Alexander Grothendieck formuló el concepto en su tratado Éléments de géométrie algébrique. Una de las metas fue desarrollar el formalismo necesario para resolver problemas profundos en geometría algebraica, como las conjeturas de Weil (la última de las cuales fue demostrada por Pierre Deligne). Asimismo, la teoría de esquemas permite el uso sistemático

de métodos de topología y álgebra homológica. Al incluir consideraciones sobre puntos racionales, la teoría de esquemas introduce una fuerte conexión entre geometría algebraica y teoría de números, lo que eventualmente permitió a Wiles demostrar el último teorema de Fermat.

Teorema 2.1.3 *[33, Thm A 8.1.1] Sea $\mathcal{C}$ una curva hiperelíptica suave sobre K de género $g \geq 1$ tal que $\mathcal{C}(K) \neq \emptyset$. Existe una variedad abeliana $\mathcal{J}(\mathcal{C})$, llamada $Jacobiano\ de\ \mathcal{C}$ y una inyección $f : \mathcal{C} \hookrightarrow \mathcal{J}(\mathcal{C})$ llamada la incrustación de $\mathcal{C}$, con las siguientes propiedades:*

- *f se extiende linealmente a los divisores de $\mathcal{C}$. Entonces induce un isomorfismo de grupo entre $Pic^0(\mathcal{C})$ y $\mathcal{J}(\mathcal{C})$.*
- *Para cada $r \geq 0$ define una subvariedad $W_r \subseteq \mathcal{J}(\mathcal{C})$ dada por la suma de r copias de $f(\mathcal{C})$: $W_r = f(\mathcal{C}) + \cdots + f(\mathcal{C})$. Por convención $W_0 = 0$, entonces $dim(W_r) = min\{r, g\}$ y $W_g = \mathcal{J}(\mathcal{C})$. En particular $dim(\mathcal{J}(\mathcal{C})) = g$.*

De este modo, hemos observado que la construcción desarrollada en el Capítulo 1 permite asociar, a partir de una curva $\mathcal{C}$ de género 2 (definidas en 1.1.1), una variedad abeliana. Además, analizaremos cómo la idea subyacente en la construcción del grupo de Picard puede extenderse al contexto de variedades abelianas, lo que conduce naturalmente a la definición formal de la variedad dual asociada.

Procederemos ahora a presentar algunos resultados fundamentales sobre variedades abelianas que serán esenciales para continuar con el desarrollo de la teoría.

Teorema 2.1.4 *Toda variedad abeliana es un grupo abeliano.*

Demostración. Ver [43, Thm 3.15] ■

Observación 2.1.2 *Observamos que la estructura de grupo algebraico induce aplicaciones naturales, por ejemplo traslaciones por un elemento $x \in A$ que denotamos $t_x : A \to A$, la aplicación $t_x(z) = x + z$ para todo $z \in A$. t_x es biyectiva con inverso t_{-x}.*

Proposición 2.1.1 *Si $f : A \to B$ es un morfismo entre variedades abelianas y sea $t_x(z) = z + x$ la traslación por x . Entonces la función $t_{-f(0)} \circ f$ es un homomorfismo de grupos.*

Corolario 2.1.1 *Si $f(0) = 0$, f es un homomorfismo de grupos.*

Como A es una variedad abeliana, entonces es una variedad algebraica, luego podemos replicar lo hecho para $\mathcal{C}$ en el capítulo anterior, ver 1.8.

Recordemos además que, $\mathscr{L}(D)$ en 1.10.4 y por 1.10.2 es un K espacio vectorial de dimensión finita. Considerar $\mathscr{L}(D) = \langle f_0, \ldots, f_N \rangle$, con $f_i \in K(A)$ una K-base.

Definición 2.1.4 *Sea $D \in Div(A)$, definimos el morfismo racional*

$$\begin{array}{rccc} \varphi_D : & A & \longrightarrow & \mathbb{P}(K)^N \\ & x & \longmapsto & (f_0(x) : \cdots : f_N(x)). \end{array}$$

Definición 2.1.5 *Sea X y Y dos variedades algebraicas sobre un cuerpo K, y sea $f : X \to Y$ un morfismo de variedades algebraicas. Decimos que f es una **inmersión** si, para todo punto $p \in X$, la diferencial $df_p : T_pX \to T_{f(p)}Y$ es una aplicación lineal inyectiva entre los espacios tangentes de X en p y de Y en $f(p)$.*

En otras palabras, f es una inmersión si, en cada punto $p \in X$, el morfismo f preserva la estructura local de X al mapearla en Y. Esto se puede verificar a través de las siguientes condiciones equivalentes:

- *El morfismo f es localmente inyectivo. Esto significa que existe un entorno abierto de cada punto $p \in X$ tal que f es inyectivo en ese entorno.*
- *La matriz jacobiana de f es invertible en cada punto $p \in X$, lo que implica que las derivadas parciales de las funciones que definen f no se anulan en ningún punto.*
- *La diferencial df_p es inyectiva para cada punto $p \in X$, lo que significa que no colapsa ninguna dirección tangente en X.*

Ejemplo 2.1.3 *Consideremos las variedades algebraicas $X = \mathbb{A}^1$ (la recta afín) y $Y = \mathbb{A}^2$ (el plano afín). Supongamos que tenemos el siguiente morfismo $f : \mathbb{A}^1 \to \mathbb{A}^2$:*

$$f(t) = (t, t^2).$$

Este es un morfismo de variedades afines, donde t es la coordenada en $\mathbb{A}^1$ y (t, t^2) es la imagen en $\mathbb{A}^2$. Este morfismo describe una parábola en el plano. El morfismo f es una inmersión porque su diferencial, que es la derivada de f en términos de las coordenadas locales, es inyectiva. En este caso, la derivada de $f(t) = (t, t^2)$ es:

$$df(t) = \left(\frac{d}{dt} t, \frac{d}{dt} t^2 \right) = (1, 2t).$$

Para cualquier t, esta derivada es no nula, ya que el vector $(1, 2t)$ nunca es el vector cero, excepto en el punto $t = 0$ (pero aún así no colapsa direcciones tangentes en ese punto). Esto garantiza que, localmente, el morfismo no colapsa direcciones.

En términos geométricos, la parábola $f(t) = (t, t^2)$ no se dobla, ni colapsa en ningún punto: se comporta como una curva suave, lo que asegura que el morfismo f es una inmersión.

Definición 2.1.6 *Sea A una variedad abeliana, $D \in Div(A)$.*

- *D es un divisor muy amplio si φ_D es una inmersión.*
- *D es amplio si existe m entero positivo tal que mD es muy amplio.* [1]

Definición 2.1.7 *Sea $f : X \to Y$ un morfismo entre variedades algebraicas y sea D un divisor en Y. El pullback de D por f, denotado f^*D, es un divisor en X definido como sigue:*

$$f^*D = \sum_i a_i [f^{-1}(V_i)],$$

donde $D = \sum_i a_i [V_i]$ es la descomposición de D en términos de sus componentes irreducibles V_i en Y, y $[f^{-1}(V_i)]$ es el divisor generado por la preimagen de V_i bajo el morfismo f, con la misma multiplicidad a_i de cada V_i en D.

En otras palabras, f^*D es el divisor en X obtenido al tomar las preimágenes de las subvariedades V_i que componen D, con las mismas multiplicidades.

Ejemplo 2.1.4 *Consideremos el morfismo $f : \mathbb{A}^2 \to \mathbb{P}^2$ dado por:*

$$f(x, y) = (x : y : 1),$$

donde $\mathbb{A}^2$ es el plano afín y $\mathbb{P}^2$ es el plano proyectivo. Sea D el divisor en $\mathbb{P}^2$ dado por la línea L definida por la ecuación $y = 0$. Es decir, el divisor D es:

$$D = [L],$$

donde L es la línea en $\mathbb{P}^2$.

El pullback f^*D es el divisor en $\mathbb{A}^2$ que se obtiene al tomar la preimagen de L bajo f. La preimagen de L bajo f es la línea $y = 0$ en $\mathbb{A}^2$. Por lo tanto, el pullback f^*D es:

[1] En el contexto de geometría algebraica y curvas elípticas, el término 'amplio' y 'muy amplio' se traduce al inglés como 'ample' y 'very ample'.

$$f^*D = [\{(x,0) \in \mathbb{A}^2 : x \in k\}],$$

que es la línea $y = 0$ *en* $\mathbb{A}^2$*, con multiplicidad 1.*

Teorema 2.1.5 *(Cuadrado) Sean* A *una variedad abeliana y* $D \in Div(A)$ *un divisor sobre* A*. Sean* $a, b \in A$*, y* $t_x : A \to A$ *el morfismo de traslación dado por* $t_x(z) = x + z$ *para* $z \in A$*. Entonces, para* $D \in Div(A)$*, se cumple la siguiente relación de equivalencia de divisores:*

$$t^*_{a+b}D + D \sim t^*_a D + t^*_b D.$$

Aquí t^*_{a+b} *es el pullback de* D *bajo la traslación por* $a + b$*, y* t^*_a*,* t^*_b *son los pullbacks bajo las traslaciones por* a *y* b*, respectivamente. La notación* $\sim$ *denota equivalencia de divisores en* A*, es decir, que los dos lados difieren por un divisor principal.*

Demostración. Consideremos el morfismo de traslación en una variedad abeliana A asociado a un punto $x \in A$ está dado por

$$t_x : A \to A, \quad t_x(z) = x + z \quad \text{para todo } z \in A.$$

Este es un morfismo afín, que simplemente traslada cada punto de A por el vector $x \in A$. Dado un divisor $D \in \mathrm{Div}(A)$, el *pullback* de D bajo t_x, denotado por $t^*_x D$, está dado por 2.1.7,

$$t^*_x D = \sum_{P \in D} \text{multiplicidad}(P) \cdot (t_x^{-1}(P)),$$

donde $t_x^{-1}(P)$ denota el punto $P' \in A$ tal que $t_x(P') = P$, es decir, $P' = P - x$. Observemos que la traslación por $a + b$ sobre D se puede descomponer en la composición de traslaciones por a y b por separado. Es decir,

$$t^*_{a+b}D = t^*_a \circ t^*_b D.$$

La conmutatividad de la operación de adición en el grupo abeliano A garantiza que las traslaciones conmutan entre sí:

$$t^*_a \circ t^*_b = t^*_b \circ t^*_a.$$

Por lo tanto, la traslación por $a + b$ es equivalente a aplicar primero la traslación por a

y luego por b, lo que nos lleva a

$$t_{a+b}^* D \sim t_a^* D + t_b^* D.$$

Ahora, tenemos que considerar cómo la traslación afecta a los divisores. Dado que las traslaciones en A son isomorfismos, las clases de divisores son invariantes bajo traslaciones. Es decir, para cualquier divisor $D \in \mathrm{Div}(A)$, se cumple que

$$t_x^* D \sim D \quad \text{para todo } x \in A.$$

Por lo tanto, usando esta propiedad y la descomposición de traslaciones, obtenemos la equivalencia de divisores:

$$t_{a+b}^* D + D \sim t_a^* D + t_b^* D.$$

Hemos demostrado que, para cualquier divisor $D \in \mathrm{Div}(A)$ sobre una variedad abeliana A, y para cualquier par de puntos $a, b \in A$, se cumple la siguiente equivalencia de divisores:

$$t_{a+b}^* D + D \sim t_a^* D + t_b^* D.$$

Este resultado es una propiedad clave de las traslaciones en variedades abelianas, y muestra cómo el comportamiento de los divisores bajo traslaciones se descompone de manera natural en términos de las traslaciones individuales. La equivalencia de divisores implica que las traslaciones por $a+b$ y las traslaciones por a y b por separado tienen el mismo efecto en términos de clases de divisores. ■

Corolario 2.1.2 *Sean A una variedad abeliana y $D \in Div(A)$, definimos la función*

$$\begin{array}{rccc} \psi_D : & A & \longrightarrow & Pic(A) \\ & a & \longmapsto & [t_a^* D - D], \end{array}$$

ψ_D es un homomorfismo de grupos.

Demostración. Sean $a, b \in A$,

$$\begin{aligned}\psi_D(a+b) &= [t^*_{a+b}D - D],\\ &= [t^*_a D + t^*_b D - D - D], \quad por \ \ 2{,}1{,}5,\\ &= [t^*_a D - D] + [t^*_b D - D],\\ &= \psi_D(a) + \psi_D(b).\end{aligned}$$

■

Observación 2.1.3 *Sea A una variedad abeliana, para todo $b \in A$, y $D \in Div(A)$,*

$$\begin{aligned}t^*_b(t^*_a D - D) &= t^*_b(t^*_a D) - t^*_b D,\\ &= (t_a \circ t_b)^* D - t^*_b D,\\ &= t^*_{a+b} D - t^*_b D,\\ &\sim t^*_a D - D, \quad por \ \ 2{,}1{,}5.\end{aligned}$$

Es decir $t^*_b[t^*_a D - D] = [t^*_a D - D]$, o bien $t^*_b \psi_D(a) = \psi_D(a)$.

2.2. Dual de una variedad abeliana

Como observación principal, destacamos que el concepto de dual es clave para la definición de la polarización y, en particular, de la polarización principal. En este contexto, surgen tres situaciones importantes a considerar:

1. En el caso de una curva elíptica, es bien sabido que esta admite un grupo que, esencialmente, está dado por los puntos de la propia curva.

2. Para curvas de género mayor o igual a 2, esta propiedad no se mantiene; en tales casos, la curva se inyecta de manera natural en una variedad abeliana asociada.

3. A partir de la variedad abeliana construida, introduciremos su grupo de Picard y analizaremos cómo se relaciona esta variedad con su dual, profundizando en las conexiones entre ambos conceptos.

Definición 2.2.1 *Definimos el subgrupo $Pic^0(A)$ de $Pic(A)$, como*

$$Pic^0(A) := \{D \in Pic(A) : t^*_b D = D\}.$$

Por la observación 2.1.3, $Pic^0(A)$ es no trivial, ademas dado $D \in Div(A)$, $Im(\psi_D) \subseteq Pic^0(A)$. $Pic^0(A)$ tiene estructura de variedad abeliana; más aún $Pic^0(A)$ se llama la variedad abeliana dual de A, denotada por $A^\vee$.

Teorema 2.2.1 *Sea A una variedad abeliana y $D \in Div(A)$ con $D \geq 0$. Los siguientes enunciados son equivalentes,*

- *D es amplio.*
- *$Im(\psi_D) = Pic^0(A)$.*
- *$ker\psi_D$ es finito.*

Definición 2.2.2 *Sea A una variedad abeliana, definimos el grupo de $Neron - Severi$ por*

$$NS(A) = Pic(A)/Pic^0(A).$$

2.3. Isogenias

El teorema 2.2.1 nos dice, esencialmente que, por cada divisor amplio tenemos morfismo con las propiedades descritas en la siguiente definición.

Definición 2.3.1 *Sean A e B variedades abelianas sobre $K = \mathbb{F}_q$, $q = p^n$, con p primo. Decimos que un homomorfismo $\phi : A \to B$ es una isogenia si es sobreyectivo y su núcleo es finito. Si existe tal homomorfismo diremos que A y B son isogenas y lo denotamos por $A \sim_K B$.*[2]

Definición 2.3.2 *Sea A y B dos variedades abelianas sobre un cuerpo finito K. Decimos que una isogenia simétrica entre A y B es una isogenia sobreyectiva $\varphi : A \to B$ tal que existe una isogenia inversa $\psi : B \to A$ que satisface las siguientes propiedades:*

- *La composición de φ y ψ es un múltiplo de la aplicación identidad de B, es decir,*

$$\varphi \circ \psi = [m] \cdot \mathrm{id}_B,$$

donde $m \in \mathbb{Z}$ es un entero.

[2] En algunos textos se define isogenia, de forma equivalente, como un homomorfismo no constante que lleva el neutro en el neutro.

- *La composición de ψ y φ es un múltiplo de la aplicación identidad de A, es decir,*

$$\psi \circ \varphi = [n] \cdot \mathrm{id}_A,$$

  donde $n \in \mathbb{Z}$ es otro entero.

Aquí, id_A y id_B son las aplicaciones identidad en las variedades abelianas A y B, respectivamente, y $m, n \in \mathbb{Z}$ son enteros.

Definición 2.3.3 *El grado de separabilidad de ϕ es el grado separable de la extensión $[\mathbb{F}_q(A) : \phi^*(\mathbb{F}_q(B)]$. Decimos que ϕ es separable si la extensión $\mathbb{F}_q(A)|\phi^*(\mathbb{F}_q(B)$ es separable, donde $\phi^* : \mathbb{F}_q(B) \to \mathbb{F}_q(X)$ y $\phi^*(f) = f \circ \phi$, es decir ϕ^* el pullback de ϕ. De manera análoga para el caso no separable.*

Ejemplo 2.3.1 *Un ejemplo importante de isogenia es la multiplicación por n, es decir,*

$$\begin{array}{rccc} [n]_A : & A & \longrightarrow & A \\ & x & \longmapsto & n \cdot x. \end{array}$$

Escribiremos $A[n] := ker[n]_A \subseteq X$.

Teorema 2.3.1 *Sea X una variedad abeliana, entonces existe una correspondencia uno a uno entre:*

- *Subgrupos finitos $H \leq X$.*
- *Isogenias separables $\phi : X \to Y$.*

Demostración. Ver [36, Thm 4.] ■

Definición 2.3.4 *Decimos que $\phi_1 : X \to Y_1$ y $\phi_2 : X \to Y_2$ con $ker\phi_1 = ker\phi_2 = H$ son iguales si existe un isomorfismo $\psi : Y_1 \to Y_2$ tal que $\phi_2 = \psi \circ \phi_1$, que es establecido por $H = ker\phi$ y $Y = X/H$.*

Observación 2.3.1 *Las isogenias están únicamente determinadas por su kernel. Sea $\mathcal{J}(\mathcal{C}_1)$ y $\mathcal{J}(\mathcal{C}_2)$ los jacobianos de curvas suaves $\mathcal{C}_1$ y $\mathcal{C}_2$. Sea $N \subseteq J(C_1)$ un subgrupo finito. Existe una única isogenia (salvo isomorfismo) $\phi : \mathcal{J}(\mathcal{C}_1) \to \mathcal{J}(\mathcal{C}_2)$ con núcleo exactamente N.*

Demostración. *Existencia: Se construye la variedad cociente $J(C_1)/N$. Como N es un subgrupo finito de una variedad abeliana, el cociente es otra variedad abeliana $A = \mathcal{J}(\mathcal{C}_1)/N$ y la proyección canónica*

$$\pi : \mathcal{J}(\mathcal{C}_1) \to A,$$

es un morfismo de variedades abelianas con núcleo N. Si $A \cong \mathcal{J}(\mathcal{C}_2)$, entonces podemos tomar $\phi = \pi$.

Unicidad: Supongamos que existen dos isogenias $\phi, \psi : \mathcal{J}(\mathcal{C}_1) \to \mathcal{J}(\mathcal{C}_2)$ con $\ker(\phi) = N = \ker(\psi)$. Consideremos el morfismo

$$\psi^{-1} \circ \phi : \mathcal{J}(\mathcal{C}_1) \to \mathcal{J}(\mathcal{C}_1).$$

Este es un endomorfismo de $\mathcal{J}(\mathcal{C}_1)$ cuya restricción al núcleo N es trivial. Como ϕ y ψ inducen el mismo cociente $\mathcal{J}(\mathcal{C}_1)/N$, se sigue que $\psi^{-1} \circ \phi$ actúa como la identidad en dicho cociente, lo que implica que $\phi = \psi$. ■

Definición 2.3.5 *Sea $\phi : \mathcal{J}(\mathcal{C}_1) \to \mathcal{J}(\mathcal{C}_2)$ una isogenia entre variedades abelianas. Se dice que ϕ es una $(a_1, \ldots, a_n)$-isogenia si su núcleo es un grupo abeliano finito isomorfo a*

$$\ker\phi \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z},$$

donde $n \geq 1$ y los enteros a_i satisfacen la condición de divisibilidad $a_i \mid a_{i+1}$ para todo i.

Esto se justifica utilizando la teoría de módulos libres finitamente generados sobre dominios de ideales principales.

Observación 2.3.2 *Por el Teorema 2.2.1, el homomorfismo ψ_D definido en 2.1.2 es una isogenia asociada al divisor amplio $D \in \mathrm{Div}(A)$. En particular, $\ker\psi_D$ es un grupo finito de la forma*

$$\ker\psi_D \cong (\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z})^2,$$

donde $n = \dim A$ y $d_1, \ldots, d_n$ son enteros positivos tales que $d_i \mid d_{i+1}$ para cada i. Diremos que la tupla $(d_1, \ldots, d_n)$ es el tipo de la polarización inducida por D.

En este contexto, el divisor D induce una polarización en A, y ψ_D es la isogenia de la variedad abeliana asociada a esta polarización. El orden de $\ker\psi_D$ es igual al grado de la isogenia y está dado por $\prod_{i=1}^{n} d_i^2$.

Teorema 2.3.2 *Si $f : A \to B$ es una isogenia de grado d, entonces existe una isogenia $g : B \to A$ donde $g \circ f = [d]_A$ y $f \circ g = [d]_B$*

Demostración. Ver [2, Prop. 5.12.] ■

Corolario 2.3.1 *La relación " $\sim_K$ " dada por, $A \sim_K B$ si y solo si existe una isogenia de A en B, con cuerpo base K, es una relación de equivalencia.*

2.4. Polarización

En el contexto de variedades abelianas, en particular de curvas hiperelípticas de género 2, la noción de polarización juega un papel crucial en la clasificación. En el contexto de isogenias, cuando estas preservan una polarización, y en particular la polarización principal, se limitan a aquellas que van de un jacobiano de una curva hiperelíptica a otro jacobiano de curva hiperelíptica.

Este tipo de isogenias son esencialmente las que preservan la estructura geométrica y algebraica asociada a las curvas hiperelípticas.

En el estudio de isogenias entre variedades abelianas de dimensión dos, se pueden identificar distintas clases de isogenias: isogenias genéricas, que relacionan el jacobiano de una curva de género dos con otro jacobiano; isogenias de separación, que descomponen un jacobiano como producto de curvas elípticas; isogenias de producto, que corresponden a isogenias entre productos de curvas elípticas; e isogenias de pegado, que conectan un producto de curvas elípticas con un jacobiano. En el presente trabajo, nos enfocaremos en el estudio de las isogenias genéricas y de separación, estableciendo criterios que permitan determinar cuándo el jacobiano de una curva es isogena a una variedad abeliana de tipo jacobiano o a un producto de curvas elípticas.

Definición 2.4.1 *Sea A una variedad abeliana. La isogenia $\psi_D : A \to A^\vee$ determinada por el divisor amplio D es llamada polarización. Diremos ademas que D es una polarización principal si ψ_D es un isomorfismo. Si A es una variedad abeliana para la cual existe dicha polarización principal, la llamaremos variedad abeliana principalmente polarizada y escribiremos $VAPP$.*

Teorema 2.4.1 *Sea $f : X \to Y$ una isogenia. Si $\varphi : Y \to Y^\vee$ es una polarización, entonces*

$f^*\varphi := f^* \circ \varphi \circ f$, $f^*\varphi : X \to X^\vee$ es una polarización.

$$\begin{array}{ccc} Y & \xrightarrow{\varphi} & Y^\vee \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle f^*} \\ X & \xrightarrow{f^*\varphi} & X^\vee \end{array}$$

Demostración. De 2.3.1, tenemos que la composición de isogenias es también una isogenia, por tanto, $f^*\varphi$ es de nuevo una isogenia. Para verificar que es una polarización, ver [2, Prop 11.8]. ■

¿Por qué son importantes las polarizaciones principales? Recordemos que dada una curva hiperelíptica $\mathcal{C}$, construimos su $Pic^0(\mathcal{C})$ y vimos que se identifica con $\mathcal{J}(\mathcal{C})$, ver 1.1.1,1.8.1 y 2.1.2.

Dado $Q \in \mathcal{C}$, en general se suele tomar $Q = \infty$, tenemos la inclusión o bien la función de Abel-Jacobi, que es una inmersión, [16, Thm 17, Prop 18]:

$$\begin{array}{rccc} \alpha_Q : & \mathcal{C} & \longrightarrow & \mathcal{J}(\mathcal{C}) \\ & P & \longmapsto & [P - Q] \end{array}$$

Definición 2.4.2 *Sea $\mathcal{C}$ una curva de género g suave, $Q \in \mathcal{C}$, definimos el divisor Θ inducido por la suma de $g-1$ veces la función de Abel-Jacobi:*

$$\begin{aligned} \Theta &:= \alpha_Q(\mathcal{C}) + \cdots + \alpha_Q(\mathcal{C}), \\ &= \{[P_1 - Q] + [P_2 - Q] + \cdots + [P_{g-1} - Q] : P_i \in \mathcal{C}\}, \\ &= \{[P_1 + \cdots + P_{g-1} - (g-1)Q] : P_i \in \mathcal{C}\}, \\ &\subseteq \mathcal{J}(\mathcal{C}). \end{aligned}$$

Dicho de otro modo, Θ es la imagen de la función

$$\begin{array}{ccc} \mathcal{C}^{g-1} & \longrightarrow & \mathcal{J}(\mathcal{C}) \\ (P_1, \ldots, P_{g-1}) & \longmapsto & [P_1 + \cdots, P_{g-1} - (g-1)Q] \end{array}$$

La propiedad fundamental que queremos viene asociada a este divisor Θ.

Teorema 2.4.2 *(Riemann) Sea $\mathcal{C}$ una curva de género g. El divisor Θ es amplio y es una polarización principal.*

Demostración. Consideremos

$$\begin{array}{rccc} \psi_\Theta: & \mathcal{J}(\mathcal{C}) & \longrightarrow & Pic^0(\mathcal{J}(\mathcal{C})) \\ & a & \longmapsto & [t_a^*\Theta - \Theta]. \end{array}$$

Es un Isomorfismo. [1, Ch. 1.5., pp 25], [3, Th. 45.]. ■

Definición 2.4.3 *Sea X una curva proyectiva suave. Definimos los conjuntos, salvo isogenias:*

$$\mathcal{M}_g = \{X : X \text{ es una curva proyectiva de género } g\}$$

$\mathcal{A}_g = \{(A, D) : A \text{ es variedad abeliana de dimensión } g, D \text{ es una polarización principal}\}$

Teorema 2.4.3 *(Torelli) Sea X una curva proyectiva suave. La asignación que envía a la curva X es un incrustamiento salvo isogenias, dicho de otra forma. la función j es inyectiva*

$$\begin{array}{rccc} j: & \mathcal{M}_g & \longrightarrow & \mathcal{A}_g \\ & X & \longmapsto & (\mathcal{J}(X), \Theta). \end{array}$$

Demostración. Ver [11, Thm 4.1] ■

El teorema anterior nos asegura que cuando consideramos las curvas de género 2, bajo la relación de equivalencia de ser isogenias, esta queda determinada por una única variedad abeliana de dimensión 2 y una polarización. Más aún, el siguiente teorema determina completamente $\mathcal{A}_2$.

Teorema 2.4.4 *Si A es una variedad abeliana sobre $\overline{\mathbb{F}}_p$ principalmente polarizada, entonces $A \cong \mathcal{J}(X)$ para alguna curva X de género 2, o bien $A \cong E_1 \times E_2$ con E_i curvas elípticas. Dicho de otra forma*

$$\mathcal{A}_2 = j(\mathcal{M}_2) \sqcup \{E_1 \times E_2 : E_1, E_2 \text{ curvas elípticas}\}.$$

Demostración. Ver [18, Th. 3.1.] y [46, Th. 1.7.] ■

Observación 2.4.1 *La caracterización del teorema anterior, implica a su vez una caracterización para isogenias. Notar que la descripción de un jacobiano como variedad abeliana para una curva de género 2 es altamente no trivial. En [5] se da una construcción explícita resultado con una curva proyectiva en $\mathbb{P}^{15}$, definida por 72 formas cuadráticas sobre K.*

Ejemplo 2.4.1 *Veamos un ejemplo de cuando tenemos $\mathcal{J}(\mathcal{C}) \cong E_1 \times E_2$. Consideremos $\mathcal{C}$ curva de género 2 definida por*

$$\mathcal{C} : y^2 = Ax^6 + Bx^4 + Cx^2 + D.$$

Podemos definir E_1 y E_2 dadas por

$$E_1 : y^2 = Ax^3 + Bx^2 + Cx + D \quad y \quad E_2 : y^2 = Dx^3 + Cx^3 + Bx + A.$$

Definimos los morfismo no constantes $(x, y) \mapsto (x^2, y)$ y $(x, y) \mapsto (1/x^2, y/x^3)$ respectivamente. El jacobiano de la curva de género 2, denotado por $\mathcal{J}(\mathcal{C})$, tiene una polarización principal, mientras que el jacobiano de una curva elíptica $\mathcal{J}(E_i)$ es simplemente E_i mismo, con su polarización canónica. Los morfismos inducen un mapa

$$\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(E_1) \times \mathcal{J}(E_2) \cong E_1 \times E_2.$$

Para que esta isogenia preserve la polarización, el núcleo de ϕ debe ser isotrópico con respecto al emparejamiento de Weil que definiremos en la siguiente sección 2.5.2. En este caso, dado que los morfismos son de la forma $(x, y) \mapsto (x^2, y)$, el núcleo típico incluiría puntos con x relacionado con raíces de la unidad en un cierto cuerpo de definición. Sin embargo, en isogenias inducidas por estas transformaciones cuadráticas, el núcleo no suele ser isotrópico, lo que sugiere que la isogenia no preserva la polarización. Esto ilustra que, aunque una variedad abeliana principalmente polarizada puede ser isógena a un producto de curvas elípticas, dicha isogenia no necesariamente preserva la principalidad de la polarización.

Queremos estar en el ámbito donde la única posibilidad para una isogenia sea entre dos jacobiano asociados a una curva hiperelíptica, ademas de conservar la polarización principal, para ello introduciremos los emparejamientos, que dará una clasificación al respecto.

2.5. Emparejamientos

Hemos visto algunas características de las isogenias entre variedades abelianas, y las condiciones para que dichas isogenias sean entre jacobianas de curvas de género 2 o producto de curvas elípticas.

Queremos trabajar específicamente con isogenias de tipo (ℓ,ℓ) como se definieron en 2.3.5, luego definiremos nociones para poder determinar cuando tenemos una de estas isogenias.

Definición 2.5.1 *El ℓ-emparejamiento de Weil*
Para una curva elíptica E definida sobre K y un entero ℓ no divisible por la característica de K, existe una forma bilineal,

$$E(\overline{K})[\ell] \times E(\overline{K})[\ell] \to \mu_\ell(\overline{K}),$$

donde $\mu_\ell(\overline{K})$ es el grupo de las ℓ-raíces de la unidad en $\overline{K}$. Esta forma es llamada ℓ-emparejamiento de Weil y es no degenerada, antisimétrica, bilineal alternante y conmuta con la acción de $Gal(\overline{K}|K)$. Ver [15, Thm 26.2.3].

Para variedades abelianas la definición es esencialmente igual, salvo que la polarización y la variedad dual juegan un papel mas notorio, lo que no se desprende en el emparejamiento de Weil, puesto que las curvas elípticas son isogenas a su dual y siempre son principalmente polarizadas.

Definición 2.5.2 *(Emparejamiento para variedades abelianas)*
Sea A una variedad abeliana, definimos la forma bilineal

$$e_m : A(\overline{K})[m] \times A^\vee(\overline{K})[m] \to \mu_m(\overline{K}),$$

que es no degenerada y conmuta con $Gal(\overline{k}|K)$. Ademas si consideramos una polarización $\phi : A \to A^\vee$ una polarización, entonces puede definirse el emparejamiento de Weil(o m-emparejamiento de Weil) por

$$\begin{array}{rccc} e_m^\phi : & A(\overline{K})[m] \times A(\overline{K})[m] & \longrightarrow & \mu_m(\overline{K}) \\ & (a,b) & \longmapsto & e_m^\phi(a,b) = e_m(a,\phi(b)). \end{array}$$

Que es una forma no degenerada y bilineal. Si ϕ es de la forma ϕ_D, para algún $D \in Pic(A)$, entonces $e_m^\phi(a,b) = e_m(a,\phi(b))$ es antisimétrica. [34, Thm. 13.6], [8, Thm. 3.4], [32, Thm. 11.2].

Observación 2.5.1 *El emparejamiento de Weil sobre una variedad abeliana depende de la elección de una polarización y, por tanto, no es único de manera absoluta. Sin*

embargo, una vez fijada una polarización, dicho emparejamiento posee propiedades canónicas, como ser bilineal, alternado y no degenerado. Existen también otros emparejamientos en el contexto de variedades abelianas, como el emparejamiento de Tate, que se define en términos de la teoría de torsión en el grupo de divisores de la variedad. Al igual que el emparejamiento de Weil, el emparejamiento de Tate también depende de la polarización, pero tiene aplicaciones distintas, particularmente en la teoría de números y criptografía, donde se utiliza para establecer relaciones entre puntos de torsión, para profundizar se sugiere ver [14].

Ejemplo 2.5.1 *Consideremos* $\mathcal{C} : y^2 = \prod_{i=1}^{6}(x - r_i)$. *Por 1.14.1, sabemos que*

$$\mathcal{J}(\mathcal{C})[2] \setminus \{0\} = \left\{R_{ij} := \mathcal{J}((x - r_i)(x - r_j), 0) : i \neq j\right\}.$$

Entonces tenemos el 2-emparejamiento de Weil, dado por:

$$e_2(R_{i,j}, R_{kl}) = \begin{cases} -1 \quad si \quad |\{i,j\} \cap \{k,l\}| = 1 \\ \\ 1 \qquad\qquad \text{en otro caso.} \end{cases}$$

Observación 2.5.2 *Como se señala en el capitulo 26, sección 2 de [15] , existe una forma más operacional o concreta de dicho emparejamiento, a saber:*
Sea $\mathcal{C} : y^2 = f(x)$ *una curva hiperelíptica definida sobre un cuerpo* K, *de género* g, *donde* $f(x)$ *es un polinomio de grado* $2g+1$ *o* $2g+2$. *Para dos puntos* $P, Q \in \mathcal{C}[K]$ *de orden* m, *el* ***emparejamiento de Weil*** *se define como:*

$$e(P,Q) = \frac{r(Q)}{s(P)} \mod K^*,$$

donde:

- r *es una función racional en* $\mathcal{C}$ *con divisor* $\operatorname{div}(r) = m[P] - m[\infty]$,
- s *es una función racional en* $\mathcal{C}$ *con divisor* $\operatorname{div}(s) = m[Q] - m[\infty]$,
- K^* *es el grupo multiplicativo del cuerpo base* K,
- m *es el orden de torsión de los puntos* P *y* Q.

Definición 2.5.3 *Sea* A *una variedad abeliana con polarización principal* $\phi : A \to A^\vee$ *sobre* $\mathbb{F}_q$ *y* $mcd(\ell, q) = 1$. *Decimos que* $S \subseteq A[\ell]$ *es maximal* ℓ*-isotrópico si:*

1. *El ℓ-emparejamiento de Weil, e_ℓ^ϕ, se restringe trivialmente a S.*

2. *S no está contenido en ningún otro subgrupo de $A[\ell]$ que cumpla* 1.

La proposición [22, Prop. 1.1] nos da condiciones para la existencia de dicho subgrupo maximal isotrópico para una superficie abeliana principalmente polarizada, SAPP[3], A.

Definición 2.5.4 *[46, Def 5.1] Un subgrupo S de $A[m]$ es $bueno$, si $A[n] \not\subseteq S$ para ningún $1 < n \leq m$.*

El siguiente teorema se restringe a las isogenias cuyo dominio son jacobianos de curvas hiperelípticas.

Teorema 2.5.1 *[46, Prop 5.1] Sea $\mathcal{C}$ una curva de género 2 sobre $\mathbb{F}_p$. Sea H un subgrupo racional bueno y finito de $\mathcal{J}(\mathcal{C})(\overline{\mathbb{F}}_q)$. Existe una variedad abeliana A principalmente polarizada sobre $\mathbb{F}_q$ y una isogenia $\phi : \mathcal{J}(\mathcal{C}) \to A$ con $ker(\phi) = H$ si y solo si H es un subgrupo maximal isotrópico de $\mathcal{J}(\mathcal{C})[m]$ para algún entero positivo m.*

Más aún, se puede distinguir la estructura del subgrupo bueno maximal isotrópico.

Lema 2.5.1 *[46, Lemma 5.1] Sea A una variedad abeliana principalmente polarizada. Si H es un buen subgrupo maximal ℓ^n isotrópico, entonces H no puede ser cíclico.*

El siguiente teorema caracteriza los subgrupos maximales isotrópico y nos dice los grupos que tenemos que estudiar para comprender las (ℓ, ℓ) isogenias.

Proposición 2.5.1 *[46, Prop 5.3] Sea A una variedad abeliana principalmente polarizada. Entonces los subgrupos maximales ℓ^n isotrópico de $A[\ell^n]$ son isomorfos a*

$$\mathbb{Z}_{\ell^n} \times \mathbb{Z}_{\ell^n} \quad o \quad \mathbb{Z}_{\ell^n} \times \mathbb{Z}_{\ell^{n-k}} \times \mathbb{Z}_{\ell^k}$$

donde $1 \leq k \leq \lfloor n/2 \rfloor$.

Observación 2.5.3 *Sea $\mathcal{J}(\mathcal{C})[2]$ el grupo de 2-torsión del jacobiano de una curva de género 2. Este grupo tiene la estructura $(\mathbb{Z}/2\mathbb{Z})^4$, con $2^4 = 16$ elementos. Cualquier subgrupo isotrópico $R \subseteq \mathcal{J}(\mathcal{C})[2]$ debe satisfacer que su orden es 2^k, donde $k \in \{0,1,2,3,4\}$. Verifiquemos cuáles de estos órdenes son compatibles con la isotropía:*

[3] Para curvas de género 0 se habla de *curvas racionales*, para género 1 de *curvas elípticas*, para género 2 de *superficies abelianas*, y para género 3 en adelante de *variedades abelianas*.

- *Si* $|R| = 1$*:* $R = \{0\}$*, el subgrupo trivial, que no es interesante en este contexto.*
- *Si* $|R| = 2$*:* R *es un subgrupo cíclico* $(\mathbb{Z}/2\mathbb{Z})$*, pero no puede ser isotrópico, ya que la isotropía requiere al menos dos generadores linealmente independientes por 2.5.1.*
- *Si* $|R| = 4$*:* R *tiene estructura* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*. Este caso es compatible con la isotropía porque el emparejamiento de Weil* e_2 *se anula para todos los pares de elementos en* R*, debido a la bilinealidad y la no degeneración de* e_2*.*
- *Si* $|R| = 8$*:* R *no puede ser isotrópico, ya que existirían pares* $P, Q \in R$ *tales que* $e_2(P,Q) \neq 1$*, contradiciendo la isotropía.*
- *Si* $|R| = 16$*:* $R = J(C)[2]$*. Este es el caso maximal, pero claramente no es isotrópico, ya que la no degeneración del emparejamiento de Weil implica la existencia de elementos con* $e_2(P,Q) \neq 1$*.*

Por lo tanto, el único caso compatible con la isotropía es cuando $|R| = 4$*. Esto implica que cualquier subgrupo isotrópico* R *tiene exactamente 4 elementos, y su estructura es* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*.*

Definición 2.5.5 *Sean* A *y* B *dos VAPP's de dimensión* d *y* $\phi : A \to B$ *una isogenia. Entonces diremos que* ϕ *es una* $(\ell, \ldots, \ell)$*-isogenia si* $ker(\phi) \cong \mathbb{Z}_\ell^d$ *y* $ker(\phi)$ *es maximal* ℓ*-isotrópico.*

Hemos definido que es una polarización principal para una variedad abeliana, como se clasifican las variedades principalmente polarizadas y determinado aquellos buenos subgrupos que podemos tomar como los núcleos de las isogenias para que preserven la polarización. De ahora en mas estudiaremos las isogenias de tipo $(2,2)$.

Capítulo 3

Isogenias de Richelot

Las correspondencias de Richelot son herramientas fundamentales en el estudio de isogenias entre variedades abelianas, particularmente en el contexto de curvas hiperelípticas de género 2 y sus jacobianas. Estas correspondencias permiten describir condiciones explícitas bajo las cuales una isogenia entre variedades abelianas se puede descomponer en un producto de curvas elípticas o preservar la estructura de jacobianos.

En este capítulo, exploraremos el criterio de Richelot para determinar si una isogenia de tipo $(2,2)$ conecta el jacobiano de una curva hiperelíptica con un producto de curvas elípticas, o si establece una relación entre dos jacobianos distintos. Además, introduciremos algunas nociones generales sobre isogenias de tipo $(2^n, 2^n)$, enfatizando su rol en la clasificación de variedades abelianas polarizadas y su conexión con curvas algebraicas.

A través de estas discusiones, buscamos proporcionar un marco conceptual y práctico que facilite la comprensión de estas estructuras, destacando tanto sus aspectos teóricos como su potencial para aplicaciones en áreas como la teoría de números y la criptografía.

Ademas, queremos estudiar las isogenias de la forma $\phi : A \to A'$ tal que se pueda ver como una cadena que no retrocede, es decir, una cadena de isogenias $\phi_1, \phi_2, \ldots, \phi_n$ entre superficies abelianas $A_0, A_2, \ldots, A_n$, donde cada $\phi_i : A_{i-1} \to A_i$ es una isogenia de tipo $(2,2)$, y ninguna variedad A_i se repite a lo largo de la cadena.

$$A = A_0 \xrightarrow{\phi_1} A_1 \longrightarrow \cdots \xrightarrow{\phi_i} A_i \longrightarrow \cdots \xrightarrow{\phi_n} A_n = A'.$$

donde $ker(\phi_i) = 2^{n-1}\langle \psi_{i-1}(G_1), \psi_{i-1}(G_2)\rangle$ y $\psi_i = \phi_i \circ \cdots \circ \phi_1$.

Por el lema1.14.1, sabemos que cada elemento no nulo de $\mathcal{J}(\mathcal{C})[2]$ puede ser únicamente representado por un par de distintos puntos de Weierstrass de $\mathcal{C}$. Por lo tanto cada factor cuadrático del polinomio f que define la curva de género 2, 1.1.1, de la forma $(x-\alpha_i)(x-\alpha_j)$, determina un elemento de $\mathcal{J}(\mathcal{C})[2]$. El siguiente teorema relaciona los elementos de 2-torsión con sus respectivos factores cuadráticos utilizando el 2-emparejamiento de Weil.

Definición 3.0.1 *Sea $\mathcal{C}$ una curva de género 2, decimos que $H \leq \mathcal{J}(\mathcal{C})[2]$ es un $(2,2)$ subgrupo, si es el kernel de una $(2,2)$-isogenia.*

Lema 3.0.1 *Sea $[P],[Q] \in \mathcal{J}(\mathcal{C})[2]$ con sus factores cuadráticos asociados G_P y G_Q de $f(x)$ como se menciono anteriormente. Entonces el 2-emparejamiento de Weil $e_2(P,Q) = 1$ si y solo si G_P y G_Q son coprimos.*

Demostración. Como $[P],[Q] \in \mathcal{J}(\mathcal{C})[2]$, entonces son de la forma $[P] = [(\alpha_i,0)-(\alpha_j,0)]$ y $[Q] = [(\alpha_k,0)-(\alpha_l,0)]$, con $i \neq j$ y $k \neq l$. Por el lema 1.14.1 tenemos que $2[P] = div(a_P)$ y $2[Q] = div(a_Q)$, donde $a_P = (x-\alpha_i)/(x-\alpha_j)$ y $a_Q = (x-\alpha_k)/(x-\alpha_l)$, tenemos que por la observación 2.5.2:

$$e_2([P],[Q]) = \frac{a_P(Q)}{a_Q(P)} = \frac{(\alpha_k-\alpha_i)(\alpha_l-\alpha_j)(\alpha_i-\alpha_l)(\alpha_j-\alpha_k)}{(\alpha_k-\alpha_j)(\alpha_l-\alpha_i)(\alpha_i-\alpha_k)(\alpha_j-\alpha_l)}.$$

Siendo así, supongamos que G_P y G_Q son primos relativos entonces de lo anterior $e_2([P],[Q]) = 1$. Recíprocamente, si no lo son, entonces existen dos indices iguales, podemos tomar sin perdida de generalidad $l = j$, pero como $[P] \neq [Q]$, entonces $i \neq k$, luego de la expresión anterior $e_2([P],[Q]) = -1$ ■

Por el lema anterior, existe una relación entre los subconjuntos de $\mathcal{J}(\mathcal{C})[2]$ y los factores cuadráticos del polinomio f que define la curva de género 2, 1.1.1. Más específicamente, una relación entre $(2,2)$ subgrupos y conjuntos de 3 factores cuadráticos primos relativos dos a dos.

3.1. Descomposición cuadrática

Dada una ecuacion de la forma 1.1.1, queremos catalogar todas estas ternas de factores cuadráticos f para asociarlas con los $(2,2)$ subgrupos, el siguiente tratamiento es

estándar, pero es el que nos permitir definir mas adelante lo que llamaremos correspondencia de Richelot.

Consideremos el K-espacio vectorial $K[t]_2$ de los polinomios con coeficientes en K de grado a lo mas 2 dotado del corchete de Lie

$$[h,g] := \frac{dh}{dt}\cdot g - \frac{dg}{dt}\cdot h.$$

Observación 3.1.1 *Notemos que* $[h,g] = -[g,h]$ *y* $[\alpha p + \beta q, r] = \alpha[p,r] + \beta[q,r]$ *para todo* h,g,q,p,r *en* $K[t]_2$ *y* $\alpha,\beta \in K$.

Definición 3.1.1 *Definimos las siguientes funciones* $\Pi : K[x]_2^3 \to K[x]$ *y* $det : K[x]_2^3 \to K$ *definidas de la siguiente manera: Para* $G = (G_1, G_2, G_3)$ *elementos en* $K[t]_2$*, con* $G_i = g_{i,3}x^2 + g_{i,2}x + g_{i,1}$ *con* $i \in \{1,2,3\}$,

$$\prod(G) := G_1G_2G_3 \quad y \quad det(G) := \begin{vmatrix} g_{1,1} & g_{1,2} & g_{1,3} \\ g_{2,1} & g_{2,2} & g_{2,3} \\ g_{3,1} & g_{3,2} & g_{3,3} \end{vmatrix}.$$

La motivación de la definición anteriores por un lado, que si tomamos un f como en 1.1.1, entonces $\prod^{-1}(f)$ determina todas las ternas de factores cuadráticos. Más aún, si dicha terna es ordenada determinan puntos de Weierstrass y por tanto a saber $(2,2)$ subgrupos; por otro lado la función determinante así definida nos dará información sobre a que curvas variedad va a ser isogena, y como construir el polinomio que define la curva de llegada.

Definición 3.1.2 *Sea* $\mathcal{H}$ *el conjunto de todos los polinomios hiperelípticos de género 2 sobre* K*, en otras palabras,*

$$\mathcal{H} := \{f \in K[x] : deg(f) \in 5,6, f \text{ libre de cuadrados}\}.$$

Definimos el conjunto de descomposiciones cuadráticas por,

$$S := \left(\Pi^{-1}(\mathcal{H})\right) / \sim,$$

donde $\sim$ *define una relación de equivalencia dada por,*

$$(G_1,G_2,G_3) \sim (G_2,G_3,G_1) \sim (G_3,G_1,G_2)$$

si y solo si,

$$(G_1, G_2, G_3) \sim (\alpha G_1, \beta G_2, \gamma G_3).$$

Donde $\alpha, \beta, \gamma \in K^\times$*, tal que* $\alpha\beta\gamma = 1$*. Denotamos la imagen de un elemento* $G \in S$ *por* $[G]$*.*

Proposición 3.1.1 *Las funciones* $\Pi : K[x]_2^3 \to K[x]$ *y* $det : K[x]_2^3 \to K$ *se pueden extender naturalmente a*

$$\Pi : S \to H \quad y \quad det : S \to K$$

Demostración. Para Π es claro, pues si $[G] \in S$, entonces el representante es una permutación de los factores cuadráticos, o cada uno de los 3 factores tiene un coeficiente tal que al multiplicarlos es uno como en 3.1.2. Para det, basta notar que las clases anteriores se definieron para ser invariantes bajo la permutación (123). Dicho de otra forma, el determinante es invariante bajo cambios pares de filas, y si $G = (G_1, G_2, G_3) \sim (\alpha G_1, \beta G_2 \gamma G_3) = G'$, entonces

$$det(G') = \begin{vmatrix} \alpha g_{1,1} & \alpha g_{1,2} & \alpha g_{1,3} \\ \beta g_{2,1} & \beta g_{2,2} & \beta g_{2,3} \\ \gamma g_{3,1} & \gamma g_{3,2} & \gamma g_{3,3} \end{vmatrix} = \alpha\beta\gamma \begin{vmatrix} \alpha g_{1,1} & \alpha g_{1,2} & \alpha g_{1,3} \\ \beta g_{2,1} & \beta g_{2,2} & \beta g_{2,3} \\ \gamma g_{3,1} & \gamma g_{3,2} & \gamma g_{3,3} \end{vmatrix} = det(G).$$

■

Definición 3.1.3 *Para cada* $f \in \mathcal{H}$*, definimos las descomposiciones cuadráticas de* f *como*

$$S_f := \Pi^{-1}(f).$$

Además, definimos la involución $v : S \to S$*, dada por*

$$v([(G_1, G_2, G_3)]) := [(G_1, G_3, G_2)].$$

Observación 3.1.2 *Notemos que* $v : S \to S$ *ademas de estar bien definida agrupa aun mas los elementos de* S_f*. Dado que* v *es una involución (es decir,* $v \circ v = id$*), el subgrupo* $\langle v \rangle$ *tiene dos elementos:* $\langle v \rangle = \{id, v\}$*.*
El grupo $\langle v \rangle$ *actúa en* S_f *intercambiando las clases* $[G]$ *según la regla:* $v([G_1, G_2, G_3]) = [(G_1, G_3, G_2)]$ *esto genera pares de clases equivalentes bajo la acción de* v*. Por otro lado, si* $f \in \mathcal{H}$*, 3.1.2, notemos que* $v[G] \neq [G]$*, para ningún* f*, pues de serlo y dada la defi-*

nición de la relación de equivalencia 3.1.2, se concluye que $G_2 \equiv G_3$, pero f es libre de cuadrados.

- *Denotamos por $[S_f]$ al conjunto de las órbitas de S_f bajo la acción de v, o equivalentemente, el conjunto de clases del cociente $S_f/\langle v\rangle$.*
- *En términos prácticos, $[S_f]$ tiene la mitad del tamaño de S_f, porque cada órbita contiene exactamente dos elementos, $[G]$ y $v([G])$. Dicha órbita la llamaremos descomposición cuadrática sin signo y la denotaremos por $|G|$.*

Ejemplo 3.1.1 *Supongamos que S_f contiene las siguientes clases de equivalencia :*

$$S_f = \{[G_1, G_2, G_3], [G_1, G_3, G_2], [G_2, G_1, G_3], [G_3, G_1, G_2]\}.$$

- *La acción de v empareja $[G_1, G_2, G_3]$ con $[G_1, G_3, G_2]$, y $[G_2, G_1, G_3]$ con $[G_3, G_1, G_2]$.*
- *El cociente $[S_f]$ tiene entonces dos elementos:*

$$[S_f] = \{\{[G_1, G_2, G_3], [G_1, G_3, G_2]\}, \{[G_2, G_1, G_3], [G_3, G_1, G_2]\}\}.$$

Con las definiciones anteriores podemos establecer una correspondencia entre las descomposiciones cuadráticas sin signo de f y los $(2,2)$- subgrupos de $\mathcal{J}(\mathcal{C})[2]$; así mismo, las descomposiciones cuadráticas de f y las $(2,2)$- isogenias con dominio un jacobiano, $\mathcal{J}(\mathcal{C})$ a una variedad abeliana principalmente polarizada, VAPP, bien sea un producto de curvas elípticas o un jacobiano.

Proposición 3.1.2 *Sea $\mathcal{C} : y^2 = f(x)$ una curva de género 2. Los $(2,2)$- subgrupos de $\mathcal{J}(\mathcal{C})[2]$ están en biyección con las descomposiciones cuadráticas sin signo de f.*

Demostración. Como cada $(2,2)$ subgrupo R de $\mathcal{J}(\mathcal{C})[2]$ tiene tres elementos no nulos, por 2.5.1, 2.5.3, P_1, P_2 y P_3, sabemos que cada uno se corresponde a un factor cuadrático de f, digamos G_{P_i} con $i \in \{1,2,3\}$, que son únicos salvo multiplicación por escalar. Sabemos que R es maximal 2-isotrópico si y solo si $e_2(P_i, P_j) = 1$ con $i \neq j$, por 3.0.1, los polinomios G_{P_i} pueden ser tomados coprimos dos a dos. De lo anterior, $G_{P_1} G_{P_2} G_{P_3} = cf$ para algún $c \in K^\times$, sin perdida de generalidad, tomando $c = 1$, o bien dividiendo por $\mathcal{C}$ algún factor. Hemos entonces determinado las descomposiciones cuadráticas $[(G_{P_1}, G_{P_2}, G_{P_3})]$ y $[(G_{P_1}, G_{P_3}, G_{P_2})]$, este ultimo tomando su negativo, que es único, con ella la descomposición sin signo $|[(G_{P_1}, G_{P_2}, G_{P_3})]|$. ■

En pocas palabras el teorema anterior nos dice la buena selección de $(2,2)$ subgrupos o bien de kernels para isogenias para VAPP de forma mas explícita. Ahora cabe resaltar el teorema 2.5.1, puesto que queremos distinguir cuando una $\mathcal{J}(\mathcal{C})$ es isogena a un producto de curvas elípticas o a una $\mathcal{J}(\mathcal{C}')$ de una curva $\mathcal{C}'$ de género 2 . Veremos que esto se determina por el determinante de la descomposición seleccionada.

Definición 3.1.4 *Sea G una descomposición cuadrática de f que define a la curva de género 2 , 1.1.1. Si $det(G) = 0$, diremos que G es singular. De otro modo, G es no singular. Denotamos el conjunto de las descomposiciones no singulares por S^{ns} y dado $f \in \mathcal{H}$ denotamos el conjunto de descomposiciones no singulares de f por S^{ns}_f.*

El resultado respecto a las descomposiciones cuadráticas es que las descomposiciones no singulares determinan $(2,2)$-isogenias a jacobianos, y las descomposiciones singulares a productos de curvas elípticas. Centraremos nuestra atención en la parte no singular.

Primero notemos que dado una descomposición arbitraria G, (o bien $[G]$), se tiene que $det(v(G)) = -(det(G))$, es decir $det(G) \neq 0$ si y solo si $det(v(G)) \neq 0$. Mas aun, $\Pi(v(G)) = \Pi(G)$, entonces para cada $f \in \mathcal{H}$, S^{ns} es cerrado bajo negación.

Ejemplo 3.1.2 *Sea $K = \mathbb{F}_{11}$ y $\mathcal{C}$ la curva dada por*

$$\mathcal{C} : y^2 = f(x) = x(x^2-1)(x^2-4).$$

Entonces la descomposición $G = (x^2-1, x^2+3x+2, x-2)$ es no singular pues $det(G) = -1$.

Ejemplo 3.1.3 *Sea $K = \mathbb{F}_{83}$ y $\mathcal{C}$ la curva dada por*

$$\mathcal{C} : y^2 = f(x) = 24x^6 + 61x^5 + 48x^4 + 64x^3 + 14x^2 + 65x + 21.$$

Consideremos los siguientes polinomios cuadráticos,

$$\begin{aligned}
G_1 &= 24x^2 + 52x + 74,\\
G_2 &= x^2 + 6x + 5 = (x+1)(x+5),\\
G_2 &= x^2 + 23x + 22 = (x+1)(x+22),\\
G_2 &= x^2 + 46x + 45 = (x+1)(x+45),\\
G_2 &= x^2 + 27x + 27 = (x+5)(x+22),\\
G_2 &= x^2 + 50x + 59 = (x+5)(x+45),\\
G_2 &= x^2 + 67x + 77 = (x+22)(x+45).
\end{aligned}$$

Como G_1 es irreducible en $K[x]$, basta alternar los demás factores, así el conjunto de descomposiciones de f es

$$S_f = \left\{ \begin{matrix} [(G_1, G_2, G_7)], & [(G_1, G_7, G_2)], \\ [(G_1, G_3, G_6)], & [(G_1, G_6, G_3)], \\ [(G_1, G_4, G_5)], & [(G_1, G_5, G_4)] \end{matrix} \right\}.$$

Calculando los determinantes obtenemos que

$$\begin{aligned}
det([(G_1, G_2, G_7)]) &= 0, & det([(G_1, G_7, G_2)]) &= 0,\\
det([(G_1, G_3, G_6)]) &= 66, & det([(G_1, G_6, G_3)]) &= -66,\\
det([(G_1, G_4, G_5)]) &= 71, & det([(G_1, G_5, G_4)]) &= -71.
\end{aligned}$$

En consecuencia,

$S_f^{ns} = \{[(G_1, G_3, G_6)], [(G_1, G_6, G_3)], [(G_1, G_4, G_5)], [(G_1, G_5, G_4)]\}$.

3.2. Correspondencia de Richelot

La correspondencia de Richelot es una construcción que establece una relación entre curvas de género 2 y sus jacobianas mediante isogenias de grado 4. Dada una curva $\mathcal{C}$ de género 2, esta corresponde a una nueva curva $\mathcal{C}'$ junto con una isogenia de grado 4 entre las jacobianas $\mathcal{J}(\mathcal{C})$ y $\mathcal{J}(\mathcal{C}')$.

Esta isogenia se construye a partir de la descomposición de la ecuación de $\mathcal{C}$ en tres factores cuadráticos, lo que genera una relación entre las estructuras geométrica y

algebraica de $\mathcal{C}$ y $\mathcal{C}'$. En este capítulo se presentan algunos teoremas y resultados fundamentales que permiten obtener una intuición sobre la correspondencia de Richelot. Aunque el tratamiento detallado de esta corresponde a una tesis doctoral en la que se basa esta parte del trabajo, se incluyen las nociones esenciales que subyacen en su construcción. Para una discusión más completa, ver [45, Ch. 8.].

Teorema 3.2.1 *[45, Prop. 8.3.1] Sea $\mathcal{C}$ una curva de género 2. Si existe una descomposición cuadrática singular G de f, entonces $\mathcal{J}(\mathcal{C})$ es $(2,2)$-isogena a un producto de curvas elípticas.*

Definición 3.2.1 *Definimos el operador de Richelot, $\mathcal{R}$ como*

$$\mathcal{R} : \{G \in K[x]_2^3 : det(G) \neq 0\} \to K[x]_2^3,$$

donde

$$\mathcal{R}((G_1, G_2, G_3)) := (\delta[G_2, G_3], \delta[G_3, G_1], \delta[G_1, G_2]),$$

donde $\delta = (det(G_1, G_2, G_3))^{-1}$.

Lema 3.2.1 *[45, Lemma 8.4.3] Sean G_1, G_2 y G_3 polinomios en $K[x]_2$, tales que $det(G1, G_2, G_3) \neq 0$ y $\Pi(G_1, G_2, G_3)$ un polinomio de grado 5 (respectivamente 6). Entonces $\Pi(\mathcal{R}((G_1, G_2, G_3)))$ es un polinomio libre de cuadrados cuyo grado es 5 (respectivamente 6).*

El lema anterior establece que, dada una descomposición de un polinomio f que define una curva de género 2, la asignación de Richelot está bien definida en el sentido de que asocia a $f = G_1G_2G_3$ otro polinomio, $h = \Pi(\mathcal{R}(G_1, G_2, G_3))$ que también define una curva de género 2. Más precisamente, el polinomio obtenido, h a través de la asignación efectivamente define una curva de género 2.

Esta ultima afirmación se justifica a partir de la Observación 1.1.2, ya que es suficiente comprobar que el polinomio resultante h no tenga raíces múltiples, es decir, que sea libre de cuadrados.

El siguiente teorema combina los resultados establecidos en la Proposición 8.4.11 [45] y los conceptos desarrollados previamente en la Sección 8.3 [45].

Definición 3.2.2 *Sea $\mathcal{C} : y^2 = f(x)$ una curva de género 2, de tal manera que $f(x) = a_f \prod_{i=1}^{d}(x - r_i)$, $d \in \{5,6\}$ y $\mathcal{J}(\mathcal{C})$ su jacobiano. Dado un grupo $H \subseteq \mathcal{J}(\mathcal{C})[2]$ maximal*

2-isotrópico, entonces existe un morfismo

$$\phi : \mathcal{J}(\mathcal{C}) \to A \quad con \quad ker(\phi) = H.$$

La función ϕ es una $(2,2)$*- isogenia y A una variedad abeliana principalmente polarizada, es bien un jacobiano o un producto de dos curvas elípticas.*

Teorema 3.2.2 *Sea $\mathcal{C}$ una curva de género 2, 1.1.1 y $G = (G_1, G_2, G_3)$ una descomposición cuadrática de f dada por $G_i = g_{i,3}x^2 + g_{i,2}x + g_{i,1}$ con $i \in \{1,2,3\}$. Sea H un* $(2,2)$ *subgrupo de $\mathcal{J}(\mathcal{C})$, dado por $H = \langle \mathcal{J}(G_1, 0), \mathcal{J}(G_2, 0)\rangle$, como en 1.10.2. Sea $\phi : \mathcal{J}(\mathcal{C}) \to A$ una isogenia con kernel H y*

$$\delta = det(G) := \begin{vmatrix} g_{1,1} & g_{1,2} & g_{1,3} \\ g_{2,1} & g_{2,2} & g_{2,3} \\ g_{3,1} & g_{3,2} & g_{3,3} \end{vmatrix}.$$

1. *Si $\delta \neq 0$, entonces A es isomorfa al jacobiano de la curva C' de género 2 dada por:*

$$C' : y^2 = H_1 H_2 H_3,$$

donde

$$H_1 = \delta^{-1}[G_2, G_3], \quad H_2 := \delta^{-1}[G_3, G_1], \quad H_3 := \delta^{-1}[G_1, G_2].$$

2. *Si $\delta = 0$, entonces A es isomorfa a $E_1 \times E_2$, con E_1 y E_2 curvas elípticas dadas por*

$$E_1 : y^2 = \prod_{i=1}^{3}(a_{i,1}x + a_{i,2}), \quad E_2 : y^2 = \prod_{i=1}^{3}(a_{i,1} + a_{1,2}x),$$

donde $a_{i,0}, a_{i,1}$ son tales que $G_i = a_{i,1}(x - s_1)^2 + a_{i,2}(x - s_2)^2$ para algunos $s_1, s_2 \in K$.

Demostración. Ver [45, Thm. 8.4.1] para parte 1 y la sección 8.3 de [45] para parte 2. ■

Observación 3.2.1 *En el estudio de isogenias de Richelot en género* 2*, el signo del determinante asociado a la descomposición de la jacobiana puede interpretarse en términos de* twists cuadráticos*. Sin entrar en detalles, mencionamos que estos twists permiten distinguir entre jacobianas que no son isomorfas sobre el cuerpo base, pero que sí se vuelven isomorfas al pasar a una extensión cuadrática.*

Por ejemplo, consideremos el cuerpo finito $\mathbb{F}_5$ *y las curvas hiperelípticas de género* 2*:*

$$\mathcal{C} : y^2 = x^5 + 2x + 1 \quad y \quad \mathcal{C}' : y^2 = 2(x^5 + 2x + 1),$$

donde 2 *es un no cuadrado en* $\mathbb{F}_5$*. Las jacobianas* $\mathcal{J}(\mathcal{C})$ *y* $\mathcal{J}(\mathcal{C}')$ *no son isomorfas sobre* $\mathbb{F}_5$ *porque no existe un isomorfismo que relacione ambas ecuaciones en este cuerpo.*

Sin embargo, al pasar a la extensión cuadrática $\mathbb{F}_{25}$*, donde* 2 *admite una raíz cuadrada que denotamos por* $\sqrt{2}$*, las curvas* $\mathcal{C}$ *y* $\mathcal{C}'$ *se vuelven isomorfas. El cambio de variables explícito dado por:*$x' = x, y' = \frac{y}{\sqrt{2}}$*, así tenemos* $\mathcal{C}' : (y')^2 = (x')^5 + 2(x') + 1$ *Esto implica que las jacobianas de* $\mathcal{C}$ *y* $\mathcal{C}'$ *son isomorfas sobre* $\mathbb{F}_{25}$*. Este fenómeno refleja cómo los twists cuadráticos afectan la estructura de las jacobianas al considerar extensiones del cuerpo base. Para un tratamiento más profundo, se recomienda consultar la teoría de twists cuadráticos en el contexto de curvas elípticas y de género* 2*, [20].*

Proposición 3.2.1 *Sean* $\mathcal{C}$ *y* $\mathcal{C}'$ *como en 3.2.2 parte* 1.)*. Entonces la* $(2,2)$*-isogenia* $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ *considerada en 3.2.2, queda determinada por la correspondencia* $\mathrm{R} \subseteq \mathcal{C} \times \mathcal{C}'$ *con*

$$R := \left\{ \begin{array}{c} 0 = G_1(u)H_1(u') + G_2(u)H_2(u') \\ v v' = G_1(u)H_1(u')(u - u') \end{array} \right\}.$$

Para puntos $(P, P') = ((u, v), (u', v')) \in \mathcal{C} \times \mathcal{C}'$*.*

Demostración. [45, Thm. 8.4.11]. ■

Observación 3.2.2 *La correspondencia anterior 3.4.3, es llamada correspondencia de Richelot. Notemos que dado un punto* $P = (u, v) \in \mathcal{C}$*, la primera ecuación de 3.4.3 tiene dos soluciones para* u'*, puesto que es de grado 2 en* u'*, y por otro lado para* v' *existe una única solución fijada una de las anteriores para* u'*.*

Ejemplo 3.2.1 *Consideremos la curva* $\mathcal{C} : y^2 = x(x^2 - 1)(x^2 - 4)$*. Por 3.0.1,* $H = \langle \mathcal{J}(x^2 - x, 0), \mathcal{J}(x^2 + 3x + 2, 0) \rangle$ *es un* $(2,2)$ *subgrupo maximal isotrópico, obtenemos entonces la correspondencia*

$$R : \left\{ \begin{array}{c} 0 = 4uu' - u^2 - 5uu' + 2u'^2 - 2u + 3u' + 4 \\ v v' = (u^2 - u)(-u^2 + 4u' - 3)(u - u') \end{array} \right\}.$$

Calculemos la imagen del elemento, $M = \mathcal{J}(x^2 - x - 1, 2x - 4)$ *en su representación de Mumford 1.10.2, 1.10.2 . Buscamos* $x^2 - x - 1 \equiv mod 11$*, luego* $x = 4$ *y* $x = 8$*, así* $M = [(4,4) + (8,1) - 2\infty]$*. Fijando* $P = (4,4)$ *y* $Q = (8,1)$*, obtenemos que*

$$R_P : \left\{ \begin{array}{c} 0 = -4(u'^2 - 4u' + 5) = -4(u' - 2 - i)(u' - 2 + i) \\ 4v' = -2u' - 3 \end{array} \right\}.$$

Encontramos dos puntos sobre la curva $\mathcal{C}$*,* $P_1 = (2+i, 1-5i)$*,* $P_2 = (2-i, 1+5i)$*, de forma análoga para Q, se sigue que* $Q_1 = (-3, 0)$*,* $Q_2 = (-4, -2)$*. Por, 3.4.3, tenemos que,* $\phi(M) = [P_1 + P_2 + Q_1 + Q_2 - 4\infty] \in \mathcal{J}(\mathcal{C}')$*. Y aplicando al algoritmo de Cantor 1.11.1, obtenemos el elemento de la forma* $[P' + Q' - 2\infty]$*.*

3.3. Calculo eficiente de Isogenias

Nos centraremos en los resultados teóricos que permiten una implementación eficiente del cálculo de isogenias $(2,2)$, considerando ciertas condiciones sobre los coeficientes del polinomio que define la curva de género 2. Para ello, analizaremos en detalle dos tipos específicos de polinomios, cuya definición se presenta a continuación, y revisaremos los resultados que se derivan de ellos, ver [26, Ch. 4.].

Definición 3.3.1 *Sea* $\mathcal{C} : y^2 = f(x)$ *una curva hiperelíptica de género 2 definida sobre* K*. Decimos que la ecuación hiperelíptica 1.1.1 es de* ***tipo 1*** *si* f *es de la forma*

$$f(x) = Ex(x^2 - Ax + 1)(x^2 - Bx + C),$$

y de ***tipo 2*** *si es de la forma*

$$f(x) = (x^2 - 1)(x^2 - A)(Ex^2 - Bx + C),$$

para algunos $A, B, C, E \in K$*.*

La equivalencia entre una ecuación de tipo 1 y una de tipo 2 puede establecerse mediante el siguiente cambio de variables aplicado a la ecuación de tipo 1:

$$(x', y') = \left(\frac{x-1}{x+1}, \frac{y}{(x+1)^3} \right).$$

Observación 3.3.1 *El uso de las ecuaciones hiperelípticas anteriores combinadas con la correspondencia de Richelot da formulas más explícitas para calcular la imagen de algunos elementos. Más aún, el siguiente teorema nos dice cuando una ecuación hiperelíptica es de tipo 1 o 2.*

Proposición 3.3.1 *Sea $\mathcal{C} : y^2 = f(x)$ una curva de género 2. Supongamos que todos los puntos de Weierstrass son $K-$ racionales. Entonces existe una ecuación hiperelíptica de tipo 1 o 2 para $\mathcal{C}$.*

Demostración. Ver [26, Prop. 2.3] ■

3.4. Isogenias de Richelot para ecuaciones de tipo 1

Consideraremos ciertos resultados sobre isogenias de Richelot aplicados a ecuaciones de tipo uno, los cuales serán fundamentales para el desarrollo de un algoritmo que permitirá construir cadenas de isogenias de Richelot en secciones posteriores.

Sea ϕ una $(2,2)$ isogenia. La siguiente proposición muestra que podemos realizar un cambio de coordenadas con el mismo cuerpo base K si existe un punto K-racional J de orden 4 tal que $2 \cdot J \in ker(\phi)$.

Proposición 3.4.1 *[26, Prop. 4.1] Sean $g_1, g_2, g_3 \in K[x]$ una descomposición cuadrática de $f(x)$, $\mathcal{C} : y^2 = f(x) = g_1(x)g_2(x)g_3(x)$ una curva de género 2 y $H = \langle \mathcal{J}(g_1, 0), \mathcal{J}(g_2, 0)\rangle$ un $(2,2)$ subgrupo de $\mathcal{J}(\mathcal{C})$. Si las raíces de g_1 son $K-$racionales y existe un elemento $J_4 \in \mathcal{J}(\mathcal{C})$ un punto de $4-$torsión K racional tal que $2 \cdot J_4 = \mathcal{J}(g_1(x), 0)$, entonces existe un cambio de coordenadas racional $t : (x, y) \mapsto (x', y')$ tal que*

$$C : (y')^2 = Ex'(x'^2 - Ax' + 1)(x'^2 - B'x + C),$$

es una ecuación de tipo 1 y $H = \langle \mathcal{J}(x', 0), \mathcal{J}((x')^2 - Ax' + 1, 0)\rangle$.

Las siguientes dos proposiciones son simplemente re-escrituras del teorema 3.2.2 y 3.4.3.

Proposición 3.4.2 *Sea $\mathcal{C} : y^2 = Ex(x^2 - Ax + 1)(x^2 - Bx + C)$ una curva de género 2 definida por una ecuación de tipo 1 y sea $\phi : \mathcal{J}(\mathcal{C}) \to A$ una isogenia con kernel dado por $ker(\phi) = \langle \mathcal{J}(x, 0), \mathcal{J}(x^2 - Ax + 1, 0)\rangle \subseteq \mathcal{J}(\mathcal{C})[2]$.*

1. *Si $C \neq 1$, entonces A es isomorfa al jacobiano de la curva de género 2, $\mathcal{C}'$, dada por una ecuación de tipo 2:*

$$\mathcal{C}' : y^2 = (x^2-1)(x^2-A')(E'x^2 - B'x + C'),$$

donde

$$A' = C, \quad B' = \frac{2}{E}, \quad C' = \frac{B-AC}{E(1-c)}, \quad E' = \frac{A-B}{E(1-C)}.$$

2. *Si $C = 1$, entonces A es isomorfa a $E_1 \times E_2$ dadas por*

$$E_1 : y^2 = c_1(x-1)\left(x - \frac{A+2}{A-2}\right)\left(x - \frac{B+2}{B-2}\right), \quad E_2 : y^2 = c_2(x-1)\left(x - \frac{A-2}{A+2}\right)\left(x - \frac{B-2}{B+2}\right),$$

donde

$$c_1 = E(A-2)(B-2) \quad y \quad c_2 = -E(A+2)(B+2).$$

Proposición 3.4.3 *Sean $\mathcal{C}$ y $\mathcal{C}'$ como en 3.4.2 parte* 1.)*, en particular $C \neq 1$. Entonces la $(2,2)$ isogenia $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ definida en 3.2.2. se define por la correspondencia $R \subseteq \mathcal{C} \times \mathcal{C}'$ con*

$$R := \left\{ \begin{array}{ll} 0 & = (u^2 - Bu + 1)\cdot u'^2 + 2(C-1)u\cdot u' - Cu^2 + Bu - C \\ vv' & = (A-B)u\cdot u'^3 - ((A-B)u^2 + 2(1-C)u)\cdot u'^2 \\ & \quad + (2(1-C)u^2 - (AC-B)u)\cdot u' + (AC-B)u^2)) \end{array} \right\}.$$

Para puntos $(P,P') = ((u,v),(u',v')) \in \mathcal{C} \times \mathcal{C}'$.

El siguiente teorema nos da una formula explicita para la imagen de un elemento general $\mathcal{J}(x^2 + a_1x + a_0, b_1x + b_0) \in \mathcal{J}(\mathcal{C})$, bajo una isogenia ϕ.

Teorema 3.4.1 *[26, Thm. 4.7.] Sea $\mathcal{C} : y^2 = Ex(x^2 - Ax + 1)(x^2 - Bx + C)$ una curva de género 2 definida por una ecuación de tipo 1 y supongamos que $C \neq 1$. Además sea ϕ : $\mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ la isogenia tal que $ker(\phi) = \langle \mathcal{J}(x,0), \mathcal{J}(x^2 - Ax + 1, 0)\rangle \subseteq \mathcal{J}(\mathcal{C})[2]$ de la proposición 3.4.2. Supongamos ademas que $\mathcal{J}(a,b) = \mathcal{J}(x^2 + a_1x + a_0, b_1x + b_0) \in \mathcal{J}(\mathcal{C})$ satisface que*

$$\begin{aligned} 0 &\neq -b_1(a_1b_0 - a_0b_1) + b_0^2, \\ 0 &\neq a_0B^2 + (a_0+1)a_1B + (a_0-1)^2 + a_1^2, \\ 0 &\neq (a_0-1)(a_1^2 - 4a_0). \end{aligned}$$

Entonces

$$\phi(\mathcal{J}(a,b)) = \left[D\left(\frac{a'_4 x^4 + a'_3 x^3 + a'_2 x^2 + a'_1 + a'_0}{a'_4}, \frac{b'_3 x^3 + b'_2 x^2 + b'_1 x + b'_0}{b'_{den}} \right) - 2D'_\infty \right] \in \mathcal{J}(\mathcal{C}'),$$

donde

$$\begin{aligned}
a'_0 &= ((a_0-1)^2 + a_1^2)C^2 + (a_0+1)a_1BC + a_0B^2,\\
a'_1 &= 2\cdot(C-1)\cdot((a_0+1)a_1C + 2a_0B),\\
a'_2 &= -(a_0+1)a_1B(C+1) - 2a_0B^2 + 4a_0C^2 - 2((a_0+1)^2 + a_1^2)C + 4a_0,\\
a'_3 &= -2\cdot(C-1)\cdot(a_0B + (a_0+1)a_1),\\
a'_4 &= a_0B^2 + (a_0+1)a_1B + (a_0-1)^2 + a_1^2,\\
\eta &= a_1b_0 - a_0b_1,\\
b'_0 &= a_0\eta AB + (a_0b_0(a_0-1) + a_1\eta)AC + a_0(a_1\eta - b_0(a_0-1))B + \eta((a_0-1)^2 + a_1^2)C,\\
b'_1 &= a_0b_0AB + (a_0a_1b_0 + \eta(a_0+1))AC - 2a_0\eta A + a_0(\eta + b_1)B +\\
&\quad (2a_0a_1\eta + b_0(-a_0^2 + a_1^2 + 1))C - 2a_0a_1\eta + 2a_0b_0(a_0+1),\\
b'_2 &= -a_0\eta AB + 2a_0b_0AC + (-a_0b_0(a_0+1) - a_1\eta)A + a_0(-a_1\eta + b_0(a_1-1))B\\
&\quad + 2a_0(\eta + b_1)C - (a_0^2 + a_1^2 + 1)\eta,\\
b'_3 &= -a_0b_0AB + (-a_0^2b_1\eta)A - a_0(\eta + b_1)B - b_0((a_0-1)^2 + a_1^2),\\
b'_{den} &= (a_0-1)\cdot(-\eta b_1 + b_0^2).
\end{aligned}$$

La demostración involucra varios cálculos simbólicos que fueron realizados utilizando el Sistema de Álgebra Computacional SAGE y su implementación puede encontrarse en [25].

El teorema anterior permite una mejora significativa en la velocidad del cálculo de la isogenia, ya que evita tanto los cálculos de raíces cuadradas como la necesidad de computar una extensión de cuerpo.

3.5. Superficie de Kummer

En esta sección estudiaremos cómo las superficies de Kummer $\mathcal{K}_A = A/\langle -1\rangle$ (para A una variedad abeliana de dimensión 2) inducen estructuras relacionadas con isogenias. Nos centraremos en el caso donde $A = \mathcal{J}(\mathcal{C})$ para una curva $\mathcal{C} : y^2 = f(x)$ de gé-

nero 2, mostrando como una isogenia $\phi : A \to A'$ induce un morfismo $\phi_{\mathcal{K}} : \mathcal{K}_A \to \mathcal{K}_{A'}$, y la construcción de una matriz asociada a la acción sobre los coeficientes de $f(x)$.

Definición 3.5.1 *Para una curva $\mathcal{C} : y^2 = f(x)$ de género 2, la superficie de Kummer se define por, $\mathcal{K} = \mathcal{J}(\mathcal{C})/\langle \pm 1 \rangle = V(F) \subseteq \mathbb{P}$, la cual es una superficie cuadrática en $\mathbb{P}^3$. Esta admite un modelo de la forma:*

$$\mathcal{K} : (x_1^2 - 4x_0x_2)x_3^2 - 2F_1(x_0, x_1, x_2)x_3 + F_0(x_0x_1, x_2) = 0,$$

donde F_0, F_1 son polinomios explícitos conocidos [5, Ch. 3., pp. 17.].

Observación 3.5.1 *Sea entonces $\pi : \mathcal{J}(\mathcal{C}) \to \mathcal{K}$ la proyección. Una superficie de Kummer no es una variedad abeliana, pero tenemos la siguientes características:*

- ***Seudo-adición:*** *Sean $P, Q, P - Q \in \mathcal{J}(\mathcal{C})$, dados $\pi(P), \pi(Q), \pi(P - Q)$, obtenemos $\pi(P + Q)$.*
- ***Itweraciones:*** *Dado $n \in \mathbb{N}$, podemos calcular $\pi(n \cdot P) = n\pi(P)$.*
- ***Isogenias:*** *La isogenia $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ induce una función racional $\phi_{\mathcal{K}} : \mathcal{K} \to \mathcal{K}'$ entre superficies de Kummer. Por abuso de notación, llamaremos $\phi_{\mathcal{K}}$ una isogenia.*

$$\begin{array}{ccc} \mathcal{J}(\mathcal{C}) & \xrightarrow{\phi} & \mathcal{J}(\mathcal{C}') \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ \mathcal{K} & \xrightarrow{\phi_{\mathcal{K}}} & \mathcal{K}' \end{array}$$

Observación 3.5.2 *Para ciertos casos relacionados con la criptografía, es importante notar que dado que en la superficie de Kummer tenemos la seudo-adición, es muy útil dado que para una iteración de un punto $P \in \mathcal{J}(\mathcal{C})$, como en algoritmos de tipo Diffie-Hellman.*

Sea $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ una isogenia de Richelot, entonces existe una matriz $M = (a_{i,})_{ij}$ tal que

$$\phi_{\mathcal{K}} : \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \mapsto \begin{bmatrix} a_{0,0} & \cdots & a_{0,9} \\ \vdots & & \vdots \\ a_{3,0} & \cdots & a_{3,9} \end{bmatrix} \cdot \begin{bmatrix} x_0^2 \\ x_0x_1 \\ \vdots \\ x_3^3 \end{bmatrix}.$$

En el calculo de M existen 9 entradas nulas y 31 entradas con formulas explicitas, por ejemplo:

$$\begin{aligned} a_{0,4} = {} & g_{02}^2 g_{11} g_{12} g_{21}^2 - g_{01} g_{02} g_{12}^2 g_{21}^2 - g_{02}^2 g_{11} g_{12} g_{20} g_{22} + g_{01} g_{02} g_{12}^2 g_{20} g_{22} - \\ & g_{02}^2 g_{11}^2 g_{21} g_{22} + g_{02}^2 g_{10} g_{12} g_{21} g_{22} + g_{01}^2 g_{12}^2 g_{21} g_{22} + g_{00} g_{02} g_{12}^2 g_{21} g_{22} + \\ & g_{01} g_{02} g_{11}^2 g_{22}^2 - g_{01} g_{02} g_{10} g_{12} g_{22}^2 - g_{01}^2 g_{11} g_{12} g_{22}^2 - g_{00} g_{02} g_{11} g_{12} g_{22}^2. \end{aligned}$$

Para un estudio más detallado sobre el tema, el lector puede remitirse a [42, Ch. 2.] y [37] .

Ejemplo 3.5.1 *Sea* $\mathcal{C} : y^2 = (x^2-1)(x^2-A)(Ex^2 - Bx + C)$ *con* $B \neq 0$ *y* $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ *una* $(2,2)$ *isogenia como antes, entonces tenemos:*

$$M = \begin{pmatrix} AE-AC-C & 0 & 0 & 1 & c & -B & 0 & E & 0 & 0 \\ AB & -2(AC+AE+C) & AB+B & 0 & 2\frac{(AE+C)(C+E)}{B} & -2(AE+C+E) & 1 & B & 0 & 0 \\ AC & -AB & 0 & 0 & AE & 0 & 0 & -AE+C-E & 1 & 0 \\ A(A(4E^2-B^2)-B^2) & 0 & -4A(B^2+2CE) & 4AE & AB^2 & 0 & 0 & -B^2(A+1)+4C^2 & 4C & 1 \end{pmatrix}.$$

En la cual hay 16 entradas nulas, 4 entradas 1, y formulas simples, lo cual puede ser mas eficiente que operar con la representación de Mumford [27].

3.6. Métodos para evaluar Isogenias de Richelot.

En esta sección, se presentarán algunos comentarios sobre los métodos actuales utilizados para evaluar isogenias de Richelot. Estas (2,2)-isogenias, juegan un papel crucial en diversos contextos matemáticos y criptográficos, particularmente en el estudio de variedades abelianas de género 2 y sus curvas jacobianas asociadas. Analizaremos las técnicas más relevantes desde una perspectiva teórica y práctica, destacando sus fortalezas, limitaciones y posibles extensiones, con el objetivo de proporcionar una visión clara del estado actual de esta área de investigación.

El propósito es que dado un elemento $\mathcal{J}(a,b) \in \mathcal{J}_K(\mathcal{C})$ y una isogenia $\phi : \mathcal{J}_K(\mathcal{C}) \to \mathcal{J}_K(\mathcal{C}')$ queremos calcular la imagen de dicho elemento bajo isogenia es decir $\phi(\mathcal{J}(a,b)) \in \mathcal{J}_K(C')$.

1. **Algoritmo estándar**: 3.4.3, 3.2.1
    - Requiere factorización del polinomio a.
    - Los divisores $[P_1 + P_2 - 2\infty]$ y $[Q_1 + Q_2 - 2\infty]$ son posiblemente no $K-$ racionales.

2. **Base de Gröbner** (Castryck-Decru) [6]
   Se calcula el ideal

$$I = \langle a, y-b, y^2 - f(x), G_1(x)H_1(x') + G_2(x)H_2(x'), \\ yy' - G_1(x)H_1(x')(x-x')\rangle \subseteq K[x,y,x',y']$$

   Luego se calcula el ideal de eliminación M, respecto de x e y, es decir,

$$M = I \cap K[x', y'].$$

   En el caso general, $M = \langle a_{new}(x'), y' - b_{new}(x')\rangle$, donde $deg(a_{new}) = 4$ y $deg(b_{neq}) = 3$. El par (a_{neq}, b_{new}) es la representación de Mumford, sin reducir de $[P_1 + P_2 + Q_1 + Q_2 - 4\infty]$.

   - No se necesita factorización ni extensiones de cuerpos.
   - El calculo con bases de Gröbner es corto, y se puede hacer de forma explicita, ver [38].

3. **Formulas explicitas:**
   La idea general, es realizar calculo simbólico con coeficientes en $\mathbb{Z}[g_{00}, \ldots, g_{23}, a_1, a_0, b_1, b_0]$. Es decir, las formulas para los coeficientes de los polinomios son de la forma

$$a_{new} = x^4 + a'_3x^3 + a'_2x^2 + a'_1x + a'_0, \quad b_{new} = b'_3x^3 + b'_2x^2 + b'_1x$$

   donde $a'_i, b'_i \in \mathbb{Z}[g_{00}, \ldots, g_{23}, a_1, a_0, b_1, b_0]$.

   - El problema con este método es su poca eficiencia, por ejemplo respecto a las bases de Gröbner, reflejado en la cantidad de formulas y operaciones involucradas.

     Solución: para ello se consideran las formulas de tipo 1, 3.3.1, de forma similar a la forma de Montgomery para curvas elípticas.
   - De esta forma hay un formulario mas compacto y se evita factorización y uso de extensiones de cuerpo.

4. **Superficie de Kummer** Como variedad $\mathcal{J}_K(\mathcal{C})$ puede ser escrita como el conjunto de ceros de 72 ecuaciones en $\mathbb{P}^{15}(K)$, ver [5]. Se define la superficie de Kummer

por $\mathcal{K} = \mathcal{J}(\mathcal{C})/\langle \pm 1 \rangle$.

3.7. Isogenias $(2^n, 2^n)$

Estudiaremos brevemente las isogenias de tipo $(2^n, 2^n)$ y se presentara el algoritmo propuesto en [26] para calcular una isogenia de tipo $(2^n, 2^n)$, como secuencia de isogenias de tipo $(2,2)$.

Sea A una VAPP y $n \in \mathbb{N}$, recordemos el 2^n-emparejamiento de Weil, 2.5.2, es decir $e_{2^n} : A[2^n] \times A[2^n] \to \mu_{2^n}$ forma bilineal alternante. Para todo $n \in \mathbb{N}$, el 2^n grupo de torsión $A[2^n]$ es un $\mathbb{Z}_{2^n}$ modulo de rango 4; más específicamente, recordemos el que por el teorema 1.13.1, para una curva de genero 2, 1.1.1, su m-torsión es tal que

$$\mathcal{J}(\mathcal{C})[m] \cong (\mathbb{Z}/m\mathbb{Z})^4,$$

es decir $\mathcal{J}(\mathcal{C})[m]$ es un grupo finitamente generado de rango 4. Definiremos a continuación un tipo especial de base, la cual nos servirá para obtener subgrupos, que llamaremos más adelante, subgrupos maximales $(2,2)$-isotrópicos; los cuales se definen a partir de subgrupos maximales $(2^n, 2^n)$ isotrópicos.

Definición 3.7.1 *Decimos que una tupa (P_1, P_2, Q_1, Q_2) es una base para $\mathcal{J}(\mathcal{C})[m]$ si genera a $\mathcal{J}(\mathcal{C})[m]$ como grupo. Decimos que la base (P_1, P_2, Q_1, Q_2) para $\mathcal{J}(\mathcal{C})[m]$ es simpléctica respecto al m-emparejamiento de Weil si*

$$e_m(P_i, Q_j) = \mu^{\delta_{ij}}, \quad e_m(P_1, P_2) = e_m(Q_1, Q_2) = \mu^0 = 1,$$

donde μ es una $m-$esima raíz de la unidad y $\delta_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{en otro caso.} \end{cases}$

Observación 3.7.1 *La definición anterior se puede reescribir para el caso $(2,2)$ como: Sea $\mathcal{J}(\mathcal{C})[2]$ el subgrupo de 2-torsión del jacobiano de una curva de género 2 y sea $e_2 : \mathcal{J}(\mathcal{C})[2] \times \mathcal{J}(\mathcal{C})[2] \to \mu_2$ el emparejamiento de Weil de 2-torsión. Decimos que un conjunto de elementos $\mathcal{B} = \{J_1, J_2, J_3, J_4\}$ en $\mathcal{J}(\mathcal{C})[2]$ es una **base simpléctica** si cumple las siguientes condiciones:*

1. *$\mathcal{B}$ es una base de $\mathcal{J}(\mathcal{C})[2]$ como grupo abeliano.*

2. *La matriz del* 2*-emparejamiento de Weil en esta base, dada por*

$$M = (e_2(J_i, J_j))_{1 \le i,j \le 4},$$

satisface que al aplicar el logaritmo en base μ *(una raíz cuadrada primitiva de la unidad, es decir,* $\mu = -1$*), obtenemos la matriz*

$$\log_\mu(M) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

3. *Esta matriz es equivalente a la forma canónica simpléctica:*

$$\Omega = \begin{bmatrix} 0 & I_2 \\ -I_2 & 0 \end{bmatrix},$$

donde I_2 *es la matriz identidad de tamaño* 2×2.

Las bases simpléctica permiten entender, o definir según se vea, los $(2^n, 2^n)$ subgrupos. Dado un conjunto generador, al aplicar el algoritmo 1 del apéndice B en [28], similar al algoritmo de Gram-Schmidt, se obtiene una base simpléctica. Más aún, una propiedad importante de las bases simplécticas es que es que son preservadas bajo isogenias, lo cual es muy útil en G2SIDH, ver [28].

Sabemos por 2.5.1, que los $(2^n, 2^n)$ subgrupos de $\mathcal{J}(\mathcal{C})[2^n]$ son de la forma

$$\mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} \quad o \quad \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^{n-k}} \times \mathbb{Z}_{2^k},$$

donde $1 \le k \le \lfloor n/2 \rfloor$.

Nos interesa el caso especifico de los subgrupos de rango 2, o bien $k = 0$.

Definición 3.7.2 *Sean* A *y* A' *VAPP, decimos que una isogenia* $\phi : A \to A'$ *es una* $(2^n, 2^n)$ *isogenia si* $H = ker(\phi) \cong \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} \cong \langle H_1, H_2 \rangle$ *y llamaremos a* H *un* $(2^n, 2^n)$ *subgrupo.*

3.8. Subgrupos $(2^n, 2^n)$ y ecuaciones de tipo 2

Dado que el estudio exhaustivo de los grupos del tipo $(2^n, 2^n)$ escapa al alcance de esta sección, remitimos al lector a [28], donde se desarrollan con mayor profundidad sus propiedades algebraicas y estructurales, junto con resultados adicionales de interés.

Observación 3.8.1 *Sea A una VAPP y (J_1, J_2, J_3, J_4) una base simpléctica de $A[2^n]$ y consideremos, como se sugiere en [28, Ch. 2], la siguiente colección $(2^n, 2^n)$ subgrupos*

$$\mathcal{G} := \left\{ \langle J_1 + aJ_3 + bJ_4, J_2 + bJ_3 + cJ_4 \rangle | a, b, c \in \mathbb{Z}_{2^n} \right\}.$$

Para cada elección $(a, b, c) \in \mathbb{Z}_{2^n}^3$ define un $(2^n, 2^n)$ subgrupo diferente, siendo así, podemos considerar alguna elección especifica, ademas de ahora en adelante tendremos en cuenta las curvas de género 2, $\mathcal{C}$, de tipo 2

$$\mathcal{C} : y^2 = (x^2 - 1)(x^2 - A)(Ex^2 - Bx + C),$$

para $A, B, C, E \in K$ y la variedad abeliana $\mathcal{J}(\mathcal{C})$. Denotemos ademas los puntos de Weierstrass por

$$\left\{ (1,0), (-1,0), (\alpha,0), (-\alpha,0), (\beta,0), (\gamma,0) \right\},$$

donde α es una raíz cuadrada de A y β, γ son raíces de $Ex^2 - Bx + C$. Si $E = 0$, asignamos $\gamma = \infty$ y en este caso el polinomio $x - \gamma$ es constante.

Lema 3.8.1 *Sea $\mathcal{C}$ una curva de género 2 definida por una ecuación hiperelíptica del tipo 2, 3.3.1. Entonces $\mathcal{B} = (J_1, J_2, J_3, J_4)$ con*

$$J_1 = \mathcal{J}((x-1)(x-\alpha), 0), \quad J_3 = \mathcal{J}((x-1)(x+1), 0),$$
$$J_2 = \mathcal{J}((x+\alpha)(x-\beta), 0), \quad J_4 = \mathcal{J}((x-\beta)(x-\gamma), 0),$$

es una base simpléctica para $\mathcal{J}(\mathcal{C})[2]$, donde α, β y γ se definieron anteriormente.

Demostración.

1. **Independencia y generación**:
   Dado que $\mathcal{J}(\mathcal{C})[2]$ tiene dimensión 4 sobre $\mathbb{F}_2$, basta probar que los elementos J_1, J_2, J_3, J_4 son linealmente independientes. Como cada J_i se define a partir de

pares de puntos de Weierstrass, y estos generan $\mathcal{J}(\mathcal{C})[2]$, se concluye que $\mathcal{B}$ es una base.

2. **Forma de la matriz de emparejamiento**:
   Consideramos el emparejamiento de Weil de 2-torsion $e_2 : \mathcal{J}(\mathcal{C})[2] \times \mathcal{J}(\mathcal{C})[2] \to \mu_2$, donde $\mu_2 = \{\pm 1\}$. Según la regla de cálculo:

$$e_2(J_i, J_j) = \begin{cases} -1 & \text{si } |\{i,j\} \cap \{k,l\}| = 1, \\ 1 & \text{en otro caso.} \end{cases}$$

   Evaluamos los emparejamientos para nuestra base:

$$M = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

   Aplicamos el logaritmo en base $\mu = -1$:

$$\log_\mu(M) = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

   Observamos que esta matriz tiene la forma canónica de una matriz simpléctica:

$$\Omega = \begin{bmatrix} 0 & I_2 \\ -I_2 & 0 \end{bmatrix},$$

   donde I_2 es la matriz identidad de 2×2. Esto confirma que la base $\mathcal{B}$ es una base simpléctica para $\mathcal{J}(\mathcal{C})[2]$.

Por lo tanto, hemos probado que $\mathcal{B}$ es una base simpléctica, lo que concluye la demostración. ■

Lema 3.8.2 *Sea $\mathcal{B} = (J_1, J_2, J_3, J_4)$ y $\mathcal{C}$ como en el lema 3.8.1. Entonces el conjunto $\mathcal{G}$ de* $(2,2)$ *subgrupos 3.8.1 consta de* 8 *grupos de la forma:*

$$\langle J((x-(-1)^i)(x-(-1)^j)\alpha, 0), J((x-(-1)^{j+1}\alpha)(x-r), 0)\rangle,$$

donde $i, j \in \{0,1\}$ y $r \in \{\beta, \gamma\}$.

Demostración. Sea $i \in \{0, \ldots, 7\}$, y definimos

$$H_i = \langle J_1 + a_i J_3 + b_i J_4, J_2 + b_i J_3 + c_i J_4 \rangle,$$

donde $i = 2^2 a_i + 2^1 b_i + 2^0 c_i$, con $a_i, b_i, c_i \in \{0,1\}$, es la representación $2-$ádica de i, entonces aplicando el algoritmo de Cantor,1.11.1, obtenemos

$$\begin{aligned}
H_0 &= \langle J((x-1)(x-\alpha), 0), J((x+\alpha)(x-\beta), 0)\rangle, \\
H_1 &= \langle J((x-1)(x-\alpha), 0), J((x+\alpha)(x-\gamma), 0)\rangle, \\
H_2 &= \langle J((x+1)(x+\alpha), 0), J((x-\alpha)(x-\gamma), 0)\rangle, \\
H_3 &= \langle J((x+1)(x+\alpha), 0), J((x-\alpha)(x-\beta), 0)\rangle, \\
H_4 &= \langle J((x+1)(x-\alpha), 0), J((x+\alpha)(x-\beta), 0)\rangle, \\
H_5 &= \langle J((x+1)(x-\alpha), 0), J((x+\alpha)(x-\gamma), 0)\rangle, \\
H_6 &= \langle J((x-1)(x+\alpha), 0), J((x-\alpha)(x-\gamma), 0)\rangle, \\
H_7 &= \langle J((x-1)(x+\alpha), 0), J((x-\alpha)(x-\beta), 0)\rangle.
\end{aligned}$$

Estos son los 8 grupos deseados. ■

Definición 3.8.1 *Para una curva de género 2, $\mathcal{C}$, definida por una ecuación hiperelíptica de tipo 2, 3.3.1, decimos que una base simpléctica $\mathcal{B} = (J_1, J_2, J_3, J_4)$ de $\mathcal{J}(\mathcal{C})[2^n]$ es una* ***base simpléctica especial*** *si $2^{n-1}\mathcal{B} = (2^{n-1}J_1, 2^{n-1}J_2, 2^{n-1}J_3, 2^{n-1}J_4)$ es la base del lema 3.8.1.*

Observación 3.8.2 *En el estudio de curvas de género 2 y sus jacobianos, las bases simplécticas juegan un papel fundamental, especialmente en la descripción de la estructura de la torsión en $\mathcal{J}(\mathcal{C})[2^n]$. La elección de una base adecuada es crucial para aplicaciones en criptografía, teoría de números computacional y la teoría de isogenias. En este*

documento, describimos la construcción de una base simpléctica especial para curvas de género 2 definidas por ecuaciones de tipo 2.

Unicidad en el Caso $n = 1$ Cuando $n = 1$, el lema 3.8.1, establece una base simpléctica específica para $\mathcal{J}(\mathcal{C})[2]$. En este caso, no existen otras bases simplécticas especiales equivalentes, lo que implica su unicidad.

Construcción para $n > 1$ La base simpléctica especial se construye en los siguientes pasos:

1. Se toma una base simpléctica arbitraria $\mathcal{B}$ de $\mathcal{J}(\mathcal{C})[2^n]$.
2. Se considera la base de 2-torsión $2^{n-1}\mathcal{B}$ y se determina la transformación a la base del lema 3.8.1.
3. Este cambio de base está dado por una matriz simpléctica M con coeficientes en $\mathbb{Z}_2$.
4. Se levanta M a una matriz simpléctica M_0 con coeficientes en $\mathbb{Z}_{2^n}$.
5. Se aplica M_0 a la base original $\mathcal{B}$, obteniendo así la base simpléctica especial buscada.

Dado que el levantamiento de M a M_0 no es único en general, la base obtenida tampoco es única.

3.9. Algoritmo

Introducción El objetivo de esta sección es describir el algoritmo propuesto en la sección 5.3 de [26] para calcular isogenias $(2^n, 2^n)$ entre jacobianos de curvas de género 2 en términos de sucesiones de isogenias de Richelot. Estas isogenias son fundamentales en aplicaciones criptográficas y se definen anulando un subgrupo de $J(C)[2^n]$ de orden 2^{2n}.

Requisitos del Algoritmo El algoritmo toma como entrada:

1. Una curva de género 2 definida por una ecuación de Tipo-2.
2. Un cuerpo finito K sobre el cual está definida la curva.
3. Que la torsión $\mathcal{J}(\mathcal{C})[2^n]$ sea completamente K-racional, lo que permite trabajar con bases explícitas de torsión.

Curvas de Interés Un caso especialmente relevante es cuando $\mathcal{C}$ es una curva hiperbólica superspecial sobre $K = \mathbb{F}_{p^2}$ con $p \equiv -1 \mod 2^n$. En este caso, la proposición 3.3.1 garantiza la existencia de una ecuación de tipo-2 que facilita los cálculos.

Elección del Subgrupo de Isogenia El subgrupo de $\mathcal{J}(\mathcal{C})[2^n]$ que define la isogenia no se elige arbitrariamente, sino que proviene de un conjunto restringido $\mathcal{G}$, 3.8.1, de cardinalidad 2^{3n}. Este conjunto se construye a partir de una **base simpléctica especial** para $\mathcal{J}(\mathcal{C})[2^n]$, según la definición 3.8.1.

Desde un punto de vista práctico:

- $\mathcal{G}$ contiene más de la mitad de todos los posibles subgrupos de isogenia, por lo que la restricción no afecta significativamente la seguridad criptográfica.
- Esta elección específica de $\mathcal{G}$ ya ha sido propuesta en el contexto de G_2SIDH, [28].

Estructura del Algoritmo El algoritmo sigue los siguientes pasos:

1. **Preparación**: Se selecciona la curva $\mathcal{C}$ y se verifica que cumple con las condiciones necesarias.
2. **Construcción de la base de torsión**: Se obtiene una base simpléctica especial (J_1, J_2, J_3, J_4) para $\mathcal{J}(\mathcal{C})[2^n]$.
3. **Elección del subgrupo** H: Se selecciona un subgrupo adecuado para definir la isogenia.
4. **Cálculo de la isogenia**: Se computa la isogenia $\phi : J\mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ utilizando la información previa.

5. **Cadena de isogenias**: Si es necesario, se repiten los pasos anteriores para construir una secuencia de isogenias.

Conclusión El algoritmo descrito permite computar isogenias $(2^n, 2^n)$ de manera eficiente en curvas de género 2. La clave está en el uso de ecuaciones de Tipo-2 y en la cuidadosa selección del subgrupo de isogenia a partir del conjunto $\mathcal{G}$, lo que garantiza una implementación computacionalmente viable en aplicaciones criptográficas.

Configuración: Sea K un cuerpo finito de característica mayor que 3. Iniciamos con el jacobiano $\mathcal{J}_0$, de la curva $\mathcal{C}_0$, y un $(2^n, 2^n)$ $K-$racional $H = \langle H_1, H_2 \rangle \subseteq \mathcal{J}_0$. El objetivo es calcular la isogenia $\phi : \mathcal{J}_0 \to \mathcal{J}_n$ con kernel H.

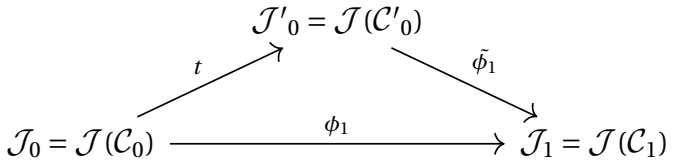
Muestreo Aleatorio Para seleccionar aleatoriamente una isogenia $(2^n, 2^n)$, se eligen tres elementos $a, b, c \in \mathbb{Z}_{2^n}$ y luego se calculan los elementos

$$H_{1,0} = J_1 + aJ_3 + bJ_4, \quad H_{2,0} = J_2 + bJ_3 + cJ_4.$$

El siguiente procedimiento calcula una isogenia $\phi : \mathcal{J}(\mathcal{C}_0) \to \mathcal{J}(\mathcal{C}_n)$ con kernel $\langle H_{1,0}, H_{2,0} \rangle$.

La isogenia ϕ es calculada como $\phi = \phi_n \circ \cdots \circ \phi_1$, donde cada $\phi_i : \mathcal{J}_{i-1} \to \mathcal{J}_i$ es una $(2,2)-$isogenia.

Primero, calculamos la $(2,2)-$isogenia $\phi_1 : \mathcal{J}_0 \to \mathcal{J}_1$ con kernel $H_{\phi_1} = \langle 2^{n-1} H_1, 2^{n-1} H_2 \rangle$. Para ello aplicamos



Donde, t es el cambio de coordenadas de una ecuación de tipo 1 a una ecuación de tipo 2 ecuación dado por la proposición 3.4.2 y el teorema 3.4.1, tal que $(x', y') = t(x, y)$, luego por la proposición 3.4.2, obtenemos una isogenia $\tilde{\phi}_1 : \mathcal{J}(\mathcal{C}'_0) \to \mathcal{J}(\mathcal{C}_1)$ de una ecuación de tipo 1 a una de tipo 2, así obteniendo $\phi_1 : \mathcal{J}(\mathcal{C}_0) \to \mathcal{J}(\mathcal{C}_1)$.

De lo anterior tenemos el proceso iterativo siguiente:

Para $1 \leq i \leq n$, se realizan los siguientes pasos:

1. Calculamos $H_1^* := 2^{n-i} H_{1,i-1}$, $H_2^* := 2^{n-i} H_{2,i-1}$, y los denotamos por $H_1^* = \mathcal{J}(g_1, 0)$, $H_2^* = \mathcal{J}(g_2, 0)$.

2. Factorizar g_1 y g_2, descritos por $g_1 = (x - \alpha_1)(x - \alpha_2)$, $g_2 = (x - \beta_1)(x - \beta_2)$.

3. Realizar el cambio de coordenadas $(x', y') = t(x, y)$ para obtener la ecuación de tipo 1
$$\mathcal{C}'_{i-1} : y'^2 = E'_{i-1} x'(x'^2 - A'_{i-1} x' + 1)(x'^2 - B_{i-1} x' + C'_{i-1}),$$
tal que $t(g_1) = x'$ y $t(g_2) = (x')^2 - A'_{i-1} x' + 1$.

4. Si $C'_{i-1} = 1$ no proseguir. De otro modo, se aplica la isogenia de Richelot $\tilde{\phi}_i : \mathcal{J}(\mathcal{C}'_{i-1}) \to \mathcal{J}(\mathcal{C}_i)$ de la proposición 3.4.2 para obtener una ecuación de tipo 2
$$\mathcal{C}_i : y^2 = (x^2 - 1)(x^2 - A_i)(E_i x^2 - B_i x + C_i),$$
y la formula de la proposición 3.4.1 para obtener $H_{1,i} = \phi_i(H_{1,i-1})$, $H_{2,i}\phi_i(H_{2,i-1})$, donde $\phi_i = \tilde{\phi}_i \circ t$.

Observación 3.9.1 *Con el método anteriormente presentado es posible ejecutar eficientemente todos los pasos en el cálculo de la cadena de isogenias. A continuación, se presentan más detalles sobre la implementación:*

1. *El primer paso consiste únicamente en realizar duplicaciones iterativas de elementos en el jacobiano. Existen algoritmos eficientes para este procedimiento, desarrollados en el contexto de la criptografía basada en curvas hiperelípticas (HECC), como se muestra en [29]. Basándonos en estos resultados, se han diseñado fórmulas específicas para ecuaciones de Tipo-2 que optimizan este cálculo.*

   Para $i < n$, también almacenamos el elemento de 4-torsión $2^{n-i-1} H_{1,i-1}$ obtenido durante la computación, el cual será utilizado posteriormente en el Paso 3.

2. *A primera vista, el segundo paso parece computacionalmente costoso, ya que implica la factorización de dos polinomios. Sin embargo, es posible aprovechar las propiedades de la base simpléctica especial $\mathcal{B}$. De acuerdo con el Lema 3.8.2 , se tiene que $\beta_1 \in \{\pm 1\}$, lo que permite determinar β_1 y β_2 mediante un análisis de casos. Además, el mismo lema implica que $\gamma_1 = -\beta_2$, lo que facilita el cálculo de γ_2 a partir de los coeficientes del polinomio g_2.*

3. *En el cuarto paso, se aplican una vez las fórmulas de la proposición 3.4.2 para obtener los coeficientes de la nueva ecuación de Tipo-2. Luego, la fórmula del Teorema 3.4.1 se emplea dos veces para calcular las imágenes de los generadores del núcleo.*

   Cabe destacar que estas fórmulas solo pueden aplicarse si el codominio de la isogenia $\tilde{\phi}_i$ es la jacobiana de una curva hiperelíptica, lo que equivale a la condición $\epsilon = C_i^0 - 1 \neq 0$, Proposición 4.2. Si se cumple $\epsilon = 0$, el algoritmo se detiene. En el contexto de G_2SIDH, donde la curva C_0 es supersingular y $n \approx \log(p)/2$, esto ocurre con una probabilidad aproximada de $\log(p)/p$, según [9].

Observación 3.9.2 *En la última isogenia de tipo $(2,2)$ dentro de la cadena, el algoritmo descrito requiere una operación de raíz cuadrada en el Paso 3. No obstante, es posible evitar este cálculo realizando una ligera modificación en la configuración. En particular, se puede elegir una curva $\mathcal{C}$ tal que $\mathcal{J}(\mathcal{C})[2^{n+1}]$ sea K-racional y proporcionar el núcleo H para una isogenia $(2^{n+1}, 2^{n+1})$, pero considerar únicamente la isogenia $(2^n, 2^n)$ definida por $2H$. En otras palabras, se omite el último paso del cálculo de la isogenia. En el caso supersingular, esto implica aumentar en dos bits el tamaño del cuerpo primo subyacente.*

Observación 3.9.3 *Por último, vemos la eficiencia de algoritmo en la discusión de la sección 5.4 de [26], lo cual es importante en las aplicaciones que involucren este tipo de estructuras.*

En la siguiente sección, a modo de ejemplo, se presentará el algoritmo G2SIDH, el cual ilustra una implementación del protocolo de intercambio de claves basado en isogenias para curvas de género 2.

3.10. (2,2)-isogenias en criptografía

Un problema importante en criptografía, es el desarrollo de protocolos de intercambio de claves. En particular durante los últimos años, ha surgido el interés de desarrollar protocolos resistentes a ataques cuánticos. El protocolo G2SIDH (Genus Two Supersingular Isogeny Diffie-Hellman) surge como una extensión del esquema SIDH. Este último, se enmarca dentro de la familia de protocolos basados en isogenias de curvas elípticas supersingulares. G2SIDH, se expande hacia la criptografía basada en

isogenias en variedades abelianas de dimensión superior. Su diseño busca mantener las ventajas de SIDH, como claves compactas y resistencia a ataques cuánticos, mientras aprovecha estructuras más ricas provenientes de curvas de género 2. Esta variante ha sido propuesta para aplicaciones criptográficas avanzadas, incluyendo esquemas de intercambio de claves y sistemas de cifrado que requieren seguridad a largo plazo. Dada su relación con isogenias entre jacobianos de curvas hiperelípticas, G2SIDH representa un paso hacia la diversificación de los protocolos basados en isogenias, con posibles beneficios en eficiencia y seguridad.

A pesar de los avances en el desarrollo de G2SIDH, se han identificado ataques teóricos que comprometen su seguridad en ciertos escenarios, al igual que ocurrió con SIDH, ver [17]. Sin embargo, estos resultados no han reducido el interés en la criptografía basada en isogenias, sino que han motivado una exploración más profunda de sus fundamentos matemáticos y de nuevas estrategias para fortalecer estos esquemas. El estudio de G2SIDH sigue siendo relevante tanto desde el punto de vista criptográfico como matemático, ya que permite comprender mejor la estructura de isogenias en variedades abelianas y desarrollar alternativas más seguras dentro de la criptografía post-cuántica.

A continuación, presentamos el siguiente algoritmo, cuya descripción detallada puede encontrarse en la sección 3.4 de [13].

Condiciones iniciales:

- Tomar un primo grande de la forma $p = 2^n 3^m d - 1$.
- Escoger una curva hiperelíptica aleatoria $\mathcal{C}/\mathbb{F}_{p^2}$, con $\mathcal{J}_\mathcal{C}$ su jacobiano.
  - Puede tomarse una en un caso especial dada por, $\mathcal{C}_0 : y^2 = x^6 + 1$.
  - $\mathcal{J}_{\mathcal{C}_0}$ es super especial, como es su doble cubierta $y^2 = x^3 + 1$.
  - Tomar una sucesión aleatoria de Isogenias de Richelot $\mathcal{J}_0 \to \mathcal{J}_1 \to \cdots \to \mathcal{J}$, tomando al menos $O(log(p))$ pasos para obtener una curva aleatoria $\mathcal{C}$.
- Calcular bases simplécticas $\{P_1, P_2, P_3 P_4\}$ para $\mathcal{J}_\mathcal{C}[2^n]$ y $\{Q_1, Q_2, Q_3, Q_4\}$ para $\mathcal{J}_\mathcal{C}[3^m]$.

Primera etapa: Alice

1. Alice escoge 12 escalares aleatorios $a_1, \ldots, a_{12} \in \{0, 1, \ldots, 2^n - 1\}$.

2. Ella calcula el subgrupo $\mathcal{A} \subseteq \mathcal{J}(\mathcal{C})[2^n]$, dado por:

$$\mathcal{A} := \langle a_1P_1+a_2P_2+a_3P_3+a_4P_4,\ a_5P_1+a_6P_2+a_7P_3+a_8P_4,\ a_9P_1+a_{10}P_2+a_{11}P_3+a_{12}P_4\rangle.$$

Los escalares (a_i) son escogidos de tal forma que $\mathcal{A}$ es maximal 2^nisotrópico.

3. Alice envía la tupa $(\mathcal{J}_{\mathcal{C}}/\mathcal{A}, \phi_{\mathcal{A}}(Q_1), \phi_{\mathcal{A}}(Q_2), \phi_{\mathcal{A}}(Q_3), \phi_{\mathcal{A}}(Q_4))$ a Bob.

¿Cómo debería escoger los escalares $a_1, \dots a_{12}$ Alice?
Sean

$$\begin{aligned} R_1 &= a_1P_1 + a_2P_2 + a_3P_3 + a_4P_4, \\ R_2 &= a_5P_1 + a_6P_2 + a_7P_3 + a_8P_4, \\ R_3 &= a_5P_1 + a_6P_2 + a_7P_3 + a_8P_4. \end{aligned}$$

- Alice debe asegurarse de que $\mathcal{A}$ es un subgrupo maximal 2^n- isotrópico de $\mathcal{J}_{\mathcal{C}}[2^n]$, es decir, debe escoger generadores R_1, R_2 y R_3 tales que

$$e_{2^n}(R_1, R_2) = e_{2^n}(R_1, R_3) = e_{2^n}(R_2, R_3) = 1.$$

- Utilizando la linealidad y que e_{2^n} es sesquilineal, entonces:

$$\begin{aligned} e(R_1, R_2) =& e(P_1, P_2)^{a_1a_6-a_2a_5} e(P_1, P_3)^{a_1a_7-a_3a_5} e(P_1, P_4)^{a_1a_8-a_4a_5} \\ & \cdot e(P_2, P_3)^{a_2a_7-a_3a_6} e(P_2, P_4)^{2a_8-a_4a_6} e(P_3, P_4)^{a_3a_8-a_4a_7} = 1. \end{aligned}$$

Alice puede hacer lo siguiente:

1. Como $e(P_i, P_j) = \mu_{2^n}^{\alpha_{i,j}}$ para algún $\alpha_{i,j} \in \mathbb{Z}$, calcula los valores $\alpha_{i,j} (mod\ 2^n)$ tales que $e(P_i, P_j) = e(P_1, P_2)^{\alpha_{i,j}}$.

2. Elige aleatoriamente $a_1, a_2, a_3, a_4 \in \{0, 1, \dots, 2^n - 1\}$ tal que al menos uno de los cuatro es impar.

3. Elige un $k \in \{0, 1, \dots, n\}$ y elige aleatorios a_5, a_6, a_7, a_8 tales que

$$\begin{aligned} & a_1a_6 - a_2a_5 + \alpha_{1,3}(a_1a_7 - a_3a_5) + \alpha_{1,4}(a_1a_8 - a_4a_5) \\ & + \alpha_{2,3}(a_2a_7 - a_3a_6) + \alpha_{2,4}(a_2a_8 - a_4a_6) + \alpha_{3,4}(a_3a_8 - a_4a_7) \equiv 0\ mod\ 2^k. \end{aligned}$$

4. Elige aleatorios $a_9, a_{10}, a_{11}, a_{12}$ tales que

$$a_1a_{10} - a_2a_9 + \alpha_{1,3}(a_1a_{11} - a_3a_9) + \alpha_{1,4}(a_1a_{12} - a_4a_9)$$
$$+ \alpha_{2,3}(a_2a_{11} - a_3a_{10}) + \alpha_{2,4}(a_2a_{12} - a_4a_{10}) + \alpha_{3,4}(a_3a_{12} - a_4a_{11}) \equiv 0 \ mod\ 2^{n-k}.$$

Primera etapa: Bob

1. Bob también escoge 12 escalares aleatorios $b_1, \ldots, b_{12} \in \{0, 1, \ldots, 3^m - 1\}$.
2. El calcula el subgrupo $\mathcal{B} \subseteq \mathcal{J}_{\mathcal{C}}[3^m]$, dado por:

$$\mathcal{B} := \langle b_1Q_1 + b_2Q_2 + b_3Q_3 + b_4Q_4,\ b_5Q_1 + b_6Q_2 + b_7Q_3 + b_8Q_4,\ b_5Q_1 + b_6Q_2 + b_7Q_3 + b_8Q_4 \rangle.$$

   Los escalares (b_i) son escogidos de tal forma que $\mathcal{B}$ es maximal 3^misotrópico.

3. Bob envía la tupa $(\mathcal{J}_{\mathcal{C}}/\mathcal{B}, \phi_{\mathcal{B}}(P_1), \phi_{\mathcal{B}}(P_2), \phi_{\mathcal{B}}(P_3), \phi_{\mathcal{B}}(P_4))$ a Bob.

Segunda etapa: Alice

1. Alice recibe la tupla de Bob y calcula:

$$\begin{aligned}\mathcal{A}' := \langle & a_1\phi_{\mathcal{B}}(P_1) + a_2\phi_{\mathcal{B}}(P_2) + a_3\phi_{\mathcal{B}}(P_3) + a_4\phi_{\mathcal{B}}(P_4), \\ & a_5\phi_{\mathcal{B}}(P_1) + a_6\phi_{\mathcal{B}}(P_2) + a_7\phi_{\mathcal{B}}(P_3) + a_8\phi_{\mathcal{B}}(P_4), \\ & a_9\phi_{\mathcal{B}}(P_1) + a_{10}\phi_{\mathcal{B}}(P_2) + a_{11}\phi_{\mathcal{B}}(P_3) + a_{12}\phi_{\mathcal{B}}(P_4)\rangle.\end{aligned}$$

2. Entonces Alice tiene la isogenia

$$\phi_{\mathcal{A}'} : \mathcal{J}_{\mathcal{C}}/\mathcal{B} \to (\mathcal{J}_{\mathcal{C}}/\mathcal{B})/\mathcal{A},$$

   y puede calcular los $G2$ invariantes de $(\mathcal{J}_{\mathcal{C}}/\mathcal{B})/\mathcal{A}'$.

Segunda etapa: Bob

1. De forma análoga, Bob recibe la tupla de Alice y calcula:

$$\begin{aligned}\mathcal{B}' := \langle & b_1\phi_{\mathcal{A}}(Q_1) + b_2\phi_{\mathcal{A}}(Q_2) + b_3\phi_{\mathcal{A}}(Q_3) + b_4\phi_{\mathcal{A}}(Q_4), \\ & b_5\phi_{\mathcal{A}}(Q_1) + b_6\phi_{\mathcal{A}}(Q_2) + b_7\phi_{\mathcal{A}}(Q_3) + b_8\phi_{\mathcal{A}}(Q_4), \\ & b_9\phi_{\mathcal{A}}(Q_1) + b_{10}\phi_{\mathcal{A}}(Q_2) + b_{11}\phi_{\mathcal{A}}(Q_3) + b_{12}\phi_{\mathcal{A}}(Q_4)\rangle.\end{aligned}$$

2. Bob entonces tiene la isogenia $\phi_{\mathcal{B}'} : \mathcal{J}_{\mathcal{C}} / \mathcal{A} \to (\mathcal{J}_{\mathcal{C}} / \mathcal{A}) / \mathcal{B}'$, y puede calcular los invariantes de $(\mathcal{J}_{\mathcal{C}} / \mathcal{A}) / \mathcal{B}'$.

Notemos que,

$$(\mathcal{J}_{\mathcal{C}} / \mathcal{A}) / \mathcal{B}' = (\mathcal{J}_{\mathcal{C}} / \mathcal{A}) / \phi_{\mathcal{A}}(\mathcal{B}) \cong \mathcal{J}_{\mathcal{C}} / \langle \mathcal{A}, \mathcal{B} \rangle \cong (\mathcal{J}_{\mathcal{C}} / \mathcal{B}) / \phi_{\mathcal{B}}(\mathcal{A}) = (\mathcal{J}_{\mathcal{C}} / \mathcal{B}) / \mathcal{A}'.$$

Así, Alice y Bob pueden calcular los G2 invariantes y usarlos como su secreto compartido.

Bibliografía

[1] ARBARELLO, E., CORNALBA, M., GRIFFITHS, P., AND HARRIS, J. *Geometry of Algebraic Curves: Volume I*. Grundlehren der mathematischen Wissenschaften. Springer New York, 2013.

[2] BAS EDIXHOVEN, GERARD VAN DER GEER, B. M. Abelian varieties, 2020. `http://van-der-geer.nl/~gerard/`.

[3] BEAUVILLE, A. Classical theta functions and their generalization, 2011. `https://api.semanticscholar.org/CorpusID:15380826`.

[4] CANTOR, D. G. Computing in the jacobian of a hyperelliptic curve. *Mathematics of Computation 48* (1987), 95–101.

[5] CASSELS, J., AND FLYNN, E. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. EBL-Schweitzer. Cambridge University Press, 1996.

[6] CASTRYCK, W., AND DECRU, T. An efficient key recovery attack on SIDH. Cryptology ePrint Archive, Paper 2022/975, 2022.

[7] COHEN, H., FREY, G., AVANZI, R., DOCHE, C., LANGE, T., NGUYEN, K., AND VERCAUTEREN, F. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 2005.

[8] CONRAD, B. 2004-05 vigre number theory working group, 2004. `http://math.stanford.edu/~conrad/vigregroup/index.html`.

[9] COSTELLO, C., AND SMITH, B. The supersingular isogeny problem in genus 2 and beyond. In *Post-Quantum Cryptography* (Cham, 2020), J. Ding and J.-P. Tillich, Eds., Springer International Publishing, pp. 151–168.

[10] EID, E. Efficient computation of cantor's division polynomials of hyperelliptic curves over finite fields. *Journal of Symbolic Computation 117* (2023), 68–100.

[11] FABER, C., AND LOOIJENGA, E. *Moduli of Curves and Abelian Varieties: The Dutch Intercity Seminar on Moduli*. Aspects of Mathematics. American mathematical society., 1999.

[12] FATIGHENTI, E. Topics on fano varieties of k3 type, 2022.

[13] FLYNN, E. V., AND TI, Y. B. Genus two isogeny cryptography. Cryptology ePrint Archive, Paper 2019/177, 2019.

[14] GALBRAITH, S., LIN, X., AND MIRELES, D. Pairings on hyperelliptic curves with a real model. Cryptology ePrint Archive, Paper 2008/250, 2008.

[15] GALBRAITH, S. D. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.

[16] GMIRA, S. Abel-Jacobi theorem. working paper or preprint, July 2015.

[17] GOH, A., LIM, C.-W., AND TI, Y. B. Generalising fault attacks to genus two isogeny cryptosystems. Cryptology ePrint Archive, Paper 2022/196, 2022.

[18] GONZÁLEZ, J., GUÀRDIA, J., AND ROTGER, V. Abelian surfaces of gl2-type as jacobians of curves. *Acta Arithmetica 116*, 3 (2005), 263–287.

[19] HARTSHORNE, R. *Algebraic geometrry*. Springer, 1997.

[20] JEONG, K., KWON, Y.-W., AND PARK, J. Decomposition of the jacobian of some twists of a genus 2 curve. *Bulletin of the Australian Mathematical Society* (2024), 1–15.

[21] KANEV, V. *Spectral curves and Prym—Tjurin varieties I*. De Gruyter, Berlin, New York, 1995, pp. 151–198.

[22] KANI, E. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik 485* (1997), 93–122.

[23] KNAPP, A. W. *Elliptic Curves. (MN-40), Volume 40*. Princeton University Press, 1992.

[24] KRICK, T. Resultante, subresultantes y sumas de sylvester, 2015. http://mate.dm.uba.ar/~krick/LaResultante.pdf.

[25] KUNZWEILER, S. Richelot isogenies., 2022. https://github.com/sabrinakunzweiler/richelot-isogenies?tab=readme-ov-file#readme.

[26] KUNZWEILER, S. Efficient computation of $(2^n, 2^n)$-isogenies. *Des. Codes Cryptogr. 92* (2024), 1761–1802.

[27] KUNZWEILER, S. Isogeny computations in higher dimensions, 25th workshop on elliptic curve cryptography., 2024. https://troll.iis.sinica.edu.tw/ecc24/slides/3-01-ecc-workshop-kunzweiler.pdf.

[28] KUNZWEILER, S., TI, Y. B., AND WEITKÄMPER, C. Secret keys in genus-2 sidh. In *Selected Areas in Cryptography* (Cham, 2022), R. AlTawy and A. Hülsing, Eds., Springer International Publishing, pp. 483–507.

[29] LANGE, T. Formulae for arithmetic on genus 2 hyperelliptic curves. *Ruhr-University of Bochum, Universit¨atsstr* (2005).

[30] LOMBARDO, D. Abelian varieties - luxembourg summer school on galois representations, 2018. https://people.dm.unipi.it/lombardo/Teaching/VarietaAbeliane1718/Notes.pdf.

[31] LORENZINI, D. *An Invitation to Arithmetic Geometry,*. American Mathematical Society, 1993.

[32] MARC HINDRY, MARUSIA REBOLLEDO, D. R. Variedades abelianas, una introducción, 2019. https://www.famaf.unc.edu.ar/~apacetti/agra3/VarAbel.pdf.

[33] MARC HINDRY, J. H. S. *Diophantic Geometry*. Springer-Verlag, New York, 2000.

[34] MILNE, J. S. Abelian varieties (v2.00), 2008. www.jmilne.org/math/.

[35] MIRANDA, R. *Algebraic curves and Riemann surfaces*. American Mathematical Society, 1995.

[36] MUMFORD, D., RAMANUJAM, C., AND MANIN, I. *Abelian Varieties*. Studies in mathematics. Hindustan Book Agency, 2008.

[37] MÜLLER, J. S. Explicit kummer surface theory for arbitrary characteristic, 2009.

[38] OUDOMPHENG, R., AND POPE, G. A note on reimplementing the castryck-decru attack and lessons learned for SageMath. Cryptology ePrint Archive, Paper 2022/1283, 2022.

[39] RIQUELME, E. Trisection for genus 2 curves in odd characteristic. *Applicable Algebra in Engineering, Communication and Computing 27* (2016), 373–397.

[40] ROJAS MENDOZA, E. A. *El teorema de Hasse-Weil*. Tesis, Universidad Nacional Mayor de San Marcos, 2020.

[41] RUSSELL, H. Albanese varieties with modulus over a perfect field, 2013.

[42] SANTOS, M. C.-R., AND FLYNN, E. V. Isogenies on kummer surfaces, 2024.

[43] SHAFAREVICH, I. R. *Basic Algebraic Geometry 1*. Springer Berlin, Heidelberg, 2013.

[44] SILVERMAN. *The arithmetic of elliptic curves*. Springer-Verlag New York, 2009.

[45] SMITH, B. Explicit endomorphisms and correspondences. *Bulletin of The Australian Mathematical Society - BULL AUST MATH SOC 74* (12 2006).

[46] TI, Y. B. Isogenies of abelian varieties in cryptography. *Bulletin of the Australian Mathematical Society 101*, 3 (2020), 508–509.