Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Tesis de Licenciatura

Curvas elípticas sobre $\mathbb{Q}(t)$ de rango alto

Marcelo Alejandro Valdettaro

Director: Ariel Pacetti
Codirector: Martín Avendaño

Septiembre de 2008

Índice general

1. Variedades **7**

1.1. Variedades Afines 7

1.2. Variedades Proyectivas 11

1.2.1. La Recta Proyectiva y el Plano Proyectivo 11

1.2.2. El Espacio Proyectivo 13

1.2.3. Variedades Proyectivas 15

1.2.4. Variedades afines $\longleftrightarrow$ Variedades proyectivas 18

1.2.5. Funciones entre variedades proyectivas 21

1.3. Curvas Algebraicas 24

1.3.1. Funciones entre curvas 29

1.3.2. Divisores 30

2. Curvas Elípticas **33**

2.1. Curvas Elípticas 33

2.1.1. Ley de grupo en curvas elípticas 37

2.1.2. Fórmulas explícitas para la ley de grupo 40

2.2. Teorema de Mordell-Weil 41

2.2.1. El grupo de puntos K-racionales 42

2.2.2. Teorema débil de Mordell-Weil 43

2.2.3. Alturas y Teorema de Mordell-Weil 43

2.2.4. Altura Canónica 47

3. Curvas Elípticas sobre $\overline{\mathbb{Q}(t)}$ - Superficies Elípticas **50**

3.1. Curvas Elípticas sobre $\overline{\mathbb{Q}(t)}$ 50

3.1.1. Alturas en curvas elípticas definidas sobre $\overline{\mathbb{Q}(t)}$ . . . 51
3.1.2. Teorema de Mordell-Weil sobre $\mathbb{Q}(t)$ . . . 56
3.1.3. Altura Canónica. . . . 58
3.2. Superficies . . . 59
3.2.1. Superficies Elípticas . . . 60
3.3. Geometría de las Superficies Fibradas . . . 66
3.3.1. Divisores sobre Superficies Fibradas . . . 66
3.3.2. Intersección . . . 80
3.3.3. Blowing Up . . . 95
3.3.4. Minimalidad de Superficies . . . 99
3.4. Geometría de las Superficies Elípticas . . . 101
3.4.1. Modelo Minimal . . . 101
3.4.2. Forma bilineal de Manin-Shioda . . . 107

4. Construcción de Mestre **124**
4.1. Una familia de Curvas Elípticas sobre $\mathbb{Q}(t)$ de rango mayor o igual que 8 . . . 124
4.2. La construcción de Mestre . . . 126

Bibliografía **128**

Introducción

Uno de los temas más importantes dentro de la Teoría de Números es el estudio de las Curvas Elípticas. Las mismas además de ser interesantes en sí mismas, son de gran utilidad para resolver numerosos problemas; también son un lugar en el que confluyen otras ramas de la matemática, como la Geometría y el Algebra. Al trabajar con Curvas Elípticas uno incursiona por estas disciplinas utilizando diferentes herramientas de cada una de ellas.

El estudio de las Curvas Elípticas ha tenido una gran relevancia histórica y permitió resolver muchos problemas difíciles. Por ejemplo fueron parte esencial en la demostración del último teorema de Fermat que dio Andrew Wiles en los años '90.

Dado un cuerpo K de característica distinta de 2, una Curva Elíptica E puede verse como el conjunto de soluciones, sobre una clausura algebraica $\overline{K}$ de K, de una ecuación del tipo:

$$y^2 = x^3 + ax^2 + bx + c,$$

donde $a, b, c \in \overline{K}$ y $f(x) = x^3 + ax^2 + bx + c$ no tiene raíces múltiples. Al conjunto $E(\overline{K})$ de sus soluciones se le puede dar estructura de grupo abeliano tomando como elemento neutro al punto proyectivo $[0 : 1 : 0]$. Si $a, b, c \in K$ y se considera el conjunto $E(K)$ de las soluciones en K, se tiene que éste es un subgrupo de $E(\overline{K})$.

Si K es un cuerpo de números, el Teorema de Mordell-Weil dice que $E(K)$ es finitamente generado y, en particular, por el Teorema de Estructura se tiene que:

$$E(K) \simeq \mathbb{Z}^r \oplus T;$$

donde T es la parte de torsión y el rango r pertenece a $\mathbb{N}_0$.

Hay muchos resultados conocidos que permiten, dada una curva elíptica E, caracterizar completamente su parte de torsión. Sin embargo el problema de calcular el rango es muy difícil y poco se sabe al respecto. La heurística muestra que las curvas elípticas con rango grande (digamos mayor o igual a dos) son "pocas"(en términos de densidades) y no se sabe que tan grande puede ser el rango de una curva elíptica. De hecho, el rango más grande conocido hoy en día es 28.

Un recurso para construir familias de curvas elípticas de rango alto es trabajar con cuerpos de funciones. Por ejemplo, si se toma $K = \mathbb{Q}(t)$, bajo una hipótesis adicional, se tiene también un teorema de Mordell-Weil y, por lo tanto, también existe una noción de rango. Un teorema de especializaciones dice que si uno tiene una curva elíptica sobre $\mathbb{Q}(t)$ con r puntos linealmente

independientes (en particular de rango al menos r), mirando casi todas sus especializaciones de t (es decir, todas salvo una cantidad finita) los r puntos siguen siendo linealmente independientes en la curva obtenida.

Una de las comodidades que ofrece trabajar con el cuerpo $\mathbb{Q}(t)$ es que hay una técnica que permite testear la independencia lineal de puntos de una manera sencilla. En este trabajo mostramos con detalle la teoría de curvas elípticas sobre cuerpos de funciones, el método para testear independencia lineal de puntos en dichas curvas y ofrecemos algunos ejemplos desarrollados exhaustivamente. Daremos también una construcción de Jean François Mestre en los años '90 de una curva elíptica sobre $\mathbb{Q}(t)$ de rango 12 y, siguiendo la esencia de su idea, contaremos cómo construimos otra familia de curvas elípticas sobre $\mathbb{Q}(t)$ con rango mayor o igual que 8 donde la independencia de los 8 puntos es más sencilla de verificar.

El trabajo está dividido en cuatro capítulos. En el primero presentamos las variedades afines y proyectivas en general y sus principales propiedades que necesitamos para más adelante.

En el segundo capítulo presentamos a las Curvas Elípticas como caso particular de variedades proyectivas y mostramos con detalle toda su estructura algebraica y geométrica.

El tercero es el capítulo central de todo el trabajo. En él trabajamos con curvas elípticas sobre $\mathbb{Q}(t)$, mostramos cómo es el procedimiento para testear la independencia lineal de puntos y desarrollamos paralelamente un ejemplo en el que aplicamos este proceso con todo detalle.

En el cuarto capítulo contamos a grandes rasgos el trabajo de Jean François Mestre y cómo es que, tomando como punto de partida sus ideas, pudimos construir la familia de curvas elípticas sobre $\mathbb{Q}(t)$ de rango 8.

Agradecimientos

Agradezco a Teresa Krick y a Roberto Miatello por haber aceptado ser jurados de esta tesis y por tomarse el trabajo de leerla con todo detalle y hacer correcciones.

Quiero expresar un gran agradecimiento a Ariel Pacetti y a Martín Avendaño por haberme permitido trabajar con ellos. No sólo fue un lujo estar al lado de personas que saben tanto, sino también fue un gran placer trabajar con ellos en un clima tan cordial y amistoso. En este sentido agradezco también, de nuevo, a Teresa Krick, porque ella también trabajó mucho con nosotros aportando conocimiento y muy buena predisposición, y todo siempre dentro de un marco realmente amable.

No me van a alcanzar las palabras para agradecer la gran ayuda que me brindó mi amigo Nicolás Sirolli. He recurrido a él por cuanto problema técnico tuve y siempre me lo resolvió con total desinterés.

También quiero agradecer profundamente a otro amigo: Gastón Freire. Gracias a él pude iniciarme en lo que es la escritura en LaTex, un mundo totalmente desconocido para mí algunos meses atrás.

Muchas gracias también a Laura Barbagallo, otra amiga, que me prestó sus apuntes.

Ya saliendo del tema específico de la tesis, agradezco obviamente a toda mi familia que siempre estuvo conmigo, no sólo a lo largo de toda la carrera, sino también a lo largo de toda mi vida. Desde mis abuelos hasta los más recientes: mis sobrinos Santiago y Joaquín.

Agradezco a los compañeros de trabajo que tuve en el CBC, porque fueron y son mucho más que compañeros.

Y también, por supuesto, a todos los compañeros que conocí desde que entré a la facultad. Pude hacer muchos amigos que hacen que ir a la facultad no sea sólo para estudiar y trabajar, sino para mucho más que eso. Por suerte son muchos y conforman una lista bien larga. Espero poder expresarles a diario todo el afecto que les tengo y mis infinitos agradecimientos por lo bien que me hacen sentir dentro y fuera de la facultad.

A todos ustedes: GRACIAS!!!

Capítulo 1

Variedades

En este capítulo haremos una breve introducción a las variedades afines y proyectivas sobre un cuerpo K perfecto. Veremos que las curvas elípticas son casos particulares de éstas. En particular nos van a interesar los casos $K = \mathbb{Q}$, ó K un cuerpo de números; y más adelante $K = \mathbb{Q}(t)$; pero la teoría de variedades es más general; así que por ahora vamos a trabajar sobre cualquier cuerpo K perfecto.

1.1. Variedades Afines

Empecemos recordando que un cuerpo K se dice perfecto si toda extensión algebraica de K es separable.

Sea K un cuerpo perfecto y $\overline{K}$ una clausura algebraica fija. El *espacio afín* sobre K de dimensión n es el conjunto:

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

El conjunto de puntos K*-racionales* en $\mathbb{A}^n$ es:

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

Consideremos el anillo de polinomios en n variables con coeficientes en $\overline{K}$. Es decir:

$$\overline{K}[\mathbf{x}] = \overline{K}[x_1, ..., x_n].$$

Dado un ideal $I \subseteq \overline{K}[\mathbf{x}]$ podemos asociarle un subconjunto de puntos de $\mathbb{A}^n$ dado por:

$$V(I) = \{P \in \mathbb{A}^n \,:\, f(P) = 0\,,\, \forall\, f \in I\}.$$

Aquí ya podemos dar la primera definición importante de este capítulo.

Definición 1.1.1. Dado K un cuerpo perfecto y $\overline{K}$ una clausura algebraica fija, llamamos *variedad afín* a un subconjunto de $\mathbb{A}^n$ de la forma $V(I)$ para algún ideal $I \subseteq \overline{K}[\mathbf{x}]$.

Dada una variedad afín V, podemos calcular el ideal $I(V)$ que la define del siguiente modo:

$$I(V) = \left\{ f \in \overline{K}\left[\mathbf{x}\right] \,:\, f(P) = 0\,,\, \forall\, P \in I \right\}.$$

Si V es una variedad, siempre se tiene $V(I(V)) = V$ pero no necesariamente se tiene para un ideal I que $I = I(V(I))$. Esto es, dado un ideal I, podemos asociarle la variedad $V(I)$. Pero si calculamos $I(V(I))$ como hicimos recién no siempre volvemos a obtener I. No es difícil verificar, sin embargo, que una inclusión sí es cierta en general:

$$I \subseteq I(V(I)).$$

Diremos que una variedad afín V es *definida sobre* K si su ideal $I(V)$ puede ser generado por polinomios en $K\left[\mathbf{x}\right]$.

Ejemplo 1.1.2. Sea $K = \mathbb{Q}$, el cuerpo de los números racionales, y una clausura algebraica fija $\overline{\mathbb{Q}}$. Sea $n = 2$. O sea, el espacio afín que estamos considerando es $\overline{\mathbb{Q}}^2$ y el anillo de polinomios asociado es $\overline{\mathbb{Q}}\left[x, y\right]$. Sea $I = \left(y - x^2\right)$. La variedad afín asociada será el conjunto V formado por todos los puntos de la parábola de ecuación $y - x^2 = 0$. Esta variedad V es definida sobre $\mathbb{Q}$, pues afirmamos que su ideal asociado es I, que puede generarse con polinomios en $\mathbb{Q}\left[x, y\right]$. Veamos que en efecto el ideal asociado a V es I. O sea:

$$I(V) = I.$$

Es claro que $I \subseteq I(V)$, pues $y - x^2$ se anula en todos los puntos de V. Para ver la otra inclusión tomemos cualquier $f \in I(V)$. Escribamos:

$$f(x, y) = (y - x^2)q(x, y) + r(x);$$

pensando a $f \in \overline{\mathbb{Q}}\left[x\right]\left[y\right]$ y haciendo el algoritmo de la división. Podemos, pues $y - x^2$ es mónico en ese anillo. De este modo, dado que $f \in I(V)$, tenemos:

$$0 = f(x, x^2) = r(x) \;\; \forall x \in \overline{\mathbb{Q}}.$$

Luego $r = 0$, por lo que $f \in I$.

Definición 1.1.3. Una variedad afín V se dice *irreducible* si no es unión de dos variedades propias no vacías.

Proposición 1.1.4. *Una variedad afín V es irreducible si, y sólo si, su ideal asociado $I(V)$ es un ideal primo.*

En el ejemplo anterior, es claro que el polinomio $f = y - x^2$ es irreducible en $\overline{\mathbb{Q}}\left[x, y\right]$; con lo cual el ideal $I(V)$ es primo y V resulta ser una variedad afín irreducible.

Notemos que la noción de irreducible es coherente con lo que uno puede intuir. Por ejemplo, si tomamos el ideal $I = (y^2 - x^2) = ((y - x)(y + x))$; que claramente no es primo, la variedad afín V asociada es la unión de las rectas $y = x$ e $y = -x$; que serían las *componentes irreducibles* de V.

Dada una variedad afín V podemos asociarle un anillo, que es el de la siguiente definición.

Definición 1.1.5. Sea V una variedad afín. Se define el *anillo de coordenadas afín* de V como:

$$\overline{K}[V] = \overline{K}[\mathbf{x}]/I(V).$$

Observemos que si V es irreducible, $\overline{K}[V]$ es un dominio íntegro, pues $I(V)$ es primo. Esto nos permite tomar su cuerpo de fracciones. Al cuerpo de fracciones de $\overline{K}[V]$ lo llamamos el *cuerpo de funciones de* V y lo notamos $\overline{K}(V)$.

Si la variedad V irreducible es definida sobre K podemos considerar el cociente:

$$K[V] = K[\mathbf{x}]/I(V).$$

$K[V]$ se llama el *anillo de coordenadas K-racionales.* Su cuerpo de fracciones es el *cuerpo de funciones K–racionales* de V y se nota $K(V)$. Una interpretación que suele hacerse es decir que $\overline{K}[V]$ consta de las funciones de $\overline{K}[\mathbf{x}]$ definidas en V.

Observemos que si $f \in \overline{K}[V]$, f induce una función bien definida $f : V \to \overline{K}$, pues si $g \in \overline{K}[V]$ está en la misma clase que f, existe $h \in I(V)$ tal que $f = g+h$, y si $P \in V$, $f(P) = g(P)+h(P) = g(P)$.

Dada una variedad afín irreducible V tenemos entonces asociado a ella el cuerpo $\overline{K}(V)$. Hay, naturalmente, un morfismo de cuerpos inyectivo de $\overline{K}$ en $\overline{K}(V)$. Podemos preguntarnos acerca del grado de trascendencia de esa extensión. Precisamente ese grado será un número asociado a V y tendrá el siguiente nombre.

Definición 1.1.6. Sea V una variedad afín irreducible. El grado de trascendencia de $\overline{K}(V)$ sobre $\overline{K}$ se llama la *dimensión* de V, y se nota $\dim(V)$.

Notar que $\dim(V)$ es siempre un número menor o igual que n. Por ejemplo, si $V = \mathbb{A}^n$, o sea, $I(V) = (0)$, $\dim(V) = n$. Si V es la variedad irreducible asociada a un ideal principal $I = (f)$, con f irreducible, $\dim(V) = n - 1$. Una forma de ver esto es la siguiente: no es difícil ver que, dado $f \in \overline{K}[\mathbf{x}]$, bajo un cambio lineal de coordenadas se puede suponer que f tiene la siguiente forma:

$$f(\mathbf{x}) = x_n^d + a_{d-1}x_n^{d-1} + \cdots + a_1x_n + a_0,$$

con

$$a_i \in \overline{K}[x_1, ..., x_{n-1}]\ ,\ \ 1 \leq i \leq d.$$

Entonces podemos pensar que:

$$\overline{K}(V) = Fracc\left(\overline{K}[\mathbf{x}]/(f)\right) = \overline{K}(\overline{x}_1, ..., \overline{x}_n) = \overline{K}(x_1, ..., x_{n-1})(x_n),$$

donde x_n satisface la ecuación $f(\mathbf{x}) = 0$. La notación *Fracc* se refiere al cuerpo de fracciones.

Por lo tanto $\overline{K}(x_1, ..., x_{n-1})(x_n)$ es algebraica sobre $\overline{K}(x_1, ..., x_{n-1})$. Luego, considerando la torre:

$$\begin{array}{c} \overline{K}(V) \\ | \\ \overline{K}(x_1, ..., x_{n-1}) \\ | \\ \overline{K} \end{array}$$

tenemos que:

$$trdeg_{\overline{K}}(\overline{K}(V)) = trdeg_{\overline{K}}(\overline{K}(x_1, ..., x_{n-1})) + trdeg_{\overline{K}(x_1,...,x_n)}(\overline{K}(V)) = (n-1) + 0 = n - 1.$$

Donde la notación $trdeg_E(F)$ significa el grado de trascendencia de la extensión de cuerpos F/E.

Vamos ahora a dar una noción de suavidad para las variedades afines. La definición que viene a continuación es bastante razonable:

Definición 1.1.7. Sea $V \in \mathbb{A}^n$ una variedad afín irreducible. Supongamos que $I(V) = (f_1, ..., f_m)$. Sea $P \in V$. Diremos que V es *no singular* en P, o que P es un punto *no singular* de V, si la matriz de $m \times n$:

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

tiene rango $n - dim(V)$.

Si V es no singular en todos los puntos $P \in V$, diremos que V es *no singular*. Si V tiene algún punto singular diremos que V es *singular*.

Por ejemplo, si V es la variedad afín irreducible asociada a un ideal I principal, digamos $I = (f)$, con f irreducible, para un punto $P \in V$ se tiene:

$$P\, es\, singular \Leftrightarrow \frac{\partial f}{\partial x_i}(P) = 0\,,\, \forall\, i.$$

Ejemplo 1.1.8. $V_1 \subseteq \overline{\mathbb{Q}}^2$: $V_1 = V(y^2 - x^3 - x)$. Es fácil ver que, en efecto, $I(V_1) = (f)$, con $f = y^2 - x^3 - x$. Para ver si V_1 tiene puntos singulares debemos resolver el siguiente sistema:

$$\begin{cases} \frac{\partial f}{\partial x}(x, y) = -3x^2 - 1 & = 0 \\ \frac{\partial f}{\partial y}(x, y) = 2y & = 0 \end{cases}$$

cuyas soluciones son puntos $P = (x, y) \notin V_1$. Luego V_1 es no singular.

Ejemplo 1.1.9. $V_2 \subseteq \overline{\mathbb{Q}}^2$: $V_2 = V(y^2 - x^3 - x^2)$. Aquí tenemos que $I(V_2) = (f)$, con $f = y^2 - x^3 - x^2$. Veamos si V_2 tiene puntos singulares. El sistema que debemos mirar es ahora:

$$\begin{cases} \frac{\partial f}{\partial x}(x, y) = 3x^2 - 2x & = 0 \\ \frac{\partial f}{\partial y}(x, y) = 2y & = 0 \end{cases}$$

Este sistema sí tiene una solución para un punto de V_2 que es el punto $P = (0, 0)$. Es decir, $P = (0, 0)$ es punto singular de V_2 y, en particular, V_2 es una variedad singular. (Ver Figura 1.1)

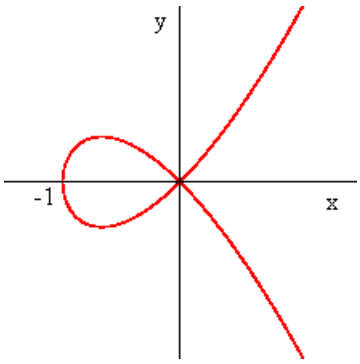


Figura 1.1: La variedad V_2 es singular en $P = (0, 0)$.

1.2. Variedades Proyectivas

Hasta ahora hemos visto subconjuntos de un espacio afín $\mathbb{A}^n$. Vamos a dar en esta parte las nociones básicas del espacio proyectivo; y haremos construcciones análogas a las que hicimos en el espacio afín.

La construcción del espacio proyectivo puede presentarse de diferentes formas. Vamos a mostrar un punto de vista algebraico y otro geométrico. Y más aún; para fijar las ideas empezaremos hablando de la recta proyectiva y el plano proyectivo, que no son más que casos particulares.

1.2.1. La Recta Proyectiva y el Plano Proyectivo

Empecemos con el punto de vista algebraico. Consideremos el plano afín $\mathbb{A}^2$ y definamos una relación de equivalencia en el conjunto $\mathbb{A}^2 - \{(0, 0)\}$. Concretamente definamos la *recta proyectiva* del siguiente modo:

$$\mathbb{P}^1 = \frac{\{(a, b) \in \mathbb{A}^2 - \{(0, 0)\}\}}{\sim}.$$

Donde:

$$(a, b) \sim (a', b') \Leftrightarrow \exists\, t \in \overline{K},\ t \neq 0\ :\ (a, b) = t(a', b').$$

O sea, son los puntos de $\mathbb{A}^2$ distintos del origen; identificando a aquellos que son múltiplos. Es decir, estamos identificando a todos los que estén sobre una misma recta de $\mathbb{A}^2$.

A una clase de equivalencia de $\mathbb{P}^1$ la notamos $[a : b]$, donde (a, b) es un representante de esa clase. Observemos que, con esta notación, tenemos:

$$[a : b] = [ta : tb]\,,\ \forall t \in \overline{K},\ t \neq 0.$$

Análogamente se construye el *plano proyectivo* definiendo la misma relación de equivalencia en $\mathbb{A}^3 - \{(0, 0, 0)\}$:

$$\mathbb{P}^2 = \frac{\{(a, b, c) \in \mathbb{A}^3 - \{(0, 0, 0)\}\}}{\sim}.$$

Donde:

$$(a,b,c) \sim (a',b',c') \Leftrightarrow \exists\, t \in \overline{K},\, t \neq 0 \,:\, (a,b,c) = t(a',b',c').$$

Y usamos la misma notación para las clases de equivalencia: $[a:b:c]$.

A los efectos teóricos no haría falta decir mucho más. Pero resulta interesante dar una perspectiva geométrica que suele aclarar un poco la idea de la construcción.

Veamos el caso del plano proyectivo. Situémonos en el plano afín $\mathbb{A}^2$ y consideremos una recta en él. Esa recta es un conjunto que consta de puntos de $\mathbb{A}^2$, y a ese conjunto de puntos le vamos a agregar uno más. Pero no otro punto de $\mathbb{A}^2$; sino un punto *en el infinito* o *punto impropio.* Un punto extra que representará la dirección de esa recta. Considerando todas las direcciones de rectas de $\mathbb{A}^2$ tenemos una familia de puntos en el infinito; y vamos a pensar al plano proyectivo intuitivamente como:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{Puntos\, en\, el\, infinito\} = \mathbb{A}^2 \cup \left\{Direcciones\, en\, \mathbb{A}^2\right\}.$$

En otras palabras, el plano proyectivo consiste en el plano afín $\mathbb{A}^2$ al cual le agregamos todos los puntos en el infinito, que son los que representan las direcciones de las rectas.

Una de las propiedades interesantes que surgen de esta perspectiva es la siguiente. Sabemos que en el plano afín $\mathbb{A}^2$, dadas dos rectas distintas, o bien se intersecan en un punto, o bien son paralelas y no se intersecan. Sin embargo, en $\mathbb{P}^2$, cualesquiera dos rectas distintas **siempre** se intersecan en un punto. En efecto, si no son paralelas estamos en el caso conocido de $\mathbb{A}^2$. Y si son paralelas, el punto en el que se intersecan es en ese punto impropio que tienen ambas: como tienen la misma dirección, tienen el mismo punto impropio, que es justamente el punto en común de ambas.

Ahora sí tratemos de formalizar la perspectiva geométrica. Dada una recta en $\mathbb{A}^2$, digamos de ecuación (vectorial):

$$\mathbb{L} \,:\, \lambda(a,b) + (a_0,b_0)\,;\, (a,b) \neq (0,0);$$

la dirección está dada por el vector (a,b). Y cualquier vector de la forma (ta,tb), para $t \neq 0$, representa la misma dirección. De manera que podemos asociar las direcciones en $\mathbb{A}^2$ con los vectores no nulos, identificando a aquellos que sean múltiplos. Notar que esto que estamos diciendo no es más que la construcción algebraica que hicimos de $\mathbb{P}^1$. En definitiva, esa familia de puntos impropios que le agregamos a $\mathbb{A}^2$ es la recta proyectiva $\mathbb{P}^1$. Con lo cual, estamos diciendo que:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1;$$

considerando a esta unión como una unión disjunta.

Veamos que las dos construcciones de $\mathbb{P}^2$, la algebraica y la geométrica, son compatibles. En efecto, hay una correspondencia biunívoca entre ambas, que es la siguiente:

Dado un punto de $\mathbb{P}^2 = \frac{\{(a,b,c)\}}{\sim}$, digamos $[a:b:c]$, tenemos dos posibilidades, que son $c = 0$ o $c \neq 0$. Si $c \neq 0$, $[a:b:c] = \left[\frac{a}{c} : \frac{b}{c} : 1\right]$; y lo asociamos entonces al punto $(\frac{a}{c}, \frac{b}{c}) \in \mathbb{A}^2$. Si $c = 0$, a $[a:b:0]$ lo asociamos al punto $[a:b] \in \mathbb{P}^1$.

Recíprocamente, dado un punto de $\mathbb{A}^2 \cup \mathbb{P}^1$, también tenemos dos posibilidades. Si el punto está en $\mathbb{A}^2$, es de la forma (a, b), y lo asociamos al punto $[a : b : 1] \in \mathbb{P}^2$. Si el punto está en $\mathbb{P}^1$, es de la forma $[a : b]$, y lo asociamos al punto $[a : b : 0] \in \mathbb{P}^2$.

$$\begin{array}{ccc} \mathbb{P}^2 & \longleftrightarrow & \mathbb{A}^2 \cup \mathbb{P}^1 \\ [a : b : c] & \longrightarrow & \begin{cases} \left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{A}^2 & si\ c \neq 0 \\ [a : b] \in \mathbb{P}^1 & si\ c = 0 \end{cases} \\ \\ [a : b : 1] & \longleftarrow & (a, b) \in \mathbb{A}^2 \\ [a : b : 0] & \longleftarrow & [a : b] \in \mathbb{P}^1 \end{array}$$

Es sencillo verificar que estas correspondencias son recíprocas.

Tratemos de ver qué nos dice esta biyección. Una manera de interpretarla es decir que $\mathbb{P}^2$ tiene una parte afín y una parte *en el infinito.* La parte afín corresponde a los puntos $[a : b : c]$ tales que $c \neq 0$. Pero sabemos que en tal caso $[a : b : c] = \left[\frac{a}{c} : \frac{b}{c} : 1\right]$; con lo cual podemos asumir que $c = 1$. De modo que la parte afín de $\mathbb{P}^2$ la integran los puntos de la forma $[a : b : 1]$. Y la parte en el infinito serán los demás, o sea, los de la forma $[a : b : 0]$.

Es natural preguntarse si el rol de c no puede ocuparlo a o b. La respuesta es afirmativa. La elección de c no es para nada canónica sino que es arbitraria. Se puede hacer exactamente el mismo proceso haciendo la distinción que hicimos de los puntos respecto de cualquiera de las otras variables. Luego haremos esto con detalle.

De esta manera, al trabajar en $\mathbb{P}^2$, si nos limitamos a mirar los puntos de la forma $[a : b : 1]$, es como si estuviéramos en $\mathbb{A}^2$, y podemos pensar que estamos en el plano afín. Luego formalizaremos un poco esta idea también.

Antes de pasar a la construcción del espacio proyectivo en general, digamos una cosa más. Ahora que pensamos a $\mathbb{P}^2$ como $\mathbb{A}^2 \cup \mathbb{P}^1$; es decir, agregarle a $\mathbb{A}^2$ la recta $\mathbb{P}^1$, podemos ser todavía más precisos con eso de que cualesquiera dos rectas distintas de $\mathbb{P}^2$ se intersecan en un punto. Porque ahora podemos considerar a $\mathbb{P}^1$ como una de las rectas de $\mathbb{P}^2$; o sea, la recta del infinito, o la recta de los puntos impropios. Y esta recta también cortará a cualquier otra recta $\mathbb{L} \subseteq \mathbb{P}^2$ en un punto exactamente; que será justamente el punto del infinito de $\mathbb{L}$; el punto asociado a su dirección.

Ahora sí que, tal vez la idea de la construcción está un poco más clara, pasemos a la definición del espacio proyectivo en general, que no es más que generalizar esto a dimensión n.

1.2.2. El Espacio Proyectivo

Definición 1.2.1. Sea K un cuerpo perfecto y $\overline{K}$ una clausura algebraica fija. El *espacio proyectivo* sobre K de dimensión n es:

$$\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = \frac{\left\{(X_0, ..., X_n) \in \mathbb{A}^{n+1} - \{(0, ..., 0)\}\right\}}{\sim}.$$

Donde:

$$(X_0, ..., X_n) \sim (Y_0, ..., Y_n) \Leftrightarrow \exists\, t \in \overline{K},\, t \neq 0, :\, (X_0, ..., X_n) = t(Y_0, ..., Y_n)$$

A una clase de equivalencia de $\mathbb{P}^n$ la notamos $[X_0 : \cdots : X_n]$, si $(X_0, ..., X_n)$ es un representante; y a las clases las llamamos *coordenadas homogéneas.* En seguida aclararemos la razón por la cual ahora usamos letras mayúsculas.

El conjunto de puntos K-*racionales* en $\mathbb{P}^n$ es:

$$\mathbb{P}^n(K) = \{[X_0 : \cdots : X_n] \in \mathbb{P}^n \,:\, X_i \in K,\ \ 0 \leq i \leq n\}\,.$$

Más precisamente, son aquellas clases $[X_0 : \cdots : X_n]$ para las cuales existe un representante con todas sus coordenadas en K.

Así como observamos en el caso $n = 2$, podemos pensar que $\mathbb{P}^n$ consta de una parte afín y una parte en el infinito. La parte afín decíamos antes que era la de los puntos de la forma $[a : b : c]$, con $c \neq 0$. Ahora diremos que la parte afín será la que conforman los puntos de la forma $[X_0 : \cdots : X_n]$ con $X_n \neq 0$.

Como dijimos antes, el rol de X_n puede ocuparlo algún otro X_i. Vamos ahora a formalizar un poco la idea de que al espacio proyectivo le podemos mirar su parte afín. Podemos pensar que $\mathbb{P}^n$ contiene varias copias de $\mathbb{A}^n$ considerando, para cada $1 \leq i \leq n$, la inclusión:

$$\begin{array}{rccl} \phi_i : & \mathbb{A}^n & \to & \mathbb{P}^n \\ & (y_1, ..., y_n) & \to & [y_1 : y_2 : \cdots : y_{i-1} : 1 : y_{i+1} : \cdots : y_n] \end{array}$$

Consideremos, dentro de $\mathbb{P}^n$, el conjunto:

$$U_i = \{P = [x_0 : \cdots : x_n] \,:\, x_i \neq 0\}\,,$$

que no es más que el complemento del hiperplano de $\mathbb{P}^n$ de ecuación $X_i = 0$. Podemos definir en U_i una *vuelta* para ϕ_i dada por:

$$\begin{array}{rccl} \phi_i^{-1} : & U_i & \to & \mathbb{A}^n \\ & [x_0 : \cdots : x_n] & \to & \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\right) \end{array}$$

De esta manera podemos trabajar con la noción de que $\mathbb{P}^n$ contiene copias de $\mathbb{A}^n$ de un modo más preciso. Concretamente, según convenga eventualmente, tomaremos *alguna* parte afín de $\mathbb{P}^n$, que será alguno de los U_i, vistos como copias de $\mathbb{A}^n$. Apuntando a los efectos puramente prácticos, ese proceso de *afinización* de $\mathbb{P}^n$ consistirá en considerar los puntos de la forma $[X_0 : \cdots : X_n] \in \mathbb{P}^n$ con $X_i \neq 0$. En tal caso:

$$[X_0 : \cdots : X_n] = \left[\frac{X_0}{X_i} : \cdots : \frac{X_{i-1}}{X_i} : 1 : \frac{X_{i+1}}{X_i} : \cdots : \frac{X_n}{X_i}\right],$$

y trabajaremos con los puntos *afines* $(x_0, ..., x_{i-1}, x_{i+1}, ..., x_n) \in \mathbb{A}^n$. Donde estamos haciendo la identificación:

$$x_0 = \frac{X_0}{X_i}, ...,\ x_{i-1} = \frac{X_{i-1}}{X_i},\ x_{i+1} = \frac{X_{i+1}}{X_i}, ...,\ x_n = \frac{X_n}{X_i}.$$

He ahí el por qué de la notación con letras mayúsculas para las coordenadas homogéneas; para distinguirlas de las coordenadas afines, que las notamos con minúsculas.

Nuestro objetivo ahora es, así como hicimos en el caso afín, definir las variedades en este nuevo espacio. Para ello necesitamos trabajar con el anillo de polinomios. Pero observemos lo siguiente. Supongamos que tenemos el polinomio $f \in \overline{\mathbb{Q}}[x, y]$, $f(x, y, z) = 2x + y^2 - z$. Tratemos de evaluar a f en puntos de $\mathbb{P}^2$. Por ejemplo, $f([1 : 2 : 1]) = 5$. Pero resulta que $[1 : 2 : 1] = [2 : 4 : 2]$, y $f([2 : 4 : 2]) = 18$. Tenemos que $f([1 : 2 : 1]) \neq f([2 : 4 : 2])$; aunque $[1 : 2 : 1] = [2 : 4 : 2]$. Esto nos dice que el polinomio f no está bien definido en $\mathbb{P}^2$. De este modo estamos obligados a limitarnos a trabajar con una familia de polinomios más restringida.

Definición 1.2.2. Sea $F \in \overline{K}[x_0, ..., x_n]$. Decimos que F es un polinomio *homogéneo* de grado d si:

$$F(tx_0, ..., tx_n) = t^d F(x_0, ..., x_n), \ \forall t \in \overline{K}.$$

Aquí tenemos algunos ejemplos de polinomios homogéneos: $F \in \overline{\mathbb{Q}}[x, y]$, $F(x, y) = 3xy + x^2$. F es homogéneo de grado 2. $G \in \overline{\mathbb{Q}}[x, y, z]$, $G(x, y, z) = xy^2 - 4x^2z + x^3 + 2xyz$. G es homogéneo de grado 3.

En otras palabras, un polinomio F es homogéneo de grado d si, y sólo si, cada uno de sus monomios tiene grado total d.

Los polinomios homogéneos son los que van a permitir definir las variedades en $\mathbb{P}^n$:

Observación 1.2.3. Si $F \in \overline{K}[x_0, ..., x_n]$ es un polinomio homogéneo (de cualquier grado):

$$F(x_0, ..., x_n) = 0 \Leftrightarrow F(tx_0, ..., tx_n) = 0, \ \forall t \in \overline{K}.$$

1.2.3. Variedades Proyectivas

Ahora sí ya estamos en condiciones de definir las variedades proyectivas. La construcción no va a ser más que copiar lo que hicimos en el caso afín, pero ahora en el contexto de $\mathbb{P}^n$.

Diremos primero que a los ideales $I \subseteq \overline{K}[x_0, ..., x_n]$ generados por polinomios homogéneos los llamaremos *ideales homogéneos.*

Igual que como hicimos en el caso afín, a cada $I \subseteq \overline{K}[\mathbf{x}] = \overline{K}[x_0, ..., x_n]$ ideal homogéneo, podemos asociarle un conjunto de $\mathbb{P}^n$ dado por:

$$V(I) = \{P \in \mathbb{P}^n : \ f(P) = 0, \ \forall f \in I \ homogéneo\}.$$

Notemos que esta definición tiene sentido gracias a la Observación 1.2.3

Definición 1.2.4. Llamamos *variedad proyectiva* a un conjunto de la forma $V(I)$ para algún ideal $I \subseteq \overline{K}[\mathbf{x}]$ homogéneo.

Dada una variedad proyectiva V, el ideal homogéneo $I(V) \subseteq \overline{K}[\mathbf{x}]$ que la define será el generado por el conjunto:

$$\left\{f \in \overline{K}[\mathbf{x}] \ : \ f \ homogéneo \ y \ f(P) = 0, \ \forall P \in V\right\}.$$

Diremos que V es *definida sobre* K si $I(V)$ puede generarse con polinomios homogéneos de $K[\mathbf{x}]$.

Análogamente al caso afín tenemos la siguiente definición.

Definición 1.2.5. Una variedad proyectiva V se dice *irreducible* si su ideal homogéneo $I(V)$ es un ideal primo de $\overline{K}[\mathbf{x}]$.

Como vimos, al espacio afín $\mathbb{A}^n$ lo podemos pensar metido en $\mathbb{P}^n$; o podemos decir que $\mathbb{P}^n$ contiene copias de $\mathbb{A}^n$. Es esperable que algo similar ocurra entre las variedades afines y proyectivas. Vamos a ver esto empezando con un ejemplo. Trabajemos en $\overline{\mathbb{Q}}$. Consideremos la variedad proyectiva $V_F \subseteq \mathbb{P}^2$ dada por:

$$V_F : Y^2Z - X^3 - Z^3 = 0.$$

O sea, el ideal de V_F es $I(V_F) = (F)$; donde $F(X, Y, Z) = Y^2Z - X^3 - Z^3$. (Notar que todo está bien definido dado que F es homogéneo). Si en $\mathbb{P}^2$ consideramos la afinización $Z = 1$; es decir, nos limitamos a mirar los puntos $[X : Y : Z]$ con $Z \neq 0$; usando la misma notación de antes (mayúsculas vs. minúsculas) estamos considerando los puntos de $\mathbb{A}^2$ de coordenadas afines (x, y). Donde $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$. En tal caso, los puntos de V_F tales que $Z \neq 0$, se corresponden con los puntos $(x, y) \in \mathbb{A}^2$ que satisfacen la ecuación:

$$y^2 - x^3 - 1 = 0.$$

Si llamamos $f(x, y) = y^2 - x^3 - 1$, tenemos la variedad afín $V_f \subseteq \mathbb{A}^2$ cuyo ideal es $I(V_f) = (f)$. Lo que vemos es que V_f es la variedad afín de $\mathbb{A}^2$ que consta de los puntos *afines* de V_F según la afinización $Z = 1$. Si miramos la relación entre los polinomios F y f es claro que se tiene:

$$f(x, y) = F(X, Y, 1).$$

Esto es justamente lo que hacemos con los puntos de $\mathbb{P}^2$ cuando los afinizamos, pero ahora con los polinomios. Precisamente, el proceso de afinizar los puntos $[X : Y : Z]$ tomando $Z = 1$; a nivel polinomios se traduce en *deshomogenizar.* O sea, decimos que f es la *deshomogenización* de F en Z si $f(x, y) = F(X, Y, 1)$.

Pero sabemos que el papel de Z puede tomarlo otra de las variables; digamos por ejemplo X. Si afinizamos con respecto a X estamos considerando los puntos de $(y, z) \in \mathbb{A}^2$, con $y = \frac{Y}{X}$, $z = \frac{Z}{X}$. En este caso al deshomogenizar F obtenemos:

$$f(y, z) = F(1, Y, Z) = y^2z - 1 - z^3.$$

Y la variedad afín $V_f \subseteq \mathbb{A}^2$ es la generada por el ideal $I(V_f) = (y^2z - 1 - z^3)$.

Hemos observado en definitiva que a la variedad proyectiva V_F podemos *mirarle* sus partes afines. O sea, podemos considerar variedades afines (3 de ellas precisamente) que resultan ser las que constan de los puntos afines de V_F en cada una de las afinizaciones de $\mathbb{P}^2$. Estas variedades afines no son más que una parte del todo, que es la variedad proyectiva V_F. ¿Y cómo obtenemos esas variedades $V_f \subseteq \mathbb{A}^2$? Deshomogenizando el polinomio F con respecto a la variable correspondiente.

Vamos ahora a hacer la construcción recíproca. Supongamos que empezamos con la variedad afín $V_f \subseteq \mathbb{A}^2$ dada por:

$$V_f \,:\, y^2 - x^3 - 1 = 0.$$

Donde, como antes, llamamos $f(x,y) = y^2 - x^3 - 1$ y V_f es la variedad asociada al ideal $I(V_f) = (f)$. Así como antes estábamos en $\mathbb{P}^2$ y, como $\mathbb{P}^2$ contiene copias de $\mathbb{A}^2$, mirábamos los puntos de la variedad que estaban sobre una de esas copias; ahora estamos en $\mathbb{A}^2$, y pensémoslo incluido en $\mathbb{P}^2$. Precisamente, miremos a las coordenadas (x,y) de $\mathbb{A}^2$ como la parte afín de coordenadas $[X:Y:Z]$ de $\mathbb{P}^2$, afinizando en Z. Esto es:

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

Así tenemos la correspondencia:

$$(x,y) \longrightarrow \left[\frac{X}{Z} : \frac{Y}{Z} : 1\right] = [X:Y:Z]\,.$$

Mirando la ecuación $f(x,y) = 0$ que teníamos, con las nuevas coordenadas se convierte en:

$$\frac{Y^2}{Z^2} - \frac{X^3}{Z^3} - 1 = 0.$$

Y multiplicando todo por Z^3 para limpiar los denominadores nos queda:

$$Y^2Z - X^3 - Z^3 = 0.$$

Así obtenemos el polinomio $F(X,Y,Z) = Y^2Z - X^3 - Z^3$ que es homogéneo y define entonces una variedad proyectiva; que es la que teníamos en un principio.

De nuevo, la forma en que pensamos a las coordenadas (x,y) como la parte afín de coordenadas homogéneas, no es la única. Arbitrariamente elegimos una. También se podía haber hecho la construcción pensando que las coordenadas (x,y) son la parte afín de coordenadas homogéneas del tipo $[X:Z:Y]$ o $[Z:X:Y]$.

De este modo, a la variedad afín $V_f \subseteq \mathbb{A}^2$ pudimos asociarle la variedad proyectiva $V_F \subseteq \mathbb{P}^2$. Para ello hicimos el proceso inverso de lo que llamamos antes deshomogenización. En este caso pasamos de coordenadas afines a coordenadas homogéneas agregando una variable extra. Y a nivel polinomios, a f le hicimos un proceso que llamamos *homogenización*, que consistió en definir F del siguiente modo:

$$F(X,Y,Z) = Z^3 f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

Es bastante claro que ambas construcciones son recíprocas. Pues si a V_F la afinizamos respecto de Z obtenemos V_f. Y si a V_f le aplicamos el proceso de homogenización de sus coordenadas volvemos a obtener V_F.

Aquí hay un detalle a tener en cuenta. Cuando uno mira la parte afín de una variedad proyectiva puede tener la *mala suerte* de que esa parte afín es vacía. Por ejemplo, si a la variedad proyectiva de $\mathbb{P}^3$ dada por:

$$V_F \,:\, F(X,Y,Z) = Z = 0,$$

la afinizáramos respecto de Z; la variedad afín resultante sería vacía. Pues en esa afinización justamente no hay puntos $[X : Y : Z]$ que satisfagan $Z = 0$. Por esto es que hay que tener el cuidado de afinizar respecto a una variable de manera de obtener una variedad afín no vacía. Sobre esto volveremos en seguida.

Una manera de interpretar este proceso es decir que V_f son los **puntos afines** de V_F, respecto de la afinización correspondiente; y que los puntos de $V_F - V_f$ son los **puntos en el infinito** de V_f; también respecto a la forma en que miramos a las coordenadas de V_f como la parte afín de ciertas coordenadas homogéneas. Por ejemplo, si la afinización consistió en pasar de coordenadas $[X : Y : Z]$ a coordenadas (x, y); los puntos en el infinito de V_f son exactamente los puntos de V_F de la forma $[X : Y : 0]$. A continuación vamos a resumir y a generalizar todo esto.

1.2.4. Variedades afines $\longleftrightarrow$ Variedades proyectivas

• ($\longleftarrow$) Sea $V \subseteq \mathbb{P}^n$ una variedad proyectiva con ideal homogéneo $I(V) \subseteq \overline{K}[\mathbf{X}]$. Consideremos, para algún $1 \leq i \leq n$ fijo, la función ϕ_i que definimos en **2.2**. Llamemos $V \cap \mathbb{A}^n = \phi_i^{-1}(V \cap U_i)$. Entonces $V \cap \mathbb{A}^n \subseteq \mathbb{A}^n$ es una variedad afín con ideal $I(V \cap \mathbb{A}^n) \subseteq \overline{K}[\mathbf{x}]$ dado por:

$$I(V \cap \mathbb{A}^n) = \{f(x_0, ..., x_{i-1}, x_{i+1}, ..., x_n) = F(x_0, ..., x_{i-1}, 1, x_{i+1}, ..., y_n) \ : \ F(X_0, ..., X_n) \in I(V)\}.$$

Donde notamos, como antes, $x_0 = \frac{X_0}{X_i}$, ..., $x_n = \frac{X_n}{X_i}$.

• ($\longrightarrow$) Sea $f \in \overline{K}[\mathbf{x}]$ y fijemos algún $1 \leq i \leq n$. Definimos $F \in \overline{K}[\mathbf{X}]$ como:

$$F(X_0, ..., X_n) = X_i^d f\left(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right);$$

donde $d = deg(f)$ es el mínimo entero que hace falta para limpiar denominadores. Decimos que F es la *homogenización* de f con respecto a X_i.

Sea entonces $V \subseteq \mathbb{A}^n$ una variedad afín con ideal $I(V) \subseteq \overline{K}[\mathbf{x}]$. Consideramos una inclusión:

$$\phi_i : \mathbb{A}^n \longrightarrow \mathbb{P}^n.$$

Diremos que la *clausura proyectiva de V respecto de i* es la variedad proyectiva $\overline{V}$ cuyo ideal homogéneo $I(\overline{V})$ está generado por:

$$\{F(X_0, ..., X_n) \ : \ F \text{ es la homogenización de } f \text{ respecto a } X_i \text{ para algún } f \in I(V)\}.$$

Las garantías de que estas construcciones se comportan como uno quisiera nos las da el siguiente resultado: (Ver [9], Capítulo I, Proposición 2.6.)

Proposición 1.2.6. *a) Sea V una variedad afín. Entonces $\overline{V}$ es una variedad proyectiva y $V = \overline{V} \cap \mathbb{A}^n$.*

b) Sea V una variedad proyectiva. Entonces $V \cap \mathbb{A}^n$ es una variedad afín y:

$$V \cap \mathbb{A}^n = \emptyset \ \text{ o bien } \quad V = \overline{V \cap \mathbb{A}^n}.$$

c) Si una variedad afín (respectivamente proyectiva) V es definida sobre K, entonces $\overline{V}$ (respectivamente $V \cap \mathbb{A}^n$) es definida sobre K.

d) Toda variedad afín V puede ser identificada con una única variedad proyectiva, que es su clausura $\overline{V}$; y los puntos de $\overline{V} - V$ son los puntos en el infinito de V.

Algo bastante inmediato es el hecho que, dada una variedad proyectiva V, siempre existe una afinización $V \cap \mathbb{A}^n$ que es no vacía.

Notemos que la unicidad del punto *d)* no se aplica en el proceso inverso. Es decir, dada una variedad proyectiva V hay varias variedades afines que le podemos asociar; que son las que corresponden a cada una de las afinizaciones de V con respecto a las diferentes variables.

Esta proposición nos dice que en cierta forma las variedades afines y las proyectivas están en correspondencia, y también lo están los polinomios de sus ideales. En muchos casos suele ser más cómodo trabajar con los polinomios deshomogenizados, y esto lo podemos hacer ya que en los puntos afines de una variedad proyectiva, ambos polinomios coinciden.

Hay una perspectiva topológica de estas ideas que es bastante interesante. Sólo nos vamos a limitar a mencionarla al pasar. Una propiedad que satisface el espacio proyectivo $\mathbb{P}^n$ es la de ser un espacio topológico *compacto*. De esta manera, cuando uno tiene una variedad afín y le calcula una clausura proyectiva $\overline{V}$; lo que está haciendo es un proceso de *compactificación* de V.

Lo que nos falta hacer con las variedades proyectivas es dar las definiciones análogas al caso afín de anillo de coordenadas, dimensión, etc. Pero veremos que las nuevas definiciones no son más que reducciones al caso afín.

Definición 1.2.7. Sea V una variedad proyectiva irreducible.

a) Elijamos una afinización $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $V \cap \mathbb{A}^n \neq \emptyset$. Definimos la *dimensión* de V como la dimensión de $V \cap \mathbb{A}^n$.

b) También con una afinización $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $V \cap \mathbb{A}^n \neq \emptyset$, definimos el *anillo de coordenadas* de V y el *cuerpo de funciones* de V respectivamente como:

$$\overline{K}\,[V \cap \mathbb{A}^n] \;\; y \;\; \overline{K}(V \cap \mathbb{A}^n).$$

Es decir, el anillo de coordenadas y el cuerpo de funciones de $V \cap \mathbb{A}^n$.

c) Sea $P \in V$. Elijamos una afinización $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $P \in V \cap \mathbb{A}^n$. Decimos que V es *no singular* en P, o que P es un punto *no singular* de P, si $V \cap \mathbb{A}^n$ es no singular en P.

Se verifica que estas definiciones son consistentes; es decir, que no dependen de la afinización. En el caso del anillo de coordenadas y el cuerpo de funciones las construcciones resultan ser canónicamente isomorfas.

Observación 1.2.8. El cuerpo de funciones de una variedad proyectiva V también puede describirse como el conjunto de las funciones racionales $F(\mathbf{X}) = \frac{f(\mathbf{X})}{g(\mathbf{X})}$ tales que:

1) f y g son polinomios homogéneos del mismo grado.

2) $g \notin I(V)$.

3) $\frac{f}{g} \sim \frac{f'}{g'}$ si $fg' - f'g \in I(V)$.

Esto es consecuencia inmediata del paso de coordenadas afines a homogéneas. Tomemos una variedad proyectiva $V \subseteq \mathbb{P}^2$ y una afinización tal que $V \cap \mathbb{A}^2 \neq \emptyset$. Dado un elemento cualquiera f en el cuerpo de funciones de $V \cap \mathbb{A}^2$, cuando lo pasamos a coordenadas homogéneas adquiere efectivamente la escritura que dice esta observación.

Pongamos un ejemplo sencillo para visualizar esto. Consideremos la misma variedad V que ya hemos usado antes, la definida por la ecuación afín:

$$V \,:\, y^2 - x^3 - 1 = 0.$$

O por la ecuación homogénea:

$$V \,:\, Y^2Z - X^3 - Z^3 = 0.$$

Sea f el polinomio:

$$f(x, y) = 1 - 2x + 3xy^2.$$

f es un polinomio del cuerpo de funciones de la variedad afín; y si lo escribimos en coordenadas homogéneas nos queda:

$$F(X, Y, Z) = 1 - 2\frac{X}{Z} + 3\frac{XY^2}{Z^3} = \frac{Z^3 - 2XZ^2 + 3XY^2}{Z^3};$$

que es efectivamente un cociente de polinomios homogéneos de igual grado. Lo mismo si partimos de un elemento f del cuerpo de funciones de $V \cap \mathbb{A}^2$ que ya es en sí un cociente de polinomios. Por ejemplo, sea f el siguiente elemento:

$$f(x, y) = \frac{2 - y + 3x^2y + y^4}{5xy + x^3}.$$

Si lo pasamos a coordenadas homogéneas obtenemos:

$$F(X, Y, Z) = \frac{2 - \frac{Y}{Z} + 3\frac{X^2Y}{Z^3} + \frac{Y^4}{Z^4}}{5\frac{XY}{Z^2} + \frac{X^3}{Z^3}} = \frac{2Z^4 - YZ^3 + 3X^2YZ + Y^4}{5XYZ^2 + X^3Z}.$$

Esta escritura es la que permite la evaluación en cualquier punto de V; ya sean puntos afines o puntos en el infinito. Obviamente que también podemos hacer el proceso inverso y pasar a coordenadas afines haciendo $Z = 1$.

Notar que no hicimos un proceso de homogenización. Sólo lo escribimos en coordenadas homogéneas. O sea, no le limpiamos los denominadores para que quedara un polinomio; porque estamos con un elemento del **cuerpo de funciones**, y no del **anillo de coordenadas**.

Como en el caso afín, si $F \in \overline{K}(V)$, F induce una función bien definida $F : V \longrightarrow \overline{K}$. Esto se ve muy claro si describimos $\overline{K}(V)$ como en la observación última.

Observemos otra cosa. Como las variedades afines están en correspondencia con las proyectivas, y sus ideales también; muchas veces solemos considerar un polinomio cualquiera y pensarlo dentro

del anillo de coordenadas de una variedad proyectiva; y a la hora de evaluarlo en algún punto del infinito, tomamos su homogenización.

Ya tenemos los conceptos básicos de las variedades proyectivas. A continuación hablaremos de las funciones que se pueden definir entre ellas.

1.2.5. Funciones entre variedades proyectivas

Definición 1.2.9. Sean V_1 y V_2 dos variedades proyectivas en $\mathbb{P}^n$. Una *función racional* de V_1 a V_2 es una función de la forma:

$$\begin{array}{ccc} \phi : V_1 & \longrightarrow & V_2 \\ & \phi = [f_0 : \cdots : f_n] & \end{array}$$

donde $f_0, ..., f_n \in \overline{K}(V_1)$ verifican que, para cada $P \in V_1$ en el que $f_0, ..., f_n$ están definidos, se tiene:

$$\phi(P) = [f_0(P) : \cdots : f_n(P)] \in V_2.$$

ϕ se dice *definida sobre* K si existe $\lambda \in \overline{K}$, $\lambda \neq 0$, tal que $\lambda f_i \in K(V_1)$, $0 \leq i \leq n$.

Observemos que $[f_0 : \cdots : f_n]$ y $[\lambda f_0 : \cdots : \lambda f_n]$ definen la misma función, pues la clase de un punto de $\mathbb{P}^n$ no se altera al multiplicar sus coordenadas por una constante no nula. Además se cumple que:

$$\phi(\lambda P) = \phi(P), \ \forall P \in V_1.$$

Según la definición una función racional no necesariamente está definida en todos los puntos de V_1. Sin embargo ese problema puede solucionarse en muchos casos. Supongamos que $\phi = [f_0 : \cdots : f_n]$ y que f_0 no está definida en $P \in V_1$. Esto significa que P anula el denominador de f_0; y podemos suponer que P no anula al numerador de f_0. Supongamos además que el resto de las f_i sí están definidas en P . Si llamamos g_0 al denominador de f_0 podemos decir lo siguiente:

$$\phi = [f_0 : \cdots : f_n] = [g_0 f_0 : \cdots : g_0 f_n] .$$

De este modo, la *nueva* f_0 sí está definida en P. Y el resto de las funciones también. Y más aún, $(g_0 f_0)(P) \neq 0$. Con lo cual, $[(g_0 f_0)(P) : \cdots : (g_0 f_n)(P)] \in \mathbb{P}^n$ está bien definido; pues, no todas sus coordenadas son nulas.

Esto que hicimos de resolver el problema que se tenía en P lo podemos generalizar y motiva la siguiente definición.

Definición 1.2.10. Una función racional $\phi = [f_0 : \cdots : f_n] : V_1 \longrightarrow V_2$ se dice *regular* o *definida* en $P \in V_1$ si existe $g \in \overline{K}(V_1)$ tal que:

a) gf_i está definida en P para $0 \leq i \leq n$.

b) Existe j, $0 \leq j \leq n$, tal que $(gf_j)(P) \neq 0$.

En tal caso se tiene:

$$\phi(P) = [(gf_0)(P) : \cdots : (gf_n)(P)]\,.$$

Una función racional que es regular en todo punto de V_1 se llama *morfismo.*

Hay que decir que lamentablemente no siempre existe esa función g para que la función racional ϕ sea regular. Si la variedad V_1 es irreducible y de dimensión 1 veremos que sí existe; pero en general no.

Observación 1.2.11. Dado un morfismo $\phi = [f_0 : \cdots : f_n]$, uno puede limpiar denominadores multiplicando a todas las coordenadas por un polinomio homogéneo adecuado, con lo cual, siempre podemos suponer que cualquier función racional ϕ es de la forma $\phi = [f_0' : \cdots : f_n']$, con los f_i' polinomios homogéneos de igual grado.

Como es de esperar, tenemos la noción de isomorfismo:

Definición 1.2.12. Dos variedades V_1 y V_2 se dicen *isomorfas* si existen morfismos:

$$\phi : V_1 \longrightarrow V_2 \;\; y \;\; \psi : V_2 \longrightarrow V_2,$$

tales que $\psi \circ \phi$ y $\phi \circ \psi$ son las identidades de V_1 y V_2 respectivamente.

V_1 y V_2 son *isomorfas sobre* K si ϕ y ψ pueden definirse sobre K.

Observación 1.2.13. Si $\phi : V_1 \longrightarrow V_2$ es un isomorfismo definido sobre K y usamos la notación $V(K) = V \cap \mathbb{P}^n(K)$, entonces ϕ identifica a los conjuntos $V_1(K)$ y $V_2(K)$. Por lo tanto sus estructuras algebraicas (que veremos en el siguiente capítulo) serán similares.

Ejemplo 1.2.14. Trabajemos en $\overline{\mathbb{Q}}$. Sea $V \subseteq \mathbb{P}^2$ dada por:

$$V \;:\; X^2 + Y^2 - Z^2 = 0.$$

Consideremos la función racional $\phi : V \longrightarrow \mathbb{P}^1$ definida como $\phi = [X + Z : Y]$. Recordemos la Observación 1.2.11 que nos permite asumir que las funciones racionales pueden escribirse de esta manera.

Claramente ϕ es regular en todos los puntos de V salvo, quizás, en $P = [1 : 0 : -1]$. Pues en el resto de los puntos de V, $[X + Z : Y] \in \mathbb{P}^1$ está bien definido ya que alguna de sus dos coordenadas es no nula. Sin embargo veamos que ϕ también es regular en $P = [1 : 0 : -1]$. En efecto:

$$X^2 - Z^2 \equiv -Y^2 (mod\, I(V)).$$

Con lo cual:

$$\phi = [X + Z : Y] = \left[X^2 - Z^2 : Y(X - Z)\right] = \left[-Y^2 : Y(X - Z)\right] = [-Y : X - Z]\,.$$

Luego, $\phi([1 : 0 : -1]) = [0 : 2] = [0 : 1] \in \mathbb{P}^1$. Es decir, ϕ también está definido en $[1 : 0 : -1]$, por lo que ϕ es un morfismo.

Notemos que, siguiendo con la notación de la Definición 1.2.10, la función $g \in \overline{\mathbb{Q}}(V)$ por la que multiplicamos a las coordenadas de ϕ para poder definir $\phi(P)$ es $g(X,Y,Z) = \frac{X-Z}{Y}$.

Si definimos $\psi : \mathbb{P}^1 \longrightarrow V$ como $\psi = \left[S^2 - T^2 : 2ST : S^2 + T^2\right]$ es fácil verificar que ψ es un morfismo que satisface que $\phi \circ \psi$ y $\psi \circ \phi$ son las identidades de V y $\mathbb{P}^1$ respectivamente; con lo cual $\psi = \phi^{-1}$ y ϕ es un isomorfismo.

Hay una noción un poco más débil que la de isomorfismo. Uno puede tener una función racional entre dos variedades V_1 y V_2 tal que exista una función racional de V_2 a V_1 que satisfaga que, en los puntos en los que ambas están definidas, las composiciones den la identidad. En otras palabras, si se restringen ambas funciones racionales a los puntos en los que ambas son morfismos; esas restricciones resultan ser isomorfismos. La definición precisa es la siguiente.

Definición 1.2.15. Sean V_1 y V_2 dos variedades proyectivas en $\mathbb{P}^n$. Una función racional $f : V_1 \longrightarrow V_2$ se dice *birracional* si existe otra función racional $g : V_2 \longrightarrow V_1$ tal que:

a) Si $P \in V_1$ es tal que $f(P)$ y $g(f(P))$ están definidos, entonces $g(f(P)) = P$.

b) Si $P \in V_2$ es tal que $g(P)$ y $f(g(P))$ están definidos, entonces $f(g(P)) = P$.

En tal caso se dice que las variedades V_1 y V_2 son *birracionalmente equivalentes*.

Si uno introduce una topología en $\mathbb{P}^n$, que no es la usual, hay una manera muy clara de interpretar lo que ocurre cuando dos variedades son birracionalmente equivalentes. Vamos a introducir esa topología en $\mathbb{P}^n$ del siguiente modo.

Definición 1.2.16. En el espacio proyectivo $\mathbb{P}^n$ se define la *Topología de Zariski* que está dada por la siguiente condición:

$$B \subseteq \mathbb{P}^n \text{ es un conjunto cerrado } \Leftrightarrow \text{ } B \text{ es una variedad proyectiva.}$$

Concretamente se define que los cerrados son las variedades proyectivas. Análogamente se puede trabajar en el espacio afín $\mathbb{A}^n$ y definir que los cerrados son las variedades afines.

Los abiertos en la topología de Zariski son entonces los complementos de las variedades. Intuitivamente, los conjuntos abiertos-Zariski en $\mathbb{P}^n$ son, en general, muy grandes; pues las variedades vienen dadas por ceros de polinomios.

Observemos qué pasa entonces si tenemos dos variedades birracionalmente equivalentes. Los puntos en los que las funciones birracionales no están definidas forman justamente una variedad. De manera que los puntos en los que sí están definidas son un abierto de cada una de las variedades respectivas y, por lo tanto, resulta que las variedades son isomorfas en ese abierto. Más aún; vale el razonamiento recíproco. Para ser precisos, tenemos la siguiente observación:

Observación 1.2.17. Sean V_1 y V_2 dos variedades proyectivas. Son equivalentes:

a) V_1 y V_2 son birracionalmente equivalentes.

b) Existen abiertos-Zariski $U_1 \subseteq V_1$ y $U_2 \subseteq V_2$ tales que U_1 y U_2 son isomorfos.

Demostración: a) $\Rightarrow$ b) ya lo comentamos antes. a) $\Rightarrow$ b) es claro. Si se tienen isomorfismos entre U_1 y U_2, extendiéndolos de alguna manera a V_1 y V_2 se tienen funciones birracionales. $\square$

Esto nos dice que, si bien es un concepto más débil que el de isomorfismo, si dos variedades son birracionalmente equivalentes, tienen mucho que ver; pues son isomorfas en un abierto, y los abiertos las cubren en gran medida.

Otra de las posibles situaciones es la siguiente. Podemos tener un **morfismo** $f : V_1 \longrightarrow V_2$ y una **función racional** (no necesariamente un morfismo) $g : V_2 \longrightarrow V_1$ tal que, en los puntos $P \in V_2$ en los que g esté definida, se tenga $f(g(P)) = P$. En tal caso lo vamos a definir así.

Definición 1.2.18. Un morfismo $f : V_1 \longrightarrow V_2$ se dice un *morfismo birracional* si existe una función racional $g : V_2 \longrightarrow V_1$ tal que, en los puntos en los que g está definida, se tiene $f(g(P)) = P$.

Notemos que el concepto de morfismo birracional es más fuerte que el de función birracional y más débil que el de isomorfismo. De hecho podemos resumir todo esto con el siguiente esquema:

$$\textit{isomorfismo} \Rightarrow \textit{morfismo birracional} \Rightarrow \textit{función birracional}$$

Ninguna de las flechas puede invertirse en general. De hecho vamos a ver un ejemplo clásico de un morfismo birracional que no es isomorfismo en el Capítulo 3 cuando definamos lo que es el Blow Up. Sin embargo, cuando las variedades involucradas son de dimensión 1 y no singulares, sí vamos a poder invertir las flechas. Esto lo veremos en la siguiente sección.

1.3. Curvas Algebraicas

En esta sección analizaremos un caso particular de variedades proyectivas que son las curvas.

Definición 1.3.1. Una *curva* $\mathcal{C} \subseteq \mathbb{P}^n$ es una variedad proyectiva irreducible de dimensión 1.

Dado que una curva sigue siendo una variedad proyectiva, y es irreducible, tenemos definidos para ella todos los conceptos que ya conocemos:

Definición 1.3.2. Sea $\mathcal{C}$ una curva.

a) Elijamos una afinización $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $\mathcal{C} \cap \mathbb{A}^n \neq \emptyset$. Definimos el *anillo de coordenadas* $\overline{K}[\mathcal{C}]$ de $\mathcal{C}$ y el *cuerpo de funciones* $\overline{K}(\mathcal{C})$ de $\mathcal{C}$ respectivamente como:

$$\overline{K}\left[\mathcal{C} \cap \mathbb{A}^n\right] \;\; y \;\; \overline{K}(\mathcal{C} \cap \mathbb{A}^n).$$

Donde, si llamamos $C = \mathcal{C} \cap \mathbb{A}^n$, entonces:

$$\overline{K}[C] = \overline{K}[\mathbf{x}]/I(C);$$

y $\overline{K}(C)$ es el cuerpo de funciones de $\overline{K}[C]$.

b) Sea $P \in \mathcal{C}$. Elijamos una afinización $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $P \in \mathcal{C} \cap \mathbb{A}^n$. Decimos que $\mathcal{C}$ es *no singular* en P, o que P es un punto *no singular* de $\mathcal{C}$, si $\mathcal{C} \cap \mathbb{A}^n$ es no singular en P.

Vamos a asociar a una curva $\mathcal{C}$ algunas estructuras algebraicas que vamos a utilizar a lo largo de todo el trabajo.

Definición 1.3.3. Sea $\mathcal{C} \subseteq \mathbb{P}^n$ una curva y sea $P \in \mathcal{C}$. Definimos el conjunto $\mathcal{M}_P \subseteq \overline{K}[\mathcal{C}]$ como:

$$\mathcal{M}_P = \left\{ f \in \overline{K}[\mathcal{C}] \,:\, f(P) = 0 \right\}.$$

Observación 1.3.4. $\mathcal{M}_P$ es un ideal maximal de $\overline{K}[\mathcal{C}]$.

En efecto, que es un ideal es claro. Para ver que es maximal basta observar que el morfismo de anillos:

$$\begin{aligned} \overline{K}[\mathcal{C}] &\longrightarrow \overline{K} \\ f &\longmapsto f(P) \end{aligned}$$

es sobreyectivo y su núcleo es exactamente $\mathcal{M}_P$. Con lo cual:

$$\overline{K}[\mathcal{C}]/\mathcal{M}_P \simeq \overline{K}.$$

Dado que $\mathcal{M}_P \subseteq \overline{K}[\mathcal{C}]$ es un ideal maximal, podemos localizar $\overline{K}[\mathcal{C}]$ en $\mathcal{M}_P$. Esa localización será una construcción que nos va a interesar.

Definición 1.3.5. Sea $\mathcal{C} \subseteq \mathbb{P}^n$ una curva y sea $P \in \mathcal{C}$. El *anillo local* de $\mathcal{C}$ en P es la localización de $\overline{K}[\mathcal{C}]$ en el ideal maximal $\mathcal{M}_P$; y lo notamos $\overline{K}[\mathcal{C}]_P$.

Podemos dar una descripción precisa de $\overline{K}[\mathcal{C}]_P$ del siguiente modo:

$$\overline{K}[\mathcal{C}]_P = \left\{ F \in \overline{K}(\mathcal{C}) \,:\, F = \frac{f}{g};\, f, g \in \overline{K}[\mathcal{C}],\, \textit{con } g(P) \neq 0 \right\}.$$

En otras palabras, $\overline{K}[\mathcal{C}]_P$ consiste en las funciones de $\overline{K}(\mathcal{C})$ definidas en el punto P.

El anillo local de una curva $\mathcal{C}$ en un punto P se vuelve mucho más útil si el punto P es un punto no singular de $\mathcal{C}$. Recordemos la siguiente definición:

Definición 1.3.6. Un anillo R se dice de *valuación discreta* si es un dominio principal con un único ideal maximal no nulo.

A un elemento $\pi \in R$ que genere al único ideal maximal no nulo se lo llama un *uniformizador local* de R.

Observación 1.3.7. Sea R un anillo de valuación discreta y sea π un uniformizador local de R. Dado $v \in Fracc(R)$, v se escribe de forma única como:

$$v = \pi^n u;$$

donde $n \in \mathbb{Z}$ y $u \in \mathcal{U}(R)$, el grupo de unidades de R.

El resultado que nos interesa es el siguiente.

Proposición 1.3.8. *Sea $\mathcal{C} \subseteq \mathbb{P}^n$ una curva y sea $P \in \mathcal{C}$. Entonces P es un punto no singular de $\mathcal{C}$ si, y sólo si, $\overline{K}[\mathcal{C}]_P$ es un anillo de valuación discreta.*

Demostración: Vamos a demostrar la implicación ($\Rightarrow$) que es la que más nos interesa.

Ya sabemos que $\overline{K}[\mathcal{C}]_P$ es un dominio con un único ideal maximal, que notamos $\mathcal{M}_P$. Sólo hace falta ver que es principal, y para ello alcanza con que $\mathcal{M}_P$ sea principal. Una forma de probar esto es viendo que el $\overline{K}[\mathcal{C}]_P/\mathcal{M}_P$ -espacio vectorial $\mathcal{M}_P/\mathcal{M}_P^2$ tiene dimensión 1. En efecto, digamos $P = (x_0, y_0)$, con lo cual $\mathcal{M}_P = \langle x - x_0, y - y_0 \rangle$.

Si la curva $\mathcal{C}$ es:

$$\mathcal{C} : h(x, y) = 0,$$

haciendo en h el desarrollo de Taylor alrededor de P tenemos:

$$h(x, y) = h(x_0, y_0) + \frac{\partial h}{\partial x}(P)(x - x_0) + \frac{\partial h}{\partial y}(P)(y - y_0) + R;$$

donde $R \in \mathcal{M}_P^2$. Entonces, para puntos $(x, y) \in \mathcal{C}$, la igualdad queda:

$$0 = \frac{\partial h}{\partial x}(P)(x - x_0) + \frac{\partial h}{\partial y}(P)(y - y_0) + R.$$

Si miramos esta igualdad en el cociente $\mathcal{M}_P/\mathcal{M}_P^2$ tenemos:

$$0 = \frac{\partial h}{\partial x}(P)(x - x_0) + \frac{\partial h}{\partial y}(P)(y - y_0).$$

Ahora usamos la hipótesis de que P es un punto no singular de $\mathcal{C}$ para asegurar que:

$$\frac{\partial h}{\partial x}(P) \neq 0 \ \text{ ó } \ \frac{\partial h}{\partial y}(P) \neq 0.$$

De modo que $\{x - x_0, y - y_0\}$ es linealmente dependiente en $\mathcal{M}_P/\mathcal{M}_P^2$, por lo que este cociente tiene dimensión 1. □

Teniendo entonces una curva $\mathcal{C}$ y un punto $P \in \mathcal{C}$ no singular, podemos definir un orden en $\overline{K}[\mathcal{C}]_P$, aprovechando la unicidad de la escritura $F = \pi^n u$ para un uniformizador local $\pi \in \overline{K}[\mathcal{C}]_P$. Precisamente, dada $F \in \overline{K}[\mathcal{C}]_P$ definimos el *orden de F en P* como:

$$ord_P(F) = máx\left\{d \in \mathbb{Z} : F \in \mathcal{M}_P^d\right\}. \quad \textbf{(1)}$$

Es decir, si $F = \pi^n u$, para un uniformizador local π, $ord_P(F) = n$. Pero resulta más cómodo usar la definición **(1)** ya que nos permite independizarnos del uniformizador local elegido.

Podemos entonces construir una función de valuación del siguiente modo:

Definición 1.3.9. Sea $\mathcal{C} \subseteq \mathbb{P}^n$ una curva y sea $P \in \mathcal{C}$ un punto no singular. La *valuación* en $\overline{K}[\mathcal{C}]_P$ es la función:

$$\begin{array}{rcl} ord_P : \overline{K}[\mathcal{C}]_P & \to & \mathbb{N}_0 \cup \{\infty\} \\ F & \to & ord_P(F) \end{array}$$

Donde convenimos $ord_P(0) = \infty$.

Podemos hacer una extensión natural de ord_P a $\overline{K}(\mathcal{C})$ definiendo:

$$ord_P(\frac{F}{G}) = ord_P(F) - ord_P(G).$$

De este modo tenemos $ord_P : \overline{K}(\mathcal{C}) \longrightarrow \mathbb{Z} \cup \{\infty\}$.

Teniendo esta función de valuación, podemos identificar a los uniformizadores locales de $\overline{K}[\mathcal{C}]_P$ como aquellos de orden 1. Concretamente, diremos que un uniformizador local para $\mathcal{C}$ en P es una función $t \in \overline{K}(\mathcal{C})$ tal que $ord_P(t) = 1$. Es decir, t es un generador de $\mathcal{M}_P$.

Las valuaciones son construcciones más generales y satisfacen ciertas propiedades conocidas. Nosotros hemos construido una valuación particular, y obviamente verificará esas propiedades. Listamos algunas de ellas, fáciles de comprobar, en la siguiente observación.

Observación 1.3.10. Con las notaciones de antes, sean $F, G \in \overline{K}(\mathcal{C})$. Entonces:

a) $ord_P(FG) = ord_P(F) + ord_P(G)$.

b) $ord_P(\frac{F}{G}) = ord_P(F) - ord_P(G)$.

c) $ord_P(F^n) = n\, ord_P(F)$, $\forall\, n \in \mathbb{Z}$.

d) $ord_P(F + G) \geq min\{ord_P(F), ord_P(G)\}$.

e) Si $ord_P(F) \neq ord_P(G)$ entonces $ord_P(F + G) = min\{ord_P(F), ord_P(G)\}$.

Con estas construcciones ahora podemos dar definiciones más precisas de algunas ideas intuitivas y que ya usamos.

Definición 1.3.11. Sea $\mathcal{C} \subseteq \mathbb{P}^n$ una curva y $P \in \mathcal{C}$ un punto no singular. Sea $F \in \overline{K}(\mathcal{C})$.

a) Si $ord_P(F) > 0$, decimos que F tiene un *cero* en P.

b) Si $ord_P(F) < 0$, decimos que F tiene un *polo* en P.

c) Si $ord_P(F) \geq 0$, decimos que F está *definida* o es *regular* en P.

Si F tiene un polo en P escribimos $F(P) = \infty$.

Proposición 1.3.12. *Sea $\mathcal{C}$ una curva no singular y sea $F \in \overline{K}(\mathcal{C})^{\times}$. Entonces hay sólo finitos puntos $P \in \mathcal{C}$ en los cuales F tiene un cero o un polo. Más aún, si F no tiene polos, $F \in \overline{K}^{\times}$.*

Demostración: Una forma sencilla de ver esto es considerando a la curva $\mathcal{C}$ como una superficie de Riemann compacta; y a la función F como una función meromorfa con dominio en ella. En tal caso resulta claro que F tiene sólo finitos puntos en los cuales tiene un cero o un polo.

Si F no tiene polos, como $\mathcal{C}$ es compacta, la imagen de F es acotada; y como consecuencia del Teorema de la aplicación abierta sale que F es constante.

Para una prueba alternativa, ver [1], Capítulo I, Lema 6.5. para la finitud del número de polos; y para la finitud de los ceros considerar $\frac{1}{F}$. Ver [1], Capítulo I, Teorema 3.4.a. para la última afirmación. □

Ejemplo 1.3.13. Consideremos la curva $\mathcal{C} \subseteq \mathbb{P}^2$ (con $K = \mathbb{Q}$) dada por la ecuación afín: $y^2 = x^3 + x$. (Recordemos la correspondencia entre variedades afines y proyectivas. Formalmente, $\mathcal{C}$ es la curva proyectiva de $\mathbb{P}^2$ cuya afinización en Z es la curva afín que tenemos). Notemos que es la misma variedad que consideramos en el Ejemplo 1.1.8. Habíamos visto que era una variedad no singular, con lo cual, en particular, $P = (0,0) \in \mathcal{C}$ es un punto no singular, y podemos entonces considerar la valuación en P. Tenemos que las funciones x e y generan $\mathcal{M}_P$, por lo que $\mathcal{M}_P = (x, y)$. Ahora, $\mathcal{M}_P^2 = (x^2, xy, y^2)$. Entonces:

$$x = y^2 - x^3 \equiv 0 \, (mod(\mathcal{M}_P^2))$$

Luego, $x \in \mathcal{M}_P^2$, por lo que $ord_P(x) \geq 2$.

Por otro lado, observemos que:

$$x(1 + x^2) = y^2.$$

Y como $1 + x^2 \notin \mathcal{M}_P$, es una unidad en $\overline{\mathbb{Q}}\,[\mathcal{C}]_P$. De modo que, en $\overline{\mathbb{Q}}\,[\mathcal{C}]_P$:

$$x = \frac{1}{1 + x^2}\, y^2 = \frac{y}{1 + x^2}\, y.$$

Con lo cual $x \in (y)$. De donde $\mathcal{M}_P = (x, y) = (y)$. Esto es, y es un uniformizador local para $\mathcal{C}$ en P.

Veamos ahora que $ord_P(x) = 2$. En efecto, como $ord_P(y) = 1$, tenemos:

$$2 = ord_P(y^2) = ord_P(x^3 + x) = mín\left\{ord_P(x^3), ord_P(x)\right\} = ord_P(x).$$

Pues dado que $ord_P(x) > 0$, $ord_P(x^3) = 3ord_P(x) \neq ord_P(x)$, y más aún, $ord_P(x^3) > ord_P(x)$.

Calculemos entonces, por ejemplo, $ord_P(2y^2 - x)$. Tenemos:

$$2y^2 - x = 2(x^3 + x) - x = 2x^3 + x = x(2x^2 + 1).$$

Entonces:

$$ord_P(2y^2 - x) = ord_P(x(2x^2 + 1)) = ord_P(x) + ord_P(2x^2 + 1) = 2 + 0 = 2.$$

En efecto, $ord_P(2x^2 + 1) = 0$, dado que no pertenece a $\mathcal{M}_P$; por lo que $2x^2 + 1$ es una unidad en $\overline{\mathbb{Q}}\,[\mathcal{C}]_P$.

1.3.1. Funciones entre curvas

Ya vimos cómo son las funciones entre variedades proyectivas en general. Pero cuando nos restringimos a trabajar con curvas aparecen propiedades interesantes. Una de ellas, muy útil por cierto, es la siguiente.

Proposición 1.3.14. *Sea $\mathcal{C}$ una curva y $P \in \mathcal{C}$ un punto no singular. Entonces cualquier función racional $\phi : \mathcal{C} \longrightarrow V$, con $V \subseteq \mathbb{P}^n$ una variedad proyectiva, es regular en P.*

En particular, si $\mathcal{C}$ es una curva no singular, cualquier función racional $\phi : \mathcal{C} \longrightarrow V$ es un morfismo. Y si $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ es una función birracional entre curvas no singulares, entonces es un isomorfismo. Con lo cual, para funciones racionales entre curvas no singulares se tiene:

$$\textit{isomorfismo} \Leftrightarrow \textit{morfismo birracional} \Leftrightarrow \textit{función birracional.}$$

Demostración: Escribamos:

$$\phi = [f_0, ..., f_n] \,;\ \textit{con } f_i \in \overline{K}(\mathcal{C}).$$

Como P es un punto no singular podemos considerar un uniformizador local t de $\mathcal{C}$ en P.

Sea:

$$m = min\left\{ord_P(f_i) \,:\, 0 \leq i \leq n\right\}.$$

Entonces $ord_P(t^{-m} f_i) \geq 0$, para $0 \leq i \leq n$, y $ord_P(t^{-m} f_j) = 0$ para algún j. Luego, cada $t^{-m} f_i$ es regular en P y $(t^{-m} f_j)(P) \neq 0$. Esto dice que ϕ es regular en P. □

Esto deja de ser cierto si la variedad del dominio no tiene dimensión 1.

Ejemplo 1.3.15. Un ejemplo de morfismo entre curvas que vamos a usar más adelante es el siguiente.

Sea $\mathcal{C}$ una curva no singular y sea $f \in \overline{K}\left(\mathcal{C}\right)$. Entonces f induce una función racional (y por lo tanto un morfismo) $f : \mathcal{C} \longrightarrow \mathbb{P}^1$ dado por:

$$f(P) = \begin{cases} [f(P) : 1] & \textit{si } f \textit{ es regular en } P \\ [1 : 0] & \textit{si } f \textit{ tiene un polo en } P \end{cases}$$

Otro de los comportamientos que tienen las funciones con dominio en una curva es el siguiente teorema, que también vamos a utilizar en los capítulos siguientes.

Teorema 1.3.16. *Sea $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ un morfismo entre dos curvas. Entonces ϕ es **constante** o **suryectivo.***

Demostración: Así como hicimos en la demostración de la Proposición 1.3.12, consideramos a nuestras curvas como superficies de Riemann compactas. Si ϕ no es suryectivo, podemos suponer que su imagen está contenida en un abierto afín. Volviendo a usar el Teorema de la aplicación abierta concluimos que, como $\mathcal{C}_1$ es compacta, entonces necesariamente ϕ es constante.

Para otra prueba, ver [1], Capítulo II, Proposición 6.8. □

Una consecuencia inmediata de este resultado es que, si la función $f \in \overline{K}(\mathcal{C})$ no es constante, entonces el morfismo inducido $f : \mathcal{C} \longrightarrow \mathbb{P}^1$ es suryectivo.

Vamos a dar una última noción referida a los morfismos entre curvas. Supongamos que tenemos dos curvas $\mathcal{C}_1$ y $\mathcal{C}_2$ definidas sobre K y un morfismo no constante (por lo tanto suryectivo) entre ellas:

$$\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2.$$

Podemos ver que ϕ induce un morfismo inyectivo entre los cuerpos de funciones:

$$\begin{aligned} \phi^* : K(\mathcal{C}_2) &\longrightarrow K(\mathcal{C}_1) \\ \phi^*(f) &= f \circ \phi \end{aligned}$$

Un resultado conocido nos asegura que $K(\mathcal{C}_1)$ es una extensión finita de $\phi^* K(\mathcal{C}_2)$. De este modo podemos dar la siguiente definición.

Definición 1.3.17. Sea $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ un morfismo no constante entre curvas. Definimos el *grado* de ϕ como:

$$deg(\phi) = [K(\mathcal{C}_1) : \phi^* K(\mathcal{C}_2)] .$$

O sea, el grado de la extensión:

$$K(\mathcal{C}_1)/\phi^* K(\mathcal{C}_2).$$

Si ϕ es constante definimos $deg(\phi) = 0$.

El grado de un morfismo es un concepto que vamos a utilizar en los próximos capítulos.

1.3.2. Divisores

Dada una curva $\mathcal{C}$ no singular, podemos construir un grupo abeliano asociado a ella que tiene muchas utilidades, algunas de las cuales vamos a aprovechar.

Recordemos que si P es no singular, el anillo $\overline{K}[\mathcal{C}]_P$ es de valuación discreta y podemos definir la función de valuación ord_P en $\overline{K}(\mathcal{C})$. Como todos los puntos de $\mathcal{C}$ son no singulares, dada una función $f \in \overline{K}(\mathcal{C})$ podemos calcular $ord_P(f)$ en cada uno de los $P \in \mathcal{C}$. Supongamos que $f \neq 0$ (con lo cual $ord_P(f) \in \mathbb{Z}\ \forall\, P \in \mathcal{C}$). Podemos considerar la siguiente suma formal:

$$\sum_{P \in \mathcal{C}} ord_P(f)(P).$$

En virtud de la Proposición 1.3.12 esta suma es finita. Observando esto, es natural considerar el $\mathbb{Z}$-módulo libre generado por los puntos $P \in \mathcal{C}$.

Definición 1.3.18. Sea $\mathcal{C}$ una curva no singular. Se define su *grupo de divisores* $\mathcal{D}iv(\mathcal{C})$ como el $\mathbb{Z}$-módulo libre generado por los puntos $P \in \mathcal{C}$. Es decir:

$$\mathcal{D}iv(\mathcal{C}) = \left\{ \sum_{P \in \mathcal{C}} n_P(P) \ :\ n_P \in \mathbb{Z},\, n_P = 0 \,\textit{para casi todo}\ P \in \mathcal{C} \right\}$$

Por lo que observamos antes, a cada $f \in \overline{K}(\mathcal{C})$, $f \neq 0$, podemos asociarle el elemento

$$div(f) = \sum_{P \in \mathcal{C}} ord_P(f)(P) \in \mathcal{D}iv(\mathcal{C}).$$

Más aún, tenemos que:

$$\begin{array}{ccc} \overline{K}(\mathcal{C})^\times & \longrightarrow & \mathcal{D}iv(\mathcal{C}) \\ f & \mapsto & div(f) \end{array}$$

es un morfismo de grupos. Esto es sencillo de verificar a partir de las propiedades que mencionamos en la Observación 1.3.10

Definición 1.3.19. Sea $\mathcal{C}$ una curva no singular y sea $D \in \mathcal{D}iv(\mathcal{C})$. Digamos:

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

Definimos el *grado* de D como:

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

Es claro que:

$$\begin{array}{ccc} \mathcal{D}iv(\mathcal{C}) & \rightarrow & \mathbb{Z} \\ D & \rightarrow & deg(D) \end{array}$$

también es un morfismo de grupos.

Notamos $\mathcal{D}iv^\circ(\mathcal{C})$ al subgrupo de $\mathcal{D}iv(\mathcal{C})$ formado por los divisores de grado 0.

Proposición 1.3.20. *Sea $\mathcal{C}$ una curva no singular y sea $f \in \overline{K}(\mathcal{C})^\times$. Entonces:*

a) $div(f) = 0 \iff f \in \overline{K}^\times$.

b) $deg(div(f)) = 0$.

Demostración: En la parte *a*), la implicación ($\Leftarrow$) es evidente. La implicación ($\Rightarrow$) es consecuencia inmediata de la Proposición 1.3.12.

Para la parte *b*), ver [1], Capítulo II, Corolario 6.10. o [9], Capítulo II, Observación 3.7. □

A los divisores de la forma $div(f)$ para alguna $f \in \overline{K}(\mathcal{C})^\times$ los llamamos *principales.* Como consecuencia de la parte ***b)*** de la última proposición, el grupo de los divisores principales es un subgrupo de $\mathcal{D}iv^\circ(\mathcal{C})$.

Si consideramos el subgrupo de los divisores principales, podemos dividir a $\mathcal{D}iv(\mathcal{C})$ por él; lo que es lo mismo que definir una relación de equivalencia dada por:

$$D_1 \sim D_2 \iff D_1 - D_2 \text{ es principal.}$$

El grupo que resulta de hacer el cociente por esa relación nos va a interesar mucho y lleva el siguiente nombre:

Definición 1.3.21. Sea $\mathcal{C}$ una curva no singular y sea $\sim$ la relación en $\mathcal{D}iv(\mathcal{C})$ definida arriba. Definimos el *grupo de Picard* de $\mathcal{C}$ como:

$$\mathcal{P}ic(\mathcal{C}) = \mathcal{D}iv(\mathcal{C})/\sim .$$

Como vimos, el subgrupo de los divisores principales también está contenido en $\mathcal{D}iv^{\circ}(\mathcal{C})$; y también podemos dividirlo. En ese caso notaremos:

$$\mathcal{P}ic^{\circ}(\mathcal{C}) = \mathcal{D}iv^{\circ}(\mathcal{C})/\sim .$$

Para terminar con este capítulo mostremos un ejemplo en el que calculemos $div(f)$ para alguna $f \in \overline{K}(\mathcal{C})^{\times}$.

Ejemplo 1.3.22. Volvamos a trabajar con la curva del Ejemplo 1.1.8: $\mathcal{C} : y^2 = x^3 + x$. Es decir, $\mathcal{C} \subseteq \mathbb{P}^2$ es la curva proyectiva dada por la ecuación $Y^2Z = X^3 + XZ^2$. Sea $F \in \overline{K}(\mathcal{C})^{\times}$, $F(X, Y, Z) = \frac{X}{Z}$ y calculemos $div(F)$. Para ello tenemos que fijarnos en cuáles puntos de $\mathcal{C}$ la función F tiene un cero o un polo. Si F tiene un cero en $[X : Y : Z] \in \mathcal{C}$ entonces $X = 0$. Y los puntos de $\mathcal{C}$ tales que $X = 0$ son exactamente $P_1 = [0 : 0 : 1]$ y $P_2 = [0 : 1 : 0]$. Si F tiene un polo en $[X : Y : Z] \in \mathcal{C}$ entonces $Z = 0$. Y el único punto de $\mathcal{C}$ tal que $Z = 0$ es P_2. En el resto de los puntos de $\mathcal{C}$ se tiene $ord_P(F) = 0$. Con lo cual:

$$div(F) = \sum_{P \in \mathcal{C}} ord_P(F)(P) = ord_{P_1}(F)(P_1) + ord_{P_2}(F)(P_2).$$

Resta calcular entonces $ord_{P_1}(F)$ y $ord_{P_2}(F)$. Notemos que P_1 es un punto de $\mathcal{C}$ que pertenece a la afinización $Z = 1$. Trabajando en esa afinización, nuestro problema se convierte en calcular el orden de la función (deshomogenizada) $f(x, y) = x$ en el punto $p_1 = (0, 0)$. Eso es exactamente lo que hicimos en el Ejemplo 1.3.13 y nos dio 2.

Para calcular $ord_{P_2}(F)$ la afinización que debemos hacer es $Y = 1$. En este caso F queda $f(x, z) = \frac{x}{z}$, la curva $\mathcal{C}$ se convierte en: $z = x^3 + xz^2$, y queremos calcular el orden de f en $p = (0, 0)$. Haciendo un razonamiento análogo al que hicimos en 1.3.13 es fácil de ver que $ord_p(x) = 1$ y $ord_p(z) = 3$. En consecuencia $ord_p(\frac{x}{z}) = -2$. Luego:

$$div(F) = 2(P_1) - 2(P_2).$$

Observemos que por la Proposición 1.3.20 sabemos que $deg(div(F)) = 0$. Por lo tanto, sabiendo que $ord_{P_1}(F) = 2$, podríamos haber concluido inmediatamente que $ord_{P_2}(F) = -2$; que es lo que efectivamente nos da.

Haciendo un desarrollo similar, podemos calcular $div(G)$, donde $G(X, Y, Z) = \frac{Y}{Z}$. Lo que se obtiene es:

$$div(G) = (Q_1) + (Q_2) + (Q_3) - 3(Q_{\infty});$$

donde $Q_1 = [0 : 0 : 1]$, $Q_2 = [i : 0 : 1]$, $Q_3 = [-i : 0 : 1]$ y $Q_{\infty} = [0 : 1 : 0]$.

La notación Q_{∞} es porque, pensando a la curva $\mathcal{C}$ afinizada en $Z = 1$, $[0 : 1 : 0]$ es el punto *en el infinito* de $\mathcal{C}$.

Capítulo 2

Curvas Elípticas

En este capítulo empezaremos a hablar de las curvas elípticas, que son el centro de nuestro interés. Las curvas elípticas son casos particulares de curvas proyectivas, con lo cual gozan de todas las propiedades geométricas que hemos comentado en el capítulo anterior. Sin embargo también tienen estructura algebraica; y más aún, como hemos dicho, estuvieron y están muy presentes en muchos aspectos de la Teoría de Números. Por lo tanto son una entidad en la cual confluyen tres grandes ramas de la matemática: Geometría, Algebra y Teoría de Números. Esta es una de las razones por las cuales son tan interesantes. A lo largo de este trabajo intentaremos sacarle un poco de provecho a todas esas cualidades que tienen.

Si bien se puede trabajar sobre cualquier cuerpo K, por cuestiones técnicas, vamos a pedir al menos que $car(K) \neq 2, 3$. Así que, en la siguiente sección, a menos que se haga alguna aclaración, K será cualquier cuerpo con $car(K) \neq 2, 3$.

2.1. Curvas Elípticas

Uno podría dar una definición de Curva Elíptica que es muy técnica y requiere varios conocimientos previos. Sin embargo no es nuestra intención ir por ese camino. En cambio vamos a dar una definición que es equivalente y que, para entenderla, no se precisa saber más de lo que contamos en el capítulo anterior. En seguida haremos un comentario sobre cuál es esa otra definición un poco más técnica.

Para nosotros una Curva Elíptica será una curva proyectiva no singular que viene dada por una ecuación con una cierta particularidad. Seamos concretos:

Definición 2.1.1. Sea K un cuerpo de característica distinta de 2 y $\overline{K}$ una clausura algebraica fija. Una *curva elíptica* es una curva proyectiva $E \subseteq \mathbb{P}^2(\overline{K})$ no singular que viene dada por una ecuación de la forma:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Donde $a, b, c \in \overline{K}$.

Bajo un simple cambio de coordenadas se puede suponer que $a = 0$. Esto es posible si $car(K) \neq 2, 3$; que es el caso que nos interesa.

Observación 2.1.2. Si afinizamos una curva elíptica E haciendo $Z = 1$ obtenemos una curva dada por la ecuación afín:

$$y^2 = x^3 + ax^2 + bx + c.$$

Es muy común trabajar con esta afinización por varias razones. Por ejemplo porque a la hora de hacer cálculos resulta más cómoda. Además la ecuación que queda es mucho más simple y recordable. Y, como ya veremos, al afinizar de esta forma sólo perdemos un punto de la curva: el punto $P = [0 : 1 : 0]$. Es decir, todos los puntos de la curva pueden encontrarse en esta afinización salvo P.

Si bien, como dijimos, no vamos a trabajar con la otra definición equivalente; no nos cuesta nada hacer un comentario al respecto, sobre todo para aquellos entendidos en el tema.

Hay un número que puede asociarse a una curva proyectiva que se lo llama *género.* El concepto de género de una curva no es sencillo de explicar, incluso hay tres definiciones de ese concepto. Una, desde el punto de vista homológico, dice esencialmente que el género de una curva (o en general, de una superficie) es la cantidad de *agujeros* que tiene el gráfico de dicha curva. Otra de las definiciones dice que el género de una curva $\mathcal{C}$ es la dimensión del $\overline{K}(\mathcal{C})$-espacio vectorial de las formas diferenciales holomorfas definidas sobre $\mathcal{C}$. Por último, hay otra definición que tiene que ver con la Topología Algebraica. Dado un poliedro, se define su *Característica de Euler* como el número $\chi = V - E + F$. Donde V, E y F son, respectivamente, el número de vértices, aristas y caras del poliedro. Resulta entonces que si uno mira a la curva proyectiva como una superficie en el plano complejo, la *triangula* y le calcula la característica de Euler, se obtiene la siguiente igualdad:

$$\chi = 2 - 2g.$$

Donde g es el género de la curva.

Pues bien, la definición alternativa de Curva Elíptica a la que hicimos referencia es que es una curva no singular de género 1 con un punto distinguido. Como dijimos, se requieren varias nociones previas para entender esta definición técnica, así que no nos vamos a meter con ella.

Se puede probar que a cualquier curva elíptica, según esta última definición, se la puede ver como una curva con una ecuación del tipo de la definición que vimos antes, luego de un cambio de coordenadas adecuado. Y recíprocamente, también es cierto que cualquier curva no singular dada por una ecuación de ese tipo es una curva elíptica. Por eso nos tomamos la libertad de ver a esa ecuación como la definición de curva elíptica; pues, en algún sentido, esa definición es equivalente a la otra.

La ecuación que dimos nosotros suele llamarse **Ecuación de Weierstrass.**

Ya vimos un ejemplo de curva elíptica en el capítulo anterior. Concretamente ya hemos trabajado con la curva $E_1 : y^2 = x^3 + x$, y vimos que E_1 es no singular.

También trabajamos con la curva $E_2 : y^2 = x^3 + x^2$, pero recordemos que verificamos que esta curva es singular; con lo cual, si bien tiene la forma de la ecuación de una curva elíptica, en

realidad no lo es.

Para verificar si una curva dada por la ecuación:

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3,$$

es efectivamente una curva elíptica; es decir, es no singular; podemos hacer un razonamiento que funcionará en general. Afinizando en $Z = 1$, nos queda:

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Llamemos $g(x, y) = y^2 - x^3 - ax^2 - bx - c$. Y $f(x) = x^3 + ax^2 + bx + c$. Entonces tenemos que:

$$P = (x_0, y_0) \in E \text{ es punto singular } \iff \frac{\partial g}{\partial x}(P) = \frac{\partial g}{\partial y}(P) = 0.$$

Pero resulta que:

$$\begin{cases} \frac{\partial g}{\partial x}(x, y) = -f'(x) & = 0 \\ \frac{\partial g}{\partial y}(x, y) = 2y & = 0 \end{cases}$$

Luego, si $P = (x_0, y_0)$ es punto singular, entonces $y_0 = f'(x_0) = 0$. Pero como además $P \in E$, dado que $y_0 = 0$, se tiene que $f(x_0) = 0$.

En resumen, si $P = (x_0, y_0) \in E$ es punto singular, entonces:

$$\begin{aligned} f(x_0) = f'(x_0) = & \quad 0 \\ y_0 = & \quad 0 \end{aligned}$$

En particular, x_0 es una raíz múltiple de f. Y es claro que, recíprocamente, si x_0 es una raíz múltiple de f entonces el punto $P = (x_0, 0) \in E$ es un punto singular. Podemos concluir en consecuencia que si $f(x) = x^3 + ax^2 + bx + c$ tiene raíces múltiples, entonces E es una curva singular.

Veamos si esa condición suficiente es también necesaria. Para ello, sólo nos falta analizar la singularidad o no de los puntos que quedaron afuera cuando hicimos la afinización. O sea, los puntos tales que $Z = 0$. Pero si ponemos $Z = 0$ en la ecuación original nos queda:

$$0 = X^3.$$

Luego, para puntos de E se tiene: $Z = 0 \Rightarrow X = 0$. Con lo cual sólo hay un punto que satisface esto que es el $[0 : 1 : 0]$. A este punto lo vamos a notar $\mathcal{O}$ y enseguida veremos por qué. Para ver si este punto es singular afinizamos la ecuación haciendo $Y = 1$ y obtenemos:

$$z = x^3 + ax^2z + bxz^2 + cz^3.$$

Si ahora llamamos $g(x, z) = z - x^3 - ax^2z - bxz^2 - cz^3$, tenemos:

$$\begin{cases} \frac{\partial g}{\partial x}(x, z) = & -3x^2 - 2axz - bz^2 \\ \frac{\partial g}{\partial z}(x, z) = & 1 - ax^2 - 2bxz - 3cz^2 \end{cases}$$

Entonces:

$$\begin{cases} \frac{\partial g}{\partial x}(0,0) = & 0 \\ \frac{\partial g}{\partial z}(0,0) = & 1 \end{cases}$$

Con lo cual, $\mathcal{O} = [0:1:0]$ nunca es singular. En consecuencia, los puntos singulares sólo pueden encontrarse en la afinización $Z = 1$. De este modo nos queda probado que:

La curva E es singular si, y sólo si, $f(x) = x^3 + ax^2 + bx + c$ tiene raíces múltiples.

Pero hay una manera muy sencilla de saber si f tiene raíces múltiples y es mirando su discriminante Δ. En este caso se tiene que $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Luego, tenemos probado el siguiente resultado.

Proposición 2.1.3. *Sea E una curva dada por la ecuación:*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Entonces:

$$E \text{ es una curva elíptica } \iff \Delta \neq 0.$$

Donde $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

Para terminar con esta parte vamos a dar un criterio para decidir si dos curvas elípticas distintas son isomorfas. Para ello vamos a definir la siguiente cantidad:

Definición 2.1.4. Sea E una curva elíptica dada por la ecuación afín:

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Definimos el *j-invariante* de E como la cantidad:

$$j = \frac{16a^2 - 48b}{\Delta}.$$

Donde Δ es el discriminante de E.

El interés que tiene el j-invariante es que es justamente un invariante bajo isomorfismos. Precisamente tenemos el siguiente resultado.

Proposición 2.1.5. *Sean E y E' dos curvas elípticas y sean j y j' sus respectivos j-invariantes. Entonces:*

$$E \text{ es isomorfa a } E' \Leftrightarrow j = j'.$$

Demostración: Ver [9], Capítulo III, Proposición 1.4.b. □

Como dijimos, las curvas elípticas, por ser curvas proyectivas, tienen todas las propiedades geométricas de cualquier curva. Pero también tienen una estructura algebraica que estudiaremos a continuación.

2.1.1. Ley de grupo en curvas elípticas

Recordemos que podemos trabajar sobre K un cuerpo cualquiera de característica distinta de 2 y de 3; pero vamos a hacer la construcción para el caso $K = \mathbb{Q}$, $\overline{K} = \overline{\mathbb{Q}}$ para que se entienda mejor la idea.

Tomemos una curva elíptica E de ecuación afín $y^2 = x^3 + ax^2 + bx + c$; $a, b, c \in \overline{\mathbb{Q}}$. Empezaremos trabajando en la afinización $Z = 1$, así que podemos pensar por ahora que $E \subseteq \overline{\mathbb{Q}}^2$ es la curva afín dada por la ecuación que dijimos.

Notemos $E(\overline{\mathbb{Q}}) \subseteq \overline{\mathbb{Q}}^2$ al conjunto de los puntos de E. Vamos a definir en el conjunto $E(\overline{\mathbb{Q}})$ una operación *suma* que lo dotará de una estructura de grupo abeliano. La operación es muy fácil de describir si la hacemos desde el punto de vista geométrico. Fijemos un punto cualquiera de $E(\overline{\mathbb{Q}})$ y llamémoslo $\mathcal{O}$. Ese será el elemento neutro. Ahora tomemos dos puntos $P, Q \in E(\overline{\mathbb{Q}})$ distintos y definamos la operación $P+Q$. Sea $\mathbb{L} \subseteq \overline{\mathbb{Q}}^2$ la recta que une los puntos P y Q. Digamos $\mathbb{L} : Ax + By + C = 0$. Supongamos que $\mathbb{L}$ corta a E en P y en Q de manera secante. Es decir, $\mathbb{L}$ no es tangente a E ni en P ni en Q. Como estamos trabajando en un cuerpo algebraicamente cerrado, y porque la ecuación de E es de grado 3; tenemos que necesariamente $\mathbb{L}$ deberá cortar a E en 3 puntos. Consideremos entonces el siguiente sistema:

$$S : \begin{cases} y^2 - x^3 - ax^2 - bx - c & = 0 \\ Ax + By + C & = 0 \end{cases}$$

Como supusimos que los puntos de contacto P y Q son simples; es decir, P y Q son soluciones del sistema S con multiplicidad 1; $\mathbb{L}$ cortará a E en un tercer punto distinto de P y de Q. Llamemos a ese nuevo punto $P \star Q$. Supongamos que $P \star Q \neq \mathcal{O}$. Tracemos entonces la recta $\mathbb{L}'$ que pasa por los puntos $\mathcal{O}$ y $P \star Q$. Supongamos de vuelta que $\mathbb{L}'$ no es tangente a E en $\mathcal{O}$ ni en $P \star Q$. Entonces $\mathbb{L}'$ deberá cortar a E en un tercer punto. Bien, a ese punto lo llamaremos $P + Q$ y esa será la suma entre P y Q. (Ver Figura 2.1).

Muchas cosas hay que decir respecto a esta definición. En primer lugar, al construir el punto $P+Q$ hemos hecho varias suposiciones que dejan de lado algunos casos particulares. Por ejemplo, podría pasar que la recta $\mathbb{L}$ sea tangente a E en P o en Q. Supongamos que $\mathbb{L}$ es tangente a E en P. Como sabemos que el sistema S tiene que tener 3 soluciones (contadas con su multiplicidad), esas 3 soluciones son Q y P **dos veces.** O sea, el tercer punto en donde $\mathbb{L}$ interseca a E es P. Es decir, $P \star Q = P$. Y la construcción sigue como antes.

También nos puede interesar cómo se calcula $P+P$. En tal caso deberíamos empezar considerando la recta $\mathbb{L}$ que pasa por P y por P. Esta sería la recta que pasa **dos veces** por P; que es la recta tangente a E en P.

Otra de las cosas que uno se pregunta es si efectivamente, con esta definición de suma, se tiene que $P + \mathcal{O} = P$. Esto es sencillo de verificar haciendo la construcción. También será fácil de ver que $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Además nos podemos preguntar si efectivamente esta operación hace de $E(\overline{\mathbb{Q}})$ un grupo abeliano. Para ello habría que verificar que es **asociativa** y **conmutativa.** Antes de discutir estas cosas

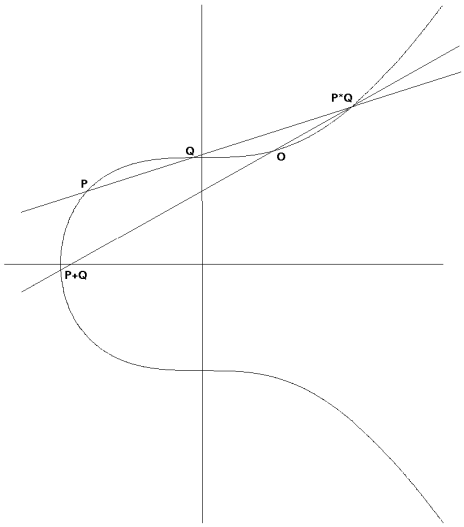


Figura 2.1: Suma en curvas elípticas

hagamos una convención. Recordemos que todo esto lo estamos haciendo en la afinización $Z = 1$. Habría que contemplar también a los puntos que estamos dejando afuera al trabajar con esa afinización. Es decir, los puntos tales que $Z = 0$. Pero recordemos que sólo hay un punto de $\mathbb{P}^2$ que satisface la ecuación, que es $[0 : 1 : 0]$. O sea, hay un único punto en el infinito. Con esto, una curva elíptica se puede ver como una curva afín de ecuación $y^2 = x^3 + ax^2 + bx + c$ más un punto en el infinito que es el $[0 : 1 : 0]$. Dada esta particularidad que tienen las curvas elípticas, es natural que a ese punto del infinito se lo trate de alguna manera especial. Y si bien el punto neutro $\mathcal{O}$ podía ser cualquiera; en general, lo más común es tomar $\mathcal{O} = [0 : 1 : 0]$.

Hay otra razón por la cual el punto $[0 : 1 : 0]$ suele elegirse como origen. Resulta que si consideramos la recta del plano proyectivo $Z = 0$; esa recta tiene que cortar a la curva en tres puntos. Pero ocurre que los tres puntos coinciden, son el $[0 : 1 : 0]$. O sea, esa recta interseca a la curva una sola vez y con multiplicidad 3. Por esto decimos que $[0 : 1 : 0]$ es un *punto de inflexión* de la curva. A la hora de hacer operaciones en el grupo $E(\overline{\mathbb{Q}})$ resulta cómodo que $\mathcal{O}$ sea un punto de inflexión. Por ejemplo, en tal caso es trivial que $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Notemos que ahora las rectas de $\mathbb{P}^2$ que pasan por $\mathcal{O}$ son aquellas cuyo punto del infinito, o punto impropio, es $[0 : 1 : 0]$; y éstas son las rectas cuya dirección es la del vector $(0, 1)$. O sea, las rectas verticales. En este caso es muy sencillo comprobar que si $P = (x, y)$, entonces $-P = (x, -y)$.

En cuanto a la conmutatividad y asociatividad de la suma que definimos, la primera es bastante clara. Sólo mirando cómo es la construcción es evidente que $P + Q = Q + P$. Sin embargo no es nada claro que la asociatividad valga. Pero también se puede hacer la construcción geométrica

y verificar que $(P+Q)+R = P+(Q+R)$. Antes de seguir estas discusiones vamos a enunciar el resultado formalmente.

Proposición 2.1.6 (Ley de Grupo)**.** *Sea K un cuerpo y $\overline{K}$ una clausura algebraica fija. Consideremos el espacio proyectivo $\mathbb{P}^2 = \mathbb{P}^2(\overline{K})$. Sea $E \subseteq \mathbb{P}^2$ una curva elíptica. Llamemos $\mathcal{O} = [0:1:0] \in E(\overline{K})$. Sean $P, Q \in E(\overline{K})$. Llamemos $\mathbb{L}$ a la recta que pasa por P y por Q (si $P = Q$, $\mathbb{L}$ es la recta tangente a E en P) y notemos $P \star Q$ al tercer punto de intersección de $\mathbb{L}$ con E. Sea $\mathbb{L}'$ la recta que pasa por $\mathcal{O}$ y por $P \star Q$. Definimos $P+Q$ como el tercer punto de $E(\overline{K})$ en el que $\mathbb{L}'$ interseca a E (pudiendo ser $P+Q = \mathcal{O}$ o $P+Q = P \star Q$ si alguna de las intersecciones tiene orden de contacto mayor a 1). La operación descripta satisface las siguientes propiedades:*

a) $(P+Q)+R = P+(Q+R),\ \forall P, Q, R \in E(\overline{K})$.

b) $P + \mathcal{O} = P,\ \forall P \in E(\overline{K})$.

c) $P + Q = Q + P,\ \forall P, Q \in E(\overline{K})$.

d) Sea $P \in E(\overline{K})$. Entonces existe un punto de $E(\overline{K})$ notado $-P$ tal que $P + (-P) = \mathcal{O}$.

En otras palabras, $(E(\overline{K}), +)$ es un grupo abeliano.

Antes ya mostramos, sin demasiada rigurosidad, que los ítems **b)** y **c)** son ciertos. El ítem **d)** también es fácil de justificar; pues se verifica fácilmente que $-P$ es el segundo punto (afín) de intersección entre E y la recta vertical que pasa por P. Concretamente, si $P = (x, y)$, $-P = (x, -y)$.

Como dijimos antes, el ítem **a)** es el que suele costar más; pero no porque haya una dificultad mayor, sólo requiere trabajo (mucho y tedioso por cierto).

A partir de la definición hay varias observaciones que uno podría hacer; una de ellas, que es muy sencilla (pues haciendo el dibujo se ve inmediatamente) es que si tenemos tres puntos alineados sobre la curva: P, Q y R; entonces:

$$P + Q + R = \mathcal{O}.$$

Como vemos, la definición de la operación suma es puramente geométrica, y no pareciera ser demasiado práctica si uno pretende manipularla de algún modo. Más precisamente, si quisiéramos ver las características que tiene el grupo $E(\overline{K})$ no sería una tarea fácil si sólo contáramos con esa única definición. Es por esto que es natural preguntarse cómo se verá esa operación suma si miramos las coordenadas de los puntos involucrados. Queremos tener una expresión de $P+Q$ que dependa de sus coordenadas. Es decir, queremos hallar las coordenadas del punto $P+Q$ en términos de las de los puntos P y Q. Es de imaginar que esto no va a ser inmediato, ya que la definición no es tan simple. Pero no con demasiado trabajo uno puede encontrar las ecuaciones que queremos. A continuación mostramos cómo se obtiene $P+Q$ si volcamos la construcción geométrica en el planteo algebraico de trabajar con las coordenadas.

2.1.2. Fórmulas explícitas para la ley de grupo

Sea $E \subseteq \mathbb{P}^2$ una curva elíptica de ecuación afín $y^2 = x^3 + ax^2 + bx + c$. Sean $P_1, P_2 \in E(\overline{K})$; $P_1 \neq \mathcal{O}$, $P_2 \neq \mathcal{O}$, $P_1 \neq P_2$ y $P_1 \neq -P_2$. En particular P_1 y P_2 son puntos afines de E; digamos que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$. Digamos también $P_1 + P_2 = (x_3, y_3)$. Llamemos:

$$\begin{aligned} \lambda = & \quad \frac{y_2 - y_1}{x_2 - x_1}. \\ \nu = & \quad y_1 - \lambda x_1 = \quad y_2 - \lambda x_2. \end{aligned}$$

Entonces se tiene:

$$\begin{aligned} x_3 = & \quad \lambda^2 - a - x_1 - x_2. \\ y_3 = & \qquad\qquad -\lambda x_3 - \nu. \end{aligned}$$

Observemos que, como $P_1 \neq P_2$ y $P_1 \neq -P_2$, se tiene que $x_1 \neq x_2$; con lo cual está todo bien definido.

Si $P_1 = \mathcal{O}$ o $P_2 = \mathcal{O}$ no hace falta mirar una fórmula. Y si $P_1 = -P_2$ tampoco. El caso $P_1 = P_2$ se analiza aparte y suele resultar interesante. En general la operación nP para $n \in \mathbb{N}$ es algo que juega un papel crucial en circunstancias que ya veremos en los próximos capítulos. En particular, para $n = 2$, se tiene que si $P = (x, y)$, entonces:

$$\textit{coordenada } x \textit{ de } 2P \ = \ \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Por razones que ya veremos, la coordenada x de $2P$ resulta más útil que la coordenada y, así que preferimos dejarla de lado y no seguir recargándonos de fórmulas.

Vamos a mostrar algunos ejemplos.

Ejemplo 2.1.7. Consideremos la curva elíptica E de ecuación afín: $y^2 = x^3 + 17$ en $\mathbb{P}^2(\overline{\mathbb{Q}})$.

Tenemos en E los puntos afines $P_1 = (-1, 4)$ y $P_2 = (2, 5)$. En este caso, obtenemos:

$$\begin{aligned} \lambda = & \quad \frac{y_2 - y_1}{x_2 - x_1} = \frac{1}{3}. \\ \nu = & \quad y_1 - \lambda x_1 = \frac{13}{3}. \end{aligned}$$

Con lo cual, si $P_3 = P_1 + P_2$, con $P_3 = (x_3, y_3)$,

$$\begin{aligned} x_3 = & \quad \lambda^2 - a - x_1 - x_2 = \quad -\frac{8}{9}. \\ y_3 = & \qquad\qquad -\lambda x_3 - \nu = \quad -\frac{109}{27}. \end{aligned}$$

O sea: $(-1, 4) + (2, 5) = (-\frac{8}{9}, -\frac{109}{27})$.

También podemos aplicar la fórmula de duplicación. Si llamamos $2P_1 = (x, y)$ tenemos que $x = \frac{137}{64}$.

Finalizando con esta parte, vamos a establecer un vínculo entre dos cosas que hemos considerado. Vimos que, dada una curva no singular $\mathcal{C}$, podemos asociarle un grupo abeliano, que hemos notado $\mathcal{P}ic^{\circ}(\mathcal{C})$, y que está formado por los divisores de grado cero, mirando sus clases al dividir por el subgrupo de los divisores principales. Pero si la curva $\mathcal{C}$ es una curva elíptica, tenemos otro grupo abeliano para asociarle, que es el que notamos $\mathcal{C}(\overline{K})$, formado por los puntos de $\mathcal{C}$ y con la operación de grupo que definimos. Cabe preguntarse si podemos establecer alguna relación entre estos dos grupos. La respuesta es afirmativa como lo precisamos en la siguiente proposición:

Proposición 2.1.8. *Sea E una curva elíptica en $\mathbb{P}^2(\overline{K})$. Se tiene la siguiente aplicación:*

$$\begin{aligned} \sigma : E(\overline{K}) &\longrightarrow \mathcal{P}ic^{\circ}(E) \\ P &\longmapsto [(P) - (\mathcal{O})] \end{aligned}$$

Donde $[(P) - (\mathcal{O})]$ denota la clase del divisor $(P) - (\mathcal{O})$ en $\mathcal{P}ic^{\circ}(E)$. Resulta que σ es una aplicación biyectiva, por lo que induce una estructura de grupo en el conjunto $E(\overline{K})$. Se tiene además que la ley de grupo en $E(\overline{K})$ inducida por σ coincide con la ley de grupo definida en la Proposición 2.1.6.

Demostración: Ver [9], Capítulo III, Proposición 3.4. □

Observación 2.1.9. La proposición anterior, además de ser un resultado muy interesante porque nos permite tener otra representación del grupo $E(\overline{K})$, resulta muy práctica para ahorrarnos algunas cuentas. Ya hemos comentado que, si bien no es difícil probar que la ley de grupo que uno define en $E(\overline{K})$ es asociativa, sí resulta ser engorroso. Pero ahora tenemos una prueba alternativa. Dado que la ley de grupo en $E(\overline{K})$ coincide con la ley de grupo en $\mathcal{P}ic^{\circ}(E)$, sólo basta verificar que ésta última es asociativa. Pero eso es trivial.

Por último, hay otro interesante corolario que se puede obtener a partir de la Proposición 2.1.8. El resultado siguiente lo vamos a usar más adelante.

Corolario 2.1.10. *Sea E una curva elíptica y sea $D = \sum n_p(P) \in \mathcal{D}iv(E)$. Entonces:*

$$D \sim 0 \Leftrightarrow \sum n_p = 0 \ \ y \ \ \sum [n_p]\,(P) = \mathcal{O}.$$

Demostración: Ver [9], Capítulo III, Corolario 3.5. □

2.2. Teorema de Mordell-Weil

Hasta ahora hemos trabajado con curvas elípticas cualesquiera en $\mathbb{P}^2(\overline{K})$. Ahora nos vamos a limitar a aquellas que están definidas sobre K. O sea, que pueden darse con una ecuación con coeficientes en K. Para esta parte el cuerpo K va a ser un cuerpo de números; es decir, una extensión finita de $\mathbb{Q}$. En esta familia de curvas uno puede considerar el subgrupo de $E(\overline{K})$ formado por los puntos que son K-racionales. En seguida verificaremos que es efectivamente un subgrupo. A este subgrupo nos dedicaremos a continuación.

2.2.1. El grupo de puntos K-racionales

Efectivamente, dada una curva elíptica E definida sobre K, el conjunto de puntos K-racionales de E es un subgrupo de $E(\overline{K})$. Esto no es para nada sorprendente. Seamos precisos y fijemos una tal curva dada por la siguiente ecuación:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3,$$

donde $a, b, c \in K$, y cuya afinización en $Z = 1$ es:

$$y^2 = x^3 + ax^2 + bx + c.$$

Recordemos que el único punto de E que no está en esta afinización es $\mathcal{O} = [0 : 1 : 0]$.

Consideramos el subconjunto de $E(\overline{K})$ formado por los puntos que son K-racionales que incluye, claro está, a $\mathcal{O}$. A este conjunto lo notamos $E(K)$. La proposición siguiente formaliza lo que ya anticipamos.

Proposición 2.2.1. *Sea K un cuerpo de números y $\overline{K}$ una clausura algebraica fija. Sea E una curva elíptica en $\mathbb{P}^2(\overline{K})$ definida sobre K. Entonces $E(K) \subseteq E(\overline{K})$ es un subgrupo.*

Demostración: Para verificar que $E(K)$ es un subgrupo de $E(\overline{K})$ necesitamos primero que el neutro $\mathcal{O}$ pertenezca a $E(K)$, lo cual ya sabemos que es cierto.

Además tenemos que verificar que la operación de grupo es cerrada dentro de $E(K)$. Es decir, que si $P, Q \in E(K)$ entonces $P+Q \in E(K)$. Pero esto es muy sencillo. En primer lugar, si $P = \mathcal{O}$ o $Q = \mathcal{O}$, nada hay que probar. Si $P \neq \mathcal{O}$ y $Q \neq \mathcal{O}$ podemos trabajar en el plano afín $Z = 1$ y usar las fórmulas de adición que explicitamos en Proposición 2.1.6. De este modo, si $P \neq Q$ y $P \neq -Q$, la fórmula para las coordenadas de $P + Q$ resulta ser suma, producto y cocientes de escalares de K. En efecto, recordemos que para obtener $P \star Q$ planteábamos el sistema:

$$S : \begin{cases} y^2 - x^3 - ax^2 - bx - c & = 0 \\ Ax + By + C & = 0 \end{cases}$$

En nuestro contexto, como E está definida sobre K y $P, Q \in E(K)$; tenemos que $a, b, c, A, B, C \in K$. Entonces las coordenadas x de P, Q y $P \star Q$ resultan ser las 3 raíces de un polinomio de grado 3 con coeficientes en K. Dado que P y Q tienen coordenadas en K, 2 de esas raíces pertenecen a K; por lo que, necesariamente, la tercera también. Así es que la coordenada x de $P \star Q$ está en K. Y mirando la segunda ecuación del sistema S, resulta que la coordenada y también. Luego $P \star Q \in E(K)$; y siguiendo con un razonamiento análogo, concluimos que $P + Q \in E(K)$.

Si $P = Q$ sacamos la misma conclusión y más aún si $P = -Q$. Con lo cual, en cualquier caso, la suma es cerrada en $E(K)$.

Por último veamos que si $P \in E(K)$ entonces $-P \in E(K)$. Esto también es inmediato, pues recordemos que si $P = (x, y)$ entonces $-P = (x, -y)$. Con lo cual no hay nada que decir y esto concluye la demostración. □

Podemos observar, si nos remitimos al Ejemplo 2.1.7, que allí sumamos dos puntos de $E(\mathbb{Q})$; y obviamente obtuvimos otro punto de $E(\mathbb{Q})$. Nos dio que $(-1,4)+(2,5)=(-\frac{8}{9},-\frac{109}{27})$.

Nuestro próximo objetivo es dar una idea de un resultado trascendental que es el **Teorema de Mordell-Weil**, que afirma que el grupo $E(K)$ es finitamente generado. Para eso tendremos que hacer algunas construcciones que también son interesantes en sí.

2.2.2. Teorema débil de Mordell-Weil

Como dijimos, para poder encaminarnos hacia el Teorema de Mordell-Weil, necesitamos pasar antes por algunos resultados. Uno de ellos es el Teorema débil de Mordell-Weil. Es una primera aproximación que parece un poco técnica pero es fundamental para llegar a nuestro objetivo. El teorema es el siguiente.

Teorema 2.2.2. (*Teorema débil de Mordell-Weil*) *Sea K un cuerpo de números y E una curva elíptica definida sobre K. Si $m \geq 2$ es un número entero, entonces:*

$$\frac{E(K)}{mE(K)},$$

es un grupo finito.

Demostración: Ver [9], Capítulo VIII, Teorema 1.1. □

2.2.3. Alturas y Teorema de Mordell-Weil

Con la meta de poder presentar las herramientas que se utilizan para demostrar el Teorema de Mordell-Weil, en esta sección introduciremos la noción de altura; que también nos será muy útil para otros propósitos.

El Teorema de Mordell-Weil será una consecuencia inmediata del Teorema débil y de lo que se llama el Teorema del Descenso. El Teorema del Descenso lo vamos a aplicar en nuestro caso al grupo de puntos K-racionales de una curva elíptica; pero es un teorema que se refiere a grupos abelianos en general, así que lo enunciaremos con toda su generalidad.

Teorema 2.2.3. (*Teorema del descenso*) *Sea A un grupo abeliano. Supongamos que se tiene una "función de altura":*

$$h : A \longrightarrow \mathbb{R},$$

que satisface las siguientes propiedades:

a) Dado $Q \in A$, existe una constante C_1, que depende de A y de Q, tal que para todo $P \in A$ se tiene:

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

b) Existe un número entero $m \geq 2$ y una constante C_2, que depende de A, tal que para todo $P \in A$ se tiene:

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

c) Para cada constante C_3, el conjunto $\{P \in A : h(P) \leq C_3\}$ es un conjunto finito.

Si además, para el entero m de b), el grupo cociente $\frac{A}{mA}$ es finito, entonces A es finitamente generado.

Demostración: Ver [9], Capítulo VIII, Proposición 3.1. □

El Teorema del Descenso nos dice que si tenemos un grupo abeliano A dotado de una *función de altura* $h : A \longrightarrow \mathbb{R}$ que satisface ciertas propiedades, A resulta ser un grupo finitamente generado. Como nuestro objetivo es acercarnos al Teorema de Mordell-Weil, que dice que $E(K)$ es un grupo finitamente generado, para aplicar el Teorema del Descenso necesitamos disponer de esa función de altura h. Eso es lo que vamos a construir a continuación.

Alturas sobre curvas elípticas

Si bien se puede definir la noción de altura en curvas elípticas sobre cualquier cuerpo de números K, nosotros vamos a limitarnos a hacer la construcción sobre $\mathbb{Q}$. No sólo para simplificar, sino también porque es el caso que realmente nos va a interesar más adelante. Empecemos por la noción de altura en $\mathbb{Q}$.

Definición 2.2.4. Sea $t \in \mathbb{Q}$, digamos $t = \frac{p}{q}$, con p y q coprimos. La *altura* de t se define como:

$$H(t) = máx\left\{|p|, |q|\right\}.$$

Naturalmente podemos extender la noción de altura al espacio $\mathbb{P}^n(\mathbb{Q})$ del siguiente modo. Dado $P \in \mathbb{P}^n(\mathbb{Q})$, multiplicando por números enteros convenientes podemos suponer que:

$$P = [x_0 : \cdots : x_n],$$

donde $x_0, ..., x_n \in \mathbb{Z}$ y $gcd(x_0, ..., x_n) = 1$. En tal caso definimos la *altura* de P como:

$$H(P) = máx\left\{|x_0|, ..., |x_n|\right\}.$$

Observemos que es sencilla la definición de altura si trabajamos en $\mathbb{Q}$ aprovechando las bondades del dominio principal $\mathbb{Z}$. Cuando lo queremos hacer en un cuerpo de números K cualquiera tenemos que ser un poco más cuidadosos.

Consideremos ahora una curva elíptica E definida sobre $\mathbb{Q}$. Dada una función $f \in \mathbb{Q}(E)$ del cuerpo de funciones $\mathbb{Q}$-racionales de E, que no sea constante, recordando el Ejemplo 1.3.15

podemos construir un morfismo de curvas suryectivo, que también notamos f, dado por:

$$f: \quad \begin{array}{ccl} E & \to & \mathbb{P}^1 \\ P & \to & \begin{cases} [f(P):1] & \textit{si } f \textit{ es regular en } P \\ [1:0] & \textit{si } f \textit{ tiene un polo en } P \end{cases} \end{array}$$

Ahora ya podemos dar la noción de altura en curvas elípticas que queríamos.

Definición 2.2.5. Sea E una curva elíptica definida sobre $\mathbb{Q}$ y sea $f \in \mathbb{Q}(E)$ una función no constante. La *altura en E relativa a f* es la función:

$$\begin{array}{rccl} h_f: & E(\mathbb{Q}) & \longrightarrow & \mathbb{R} \\ & P & \longrightarrow & \log H(f(P)) \end{array}$$

Donde $f(P)$ es la imagen de P a través de la función $f : E \longrightarrow \mathbb{P}^1$ inducida por f.

El hecho aparentemente arbitrario de considerar el logaritmo se debe a su comportamiento aditivo, que nos va a resultar más conveniente que el comportamiento multiplicativo de H.

Observación 2.2.6. En realidad la construcción es más general y la altura H puede extenderse a $\mathbb{P}^n(\overline{\mathbb{Q}})$; de manera que se puede definir:

$$\begin{array}{rccl} h_f: & E(\overline{\mathbb{Q}}) & \longrightarrow & \mathbb{R} \\ & P & \longrightarrow & \log H(f(P)) \end{array}$$

para una curva elíptica E cualquiera (no necesariamente definida sobre $\mathbb{Q}$) y $f \in \overline{\mathbb{Q}}(E)$. Sin embargo nos interesa analizar el comportamiento de la altura sobre el subgrupo $E(\mathbb{Q})$; que es lo que implica que valga el Teorema de Mordell-Weil.

Esta función de altura es la que se necesita para aplicar el Teorema del Descenso y con lo que se puede probar el Teorema de Mordell-Weil.

Teorema de Mordell-Weil sobre $\mathbb{Q}$

He aquí uno de los resultados más importantes sobre curvas elípticas.

Teorema 2.2.7. (*Teorema de Mordell-Weil*). *Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces el grupo $E(\mathbb{Q})$ es finitamente generado.*

Demostración: Ver [9], Capítulo VIII, Teorema 4.1. □

Observación 2.2.8. Como hemos comentado, hicimos la construcción de la altura sólo en $\mathbb{Q}$, pero la noción de altura también se tiene sobre cualquier cuerpo de números K y el Teorema de Mordell-Weil también vale en ese caso. De todas formas el caso $K = \mathbb{Q}$ es el que nos va a interesar más adelante.

El Teorema de Mordell-Weil nos dice que existen finitos puntos $P_1, ..., P_n \in E(\mathbb{Q})$ tales que cualquier otro punto de $E(\mathbb{Q})$ se obtiene como combinación lineal (con la operación suma en E) de los puntos $P_1, ..., P_n$. Esto no sólo es interesante y tal vez sorprendente en sí mismo; también tiene una consecuencia inmediata que nos permite caracterizar mejor al grupo $E(\mathbb{Q})$. Recordemos el siguiente resultado de grupos abelianos en general.

Proposición 2.2.9. (*Teorema de Estructura*) *Sea A un grupo abeliano finitamente generado. Entonces existe un único $r \in \mathbb{N}_0$ tal que:*

$$A \simeq \mathbb{Z}^r \oplus T,$$

donde T es la parte de torsión de A; esto es, el subgrupo formado por los elementos de orden finito.

Al número r se lo llama el rango *de A.*

Esto nos permite concluir que el grupo $E(\mathbb{Q})$ tiene esa forma; y a partir de ello se trata de estudiarlo para conocerlo lo más que se pueda. Concretamente, dada una curva elíptica E definida sobre $\mathbb{Q}$, los problemas que uno se plantea son dos:

1) Explicitar el subgrupo T

2) Hallar el rango

Estos dos problemas, hoy por hoy, involucran una dificultad bien distinta. Ocurre que hay varios resultados conocidos que permiten calcular el grupo T con total exactitud. Sin embargo, el problema de hallar el rango aún no ha podido ser resuelto en general. Todavía es poco lo que se sabe al respecto. Por ejemplo, no se sabe si el rango puede tomar valores arbitrariamente grandes. De hecho el valor más alto que se conoce es 28. Estas cuestiones las retomaremos más adelante.

En ejemplos no demasiado complicados, con un poco de trabajo, se puede calcular explícitamente el grupo $E(\mathbb{Q})$. No vamos a mostrar cómo es que se llega a estos resultados, pero listamos aquí algunos ejemplos:

1) $E : y^2 = x^3 - x$.

$$E(\mathbb{Q}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Más aún: $E(\mathbb{Q}) = \{\mathcal{O}; (0,0); (1,0); (-1,0)\}$. Aquí el rango es 0. Todos los puntos son de torsión.

2) $E : y^2 = x^3 + x$.

$$E(\mathbb{Q}) \simeq \mathbb{Z}_2.$$

Aquí: $E(\mathbb{Q}) = \{\mathcal{O}; (0,0)\}$.

3) $E : y^2 = x^3 - 5x$. Aquí se tiene que el rango es 1. Notemos que, en particular, esto dice que la ecuación:

$$y^2 = x^3 - 5x,$$

tiene *infinitas* soluciones $(x, y) \in \mathbb{Q}^2$.

2.2.4. Altura Canónica

A partir de la altura que hemos definido antes podemos hacer una construcción que mucho tiene que ver con el rango y la torsión de una curva elíptica E. A esto nos dedicamos en esta parte. Tomando como punto de partida las alturas h_f que usamos, uno puede construir una función de altura *global* para una curva elíptica cuyas propiedades son muy útiles a la hora de intentar calcular el grupo $E(\mathbb{Q})$. Antes necesitamos el siguiente lema.

Lema 2.2.10. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Sea $f \in \mathbb{Q}(E)$ una función no constante y par (esto es, $f \circ [-1] = f$, donde $[-1](P) = -P$). Entonces, para cada $P \in E(\overline{\mathbb{Q}})$, el límite:*

$$\frac{1}{deg(f)} \lim_{n\to\infty} \frac{1}{4^n} h_f([2^n]\, P),$$

existe y es independiente de f.

Demostración: Ver [9], Capítulo VIII, Proposición 9.1. □

Este lema nos asegura que la definición siguiente tiene consistencia.

Definición 2.2.11. Sea E una curva elíptica definida sobre $\mathbb{Q}$. La *altura canónica* de E es la función:

$$\hat{h} : E(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R},$$

dada por:

$$\hat{h}(P) = \frac{1}{deg(f)} \lim_{n\to\infty} \frac{1}{4^n} h_f([2^n]\, P).$$

Donde $f \in \mathbb{Q}(E)$ es cualquier función no constante y par.

La altura canónica, como dijimos, satisface propiedades muy útiles. Compilamos algunas de ellas en el siguiente resultado.

Teorema 2.2.12. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ y $\hat{h}$ su altura canónica.*

a) Para cada $P, Q \in E(\overline{\mathbb{Q}})$ se tiene la ley del paralelogramo:

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

b) Para todo $P \in E(\overline{\mathbb{Q}})$ *y* $m \in \mathbb{Z}$,

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

c) $\hat{h}$ *es una forma cuadrática en* $E(\overline{\mathbb{Q}})$*. En otras palabras,* $\hat{h}$ *es par y la aplicación:*

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

es una forma bilineal.

d) Sea $P \in E(\overline{\mathbb{Q}})$*. Entonces* $\hat{h}(P) \geq 0$ *y:*

$$\hat{h}(P) = 0 \Longleftrightarrow P \text{ es un punto de torsión.}$$

e) Sea $f \in \mathbb{Q}(E)$ *una función par. Entonces:*

$$(deg(f))\hat{h} = h_f + O(1).$$

Esto es, existen constantes C_1 *y* C_2 *que dependen de* E *y de* f *tales que:*

$$C_1 \leq (deg(f))\hat{h}(P) - h_f(P) \leq C_2 \quad , \forall P \in E(\overline{\mathbb{Q}}).$$

Además, si $\hat{h}' : E(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}$ *es otra función que satisface e) para alguna función* f *no constante, y b) para algún entero* $m \geq 2$*; entonces* $\hat{h}' = \hat{h}$*.*

Demostración: Ver [9], Capítulo VIII, Teorema 9.3. □

Este teorema nos permite, entre otras cosas, caracterizar los puntos de torsión de la curva E. De todas maneras, a los efectos prácticos no pareciera muy fácil de calcular el número $\hat{h}(P)$ para poder encontrarlos de un modo eficiente.

Por otro lado, tenemos que $\hat{h}$ es una forma cuadrática en $E(\overline{\mathbb{Q}})$ y que *d)* nos dice que vale cero en los puntos de torsión exactamente. Si nos limitamos a mirar a $\hat{h}$ sólo en $E(\mathbb{Q})$, podemos pensar que induce una forma cuadrática:

$$\hat{h}\ :\ \frac{E(\mathbb{Q})}{T} \longrightarrow \mathbb{R},$$

definida positiva. Pero dado que:

$$\frac{E(\mathbb{Q})}{T} \simeq \mathbb{Z}^r\,;$$

si consideramos la forma bilineal asociada tenemos un resultado muy útil. Pues, la forma bilineal asociada:

$$\langle\ ,\ \rangle\ :\ \frac{E(\mathbb{Q})}{T} \times \frac{E(\mathbb{Q})}{T}\ \longrightarrow \mathbb{R},$$

es no degenerada. Entonces, si tenemos $P_1, ..., P_s \in E(\mathbb{Q})$, y construimos la matriz:

$$M = (\langle P_i, P_j \rangle)_{1 \leq i,j \leq s} ;$$

resultará que si $det(M) \neq 0$, los puntos $P_1, ..., P_s$ son linealmente independientes en $\frac{E(\mathbb{Q})}{T} \simeq \mathbb{Z}^r$. Con lo cual, necesariamente $r \geq s$.

Es decir, tenemos una manera, que podrá ser cómoda o no, según el caso, de acotar inferiormente el rango de la curva elíptica E. Sobre esta idea volveremos en los siguientes capítulos.

Hasta acá se podría decir que ha llegado la primera parte del trabajo. Hemos dado todos los ingredientes necesarios para encarar la segunda parte, que es la que más nos interesa. Vamos a seguir trabajando con curvas elípticas pero el contexto será otro y por ello aparecerán construcciones nuevas; algunas de las cuales son generalizaciones de las que hasta aquí presentamos.

Capítulo 3

Curvas Elípticas sobre $\overline{\mathbb{Q}(t)}$ - Superficies Elípticas

Este es el capítulo central de todo el trabajo. Hasta ahora, para tener la noción de rango, nos limitamos a considerar curvas elípticas definidas sobre cuerpos de números. Pues ahí vimos que vale el Teorema de Mordell-Weil así el concepto de rango tiene sentido.

Ahora vamos a considerar curvas elípticas sobre el cuerpo $\overline{\mathbb{Q}(t)}$ y vamos a poder decir mucho más. No va a ser una simple generalización, porque al estar involucrada la indeterminada t la construcción adquiere mucha más riqueza. Vamos a hacer un juego de mirar la curva sobre $\overline{\mathbb{Q}(t)}$ y trazar un paralelo al considerar a t como una variable más obteniendo así una *superficie* sobre $\overline{\mathbb{Q}}$. Y allí es donde entrarán en juego muchos condimentos de la Geometría Algebraica. Pero no estamos haciendo más que una brevísima introducción. Empecemos a precisar las ideas.

3.1. Curvas Elípticas sobre $\overline{\mathbb{Q}(t)}$

Mirando la definición de Curva Elíptica que dimos en el **Capítulo 2**, si tomamos $K = \mathbb{Q}(t)$, tenemos un caso particular y no hay nada nuevo. O sea, considerar curvas elípticas sobre el cuerpo $\overline{\mathbb{Q}(t)}$ no es más que un posible ejemplo que uno puede trabajar. De manera que, en principio, no habría mucho que decir; pues ya está todo dicho. Sin embargo es mucho lo que se puede hacer, y en este trabajo sólo mostramos algo de eso. Empecemos mostrando un sencillo ejemplo.

Una curva elíptica definida sobre $\overline{\mathbb{Q}(t)}$ podría ser:

$$E : y^2 = x^3 - t^2x + t^2.$$

Esa es la ecuación afín de E. La ecuación homogenizada sería:

$$E : Y^2Z = X^3 - t^2XZ^2 + t^2Z^3.$$

Observemos que es una curva definida sobre $\mathbb{Q}(t)$. En E tenemos, por ejemplo, los puntos (afines) (t,t); $(t,-t)$; $(0,t)$; $(0,-t)$; $(1,1)$; $(1,-1)$. Este es un ejemplo que trabajaremos mucho de acá en más.

El primer planteo que nos hacemos es el siguiente. Hasta antes de empezar a hablar del Teorema de Mordell-Weil y de Alturas, el cuerpo K podía ser cualquiera de característica distinta de 2 y de 3. La pregunta es si vale el Teorema de Mordell-Weil sobre $\mathbb{Q}(t)$ y, en tal caso, cuál es el concepto de altura que se define. La respuesta es esencialmente afirmativa; vale el teorema, agregando cierta hipótesis; y para mostrar esto empezaremos hablando de la noción de altura en curvas definidas sobre $\overline{\mathbb{Q}(t)}$. Antes de esto vamos a hacer un comentario.

Observación 3.1.1. En realidad considerar el cuerpo $\mathbb{Q}(t)$ es un caso particular de algo un poco más general.

Tomamos como punto de partida cualquier cuerpo K y una clausura algebraica fija $\overline{K}$. Supongamos que tenemos una curva proyectiva no singular $\mathcal{C}$ en $\mathbb{P}^2(\overline{K})$ definida sobre K. Tenemos su cuerpo de funciones K-racionales: $k = K(\mathcal{C})$; y tomamos una clausura algebraica $\overline{k}$. Podemos considerar entonces las curvas elípticas definidas sobre ese cuerpo $\overline{k}$. Cuando miramos las curvas elípticas definidas sobre $\overline{\mathbb{Q}(t)}$ estamos haciendo exactamente eso para una curva $\mathcal{C}$ particular. Si tomamos $K = \mathbb{Q}$, y consideramos la curva:

$$\mathcal{C} \,:\, y = 0, \, o\, sea, \; \mathcal{C} = \mathbb{P}^1(\overline{\mathbb{Q}}),$$

entonces:

$$\mathbb{Q}(\mathcal{C}) = Fracc\left(\frac{\mathbb{Q}\,[x,y]}{(y)}\right) = Fracc(\mathbb{Q}\,[x]) = \mathbb{Q}(x).$$

De manera que la construcción que vamos a hacer podría ser más general, y cuando valga la pena comentaremos si hay algo que cambia cuando generalizamos; pero esencialmente nos interesa el caso en que el cuerpo de funciones K-racionales en cuestión resulta ser $\mathbb{Q}(t)$; es decir, la curva de base es $\mathcal{C} = \mathbb{P}^1(\overline{\mathbb{Q}})$.

3.1.1. Alturas en curvas elípticas definidas sobre $\overline{\mathbb{Q}(t)}$

Así como hicimos en el caso de cuerpos de números, empecemos por la noción de altura en $\mathbb{Q}(t)$. Para que se entienda mejor, va a ser conveniente trabajar primero en general con cualquier curva de base no singular $\mathcal{C}$; y después considerar nuestro caso particular $\mathcal{C} = \mathbb{P}^1(\overline{\mathbb{Q}})$.

Definición 3.1.2. Sea $\mathcal{C}$ una curva no singular definida sobre $\mathbb{Q}$. Llamemos $k = \mathbb{Q}(\mathcal{C})$ y sea $f \in k^\times$. Definimos la *altura* de f como:

$$h(f) = \sum_{p \in \mathcal{C}} máx\left\{ord_p(f), 0\right\} = \sum_{p \in \mathcal{C}} máx\left\{-ord_p(f), 0\right\}.$$

Y definimos $h(0) = 0$.

En primer lugar observemos que, como $\mathcal{C}$ es no singular, tiene sentido considerar $ord_p(f)$. Por otro lado, la Proposición 1.3.12 nos asegura que la suma es finita. Y además, como vimos en la Proposición 1.3.20, $deg(div(f)) = 0$; lo que nos dice que ambas sumas son efectivamente iguales.

Observación 3.1.3. Hay un resultado que dice que esta definición es equivalente a la siguiente:

$$h(f) = deg(f);$$

donde f es la función inducida del Ejemplo 1.3.15. Sin embargo vamos a trabajar con la otra definición; por lo que no nos preocuparemos en mostrar esta equivalencia.

Ejemplo 3.1.4. Aprovechemos algunas cuentas que ya hicimos. En el Ejemplo 1.3.13, a partir de la curva $E : y^2 = x^3 + x$; hemos calculado algunos divisores. Si:

$$F(X, Y, Z) = \frac{X}{Z},$$

siguiendo con la notación de 1.3.13, vimos que:

$$div(F) = 2(P_1) - 2(P_2).$$

Por lo tanto,

$$h(F) = 2.$$

Del mismo modo, si:

$$G(X, Y, Z) = \frac{Y}{Z},$$

vimos que:

$$div(G) = (Q_1) + (Q_2) + (Q_3) - 3(Q_\infty).$$

Con lo cual:

$$h(G) = 3.$$

Como dijimos, la altura en $\mathbb{Q}(t)$ no es más que esto mismo en el caso particular $\mathcal{C} = \mathbb{P}^1(\overline{\mathbb{Q}})$. Para simplificar la notación, escribamos directamente $\mathbb{P}^1$ para referirnos a $\mathbb{P}^1(\overline{\mathbb{Q}})$.

Ahora bien; los puntos afines $p \in \mathbb{P}^1$ son los de la forma $p = (x, 0)$. En coordenadas homogéneas, son los puntos $p = [x : 0 : 1]$. Además $\mathbb{P}^1$ contiene un punto en el infinito; o sea, que no pertenece a la afinización $Z = 1$, que es $p_\infty = [1 : 0 : 0]$. Podemos unificar esto usando coordenadas homogéneas diciendo que los puntos de $\mathbb{P}^1$ son los de la forma:

$$p = [X : 0 : Z] .$$

Recordemos que, así como hay una correspondencia entre las variedades proyectivas y las afines; también la hay entre los polinomios pertenecientes a los ideales que definen a unas y a otras. Ya hemos mostrado cómo es el proceso de homogenización y deshomogenización de los polinomios. Y también vimos en la Observación 1.2.8 que los elementos del cuerpo de funciones de una variedad proyectiva pueden verse como cocientes de polinomios homogéneos de igual grado. Supongamos entonces que tenemos $f \in k = \mathbb{Q}(t)$. Si pensamos a k como el cuerpo de funciones de $\mathbb{P}^1$ entonces f debe admitir una escritura como cociente de polinomios homogéneos de igual grado; y esta escritura tiene la ventaja de permitirnos la evaluación en todos los puntos de $\mathbb{P}^1$, tanto los afines como los del infinito (que hay uno solo y es el que notamos p_∞). Hagamos esto con cuidado.

Los polinomios homogéneos del anillo de coordenadas $\mathbb{Q}$-racionales de $\mathbb{P}^1$ son polinomios en las variables X y Z. Pues $Y = 0$ en $\mathbb{Q}\left[\mathbb{P}^1\right]$. Pero a los efectos de que haya compatibilidad con la notación actual y sobretodo con las que van a venir; a las coordenadas homogéneas las vamos a renombrar. En lugar de usar las variables X y Z usaremos las variables T y U. Insistimos, sólo es para que no haya confusiones después. Así que los polinomios homogéneos de $\mathbb{Q}\left[\mathbb{P}^1\right]$ serán polinomios en las variables T y U. De este modo, si tomamos $f \in \mathbb{Q}(t)$; digamos, por ejemplo:

$$f(t) = 1 + 2t - 3t^3 \ ;$$

podemos pasarlo a coordenadas homogéneas y obtenemos:

$$F(T,U) = 1 + 2\frac{T}{U} - 3\frac{T^3}{U^3} = \frac{U^3 + 2TU^2 - 3T^3}{U^3}$$

O si tomamos:

$$f(t) = \frac{3 - t^2 + 4t^5}{1 + 2t} \ ;$$

al pasar a coordenadas homogéneas nos queda:

$$F(T,U) = \frac{3 - \frac{T^2}{U^2} + 4\frac{T^5}{U^5}}{1 + 2\frac{T}{U}} = \frac{3U^5 - T^2U^3 + 4T^5}{U^5 + 2TU^4}.$$

O sea, F es una función definida en todos los puntos de coordenadas homogéneas $[T : U]$.

Así como lo comentamos antes, también podemos hacer el proceso inverso y pasar de coordenadas homogéneas a coordenadas afines haciendo $U = 1$.

Habiendo hecho todas estas consideraciones volvamos a lo nuestro y tratemos de escribir la definición de altura sobre $\mathbb{Q}(t)$. Como dijimos, es la misma definición que ya vimos, pero en un caso particular. Pero observando justamente la particularidad del caso, podemos dar una definición tal vez más concisa. Ocurre que si trabajamos en la afinización $U = 1$; hay un único punto en el infinito, que es $p_\infty = [1 : 0]$. Entonces si tomamos $f \in \mathbb{Q}(t)$ y queremos calcular los números $ord_p(f)$ para cada $p \in \mathbb{P}^1$; para todos menos uno, podemos trabajar con coordenadas afines. Con lo cual no nos salimos de $\mathbb{Q}(t)$ y a f lo dejamos tal como está. Sólo hay que hacer el cálculo aparte de $ord_{p_\infty}(f)$; y allí habrá que pasar f a coordenadas homogéneas. Podemos entonces usar una notación más cómoda:

$$\begin{aligned} p = [t : 1] \ &\Rightarrow \ ord_p(f) = ord_t(f) \\ p = [1 : 0] \ &\Rightarrow \ ord_p(f) = ord_\infty(f) \end{aligned}$$

Por ejemplo, sea:

$$f(t) = t^3 - t^2 = t^2(t - 1).$$

Los puntos afines en los que f tiene polos o ceros son exactamente: $p_1 = 0$ y $p_2 = 1$ (o sea, $p_1 = [0 : 1]$ y $p_2 = [1 : 1]$); en los que tiene un cero.

Calculemos el orden de f en esos puntos. Trabajamos en el afín $U = 1$. El anillo de coordenadas $\mathbb{Q}$-racionales en esta afinización es justamente $\mathbb{Q}(t)$. Dado que estamos trabajando con $\mathbb{P}^1$, que es una curva sumamente sencilla, el cálculo del orden va a ser inmediato. El ideal maximal asociado al punto afín $p_1 = 0$ es:

$$\mathcal{M}_{p_1} = (t).$$

Por lo que:

$$ord_{p_1}(f) = ord_{p_1}(t^2(t-1)) = 2ord_{p_1}(t) + ord_{p_1}(t-1) = 2.$$

El ideal maximal asociado al punto afín $p_2 = 1$ es:

$$\mathcal{M}_{p_2} = (t-1).$$

Por lo que:

$$ord_{p_2}(f) = ord_{p_2}(t^2(t-1)) = ord_{p_2}(t^2) + ord_{p_2}(t-1) = 1.$$

Sólo nos falta analizar el único punto que queda afuera en esta afinización, que es $p_\infty = [1:0]$. Para ello escribamos f en coordenadas homogéneas:

$$F(T,U) = \frac{T^3}{U^3} - \frac{T^2}{U^2} = \frac{T^3 - T^2U}{U^3}.$$

Recordemos que, como sabemos que $deg(div(F)) = 0$, podemos calcular el orden en p_∞ sin hacer la cuenta explícita; pero hagámosla para que quede más claro.

En el punto $p_\infty = [1:0]$, F tiene un polo. Por esta razón, su orden en ese punto va a ser negativo; de manera que, para calcular la altura de f, no haría falta tenerlo en cuenta. Pero sigamos con el cálculo. Para saber el orden del polo de f en ese punto afinizamos ahora en la otra variable y hacemos $T = 1$. Aquí, el anillo de coordenadas es $\mathbb{Q}(u)$; y p_∞ es el punto afín $p_\infty = 0$ (lo llamamos igual). Además F adquiere la siguiente forma:

$$f(u) = \frac{1-u}{u^3}.$$

El ideal maximal asociado al punto es:

$$\mathcal{M}_{p_\infty} = (u).$$

Por lo tanto:

$$ord_{p_\infty}(f) = ord_{p_\infty}(\frac{1-u}{u^3}) = ord_{p_\infty}(1-u) - 3ord_{p_\infty}(u) = -3.$$

Luego:

$$h(f) = 3.$$

Con estas notaciones y este procedimiento en mente escribamos la definición de altura sobre $\mathbb{Q}(t)$.

Definición 3.1.5. Sea $f \in \mathbb{Q}(t)$. Definimos la *altura* de f como:

$$h(f) = \sum_{t \in \bar{\mathbb{Q}} \cup \{\infty\}} máx\left\{ord_t(f), 0\right\} = \sum_{t \in \bar{\mathbb{Q}} \cup \{\infty\}} máx\left\{-ord_t(f), 0\right\}.$$

Donde $ord_\infty(f)$ es el orden de f en el punto $[1:0]$.

Teniendo esta definición, como hicimos antes, construimos una noción de altura sobre curvas elípticas definidas sobre $\mathbb{Q}(t)$.

Definición 3.1.6. Sea E una curva elíptica definida sobre $\mathbb{Q}(t)$. La *altura* sobre E es la función:

$$\begin{aligned} h_E &: E(\mathbb{Q}(t)) \longrightarrow \mathbb{R} \\ h_E(P) &= \begin{cases} h_x(P) = h(x) & \text{si } P = (x, y) \\ 0 & \text{si } P = \mathcal{O} \end{cases} \end{aligned}$$

Observación 3.1.7. En el caso general, si $k = \mathbb{Q}(\mathcal{C})$, la definición es exactamente la misma.

Ejemplo 3.1.8. Volvamos al ejemplo del principio:

$$E : y^2 = x^3 - t^2 x + t^2.$$

Algunas alturas de sus puntos son:

$$\begin{aligned} P_1 = (t, t) &\Rightarrow h_E(P_1) = h(t) = 1 \\ P_2 = (t, -t) &\Rightarrow h_E(P_2) = h(t) = 1 \\ P_3 = (0, t) &\Rightarrow h_E(P_3) = h(0) = 0 \end{aligned}$$

El siguiente paso es ver si esta definición de altura tiene las buenas propiedades que tiene la altura que definimos en curvas definidas sobre cuerpos de números. En efecto, tenemos el siguiente teorema.

Teorema 3.1.9. *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(t)$ y sea h_E su función de altura. Entonces:*

a) $h_E([2]\,P) = 4h_E(P) + O(1),\ \forall P \in E(k)$.

(*Esto es; existen constantes C_1 y C_2, que dependen sólo de E, tales que $C_1 \leq h_E([2]\,P) - 4h_E(P) \leq C_2,\ \forall P \in E(k)$).*

b) $h_E(P+Q) + h_E(P-Q) = 2h_E(P) + 2h_E(Q) + O(1),\ \forall P, Q \in E(k)$.

(*O sea; existen constantes D_1 y D_2, que dependen sólo de E, tales que $D_1 \leq h_E(P+Q) + h_E(P-Q) - 2h_E(P) - 2h_E(Q) \leq D_2,\ \forall P, Q \in E(k)$).*

Demostración: Ver [10], Capítulo III, Teorema 4.2. □

Este teorema nos asegura que la altura que definimos es una buena construcción que nos va a permitir asegurar que vale el Teorema de Mordell-Weil sobre $\mathbb{Q}(t)$.

3.1.2. Teorema de Mordell-Weil sobre $\mathbb{Q}(t)$

Queremos ahora mostrar que el teorema de Mordell-Weil que vimos que vale para curvas definidas sobre cuerpos de números también vale para curvas definidas sobre $\mathbb{Q}(t)$. Esto es, queremos ver que el grupo de puntos $\mathbb{Q}(t)$-racionales de una curva E definida sobre $\mathbb{Q}(t)$ es finitamente generado.

Recordemos cómo lo hicimos en el caso K un cuerpo de números. Pasamos primero por el Teorema débil de Mordell-Weil, y con la función de alturas usamos el Teorema del Descenso. En este caso vamos a seguir básicamente el mismo camino. También pasaremos por el Teorema débil, y con la noción de altura que acabamos de construir aplicaremos el Teorema del Descenso. Sin embargo hay ciertas diferencias sustanciales cuando uno intenta trazar el paralelo. En primer lugar, el Teorema débil en el caso $\mathbb{Q}(t)$ no es simplemente una adaptación del que ya conocemos al nuevo contexto. Para demostrarlo se requiere usar herramientas que son específicas del caso $\mathbb{Q}(t)$; por lo que hay que hacer un trabajo extra que resulta ineludible.

El enunciado del teorema es, de todas maneras, el mismo que antes. Nos vamos a reducir al caso que nos interesa, que es $m = 2$; siguiendo con la notación que usamos aquella vez.

Teorema 3.1.10. (*Teorema débil de Mordell-Weil sobre* $\mathbb{Q}(t)$). *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(t)$. Entonces el grupo cociente:*

$$\frac{E(k)}{2E(k)}.$$

es finito.

Demostración: Ver [10], Capítulo III, Teorema 2.1. □

Se tiene exactamente el mismo resultado para el caso general $k = \mathbb{Q}(\mathcal{C})$.

Como dijimos, si queremos copiar el procedimiento que seguimos cuando vimos el teorema en el caso de cuerpos de números, tendríamos que verificar que la función de altura que definimos satisface las hipótesis necesarias para aplicar directamente el Teorema del Descenso. El Teorema 3.1.9 parece sugerir que efectivamente ocurre lo que necesitamos; sin embargo hay una propiedad más que nos hace falta y es la siguiente:

$$\{P \in E(k) \,:\, h_E(P) \leq C\} \text{ es un conjunto finito para cualquier constante } C.$$

Lamentablemente esto no es cierto si no le agregamos una hipótesis a la curva E. La condición parece un poco técnica, pero si uno lo medita un poco se da cuenta de que es razonable que se pida.

Definición 3.1.11. Sea E una curva elíptica definida sobre $k = \mathbb{Q}(\mathcal{C})$. Decimos que E *se descompone* (splits) si existe una curva elíptica E_0 definida sobre $\mathbb{Q}$ tal que E y E_0 son isomorfas.

Es muy fácil exhibir ejemplos de curvas elípticas que sí se descomponen. Tomemos $k = \mathbb{Q}(t)$ y consideremos la curva elíptica E sobre k dada por la ecuación afín:

$$E \,:\, y^2 = x^3 + 1.$$

Claramente E sí se descompone ya que podemos tomar simplemente $E_0 = E$; pues E ya está definida sobre $\mathbb{Q}$.

Dicho de manera informal, una curva sobre $\mathbb{Q}(t)$ no se descompone si la indeterminada t aparece efectivamente en su ecuación y no puede ser eliminada con un simple cambio de coordenadas. Si queremos un ejemplo en el que puede ocurrir esto último, lo podemos conseguir con el mismo que consideramos recién. A la ecuación de E multipliquémosla a ambos miembros por t^6. Nos queda:

$$t^6y^2 = t^6x^3 + t^6.$$

O, lo que es lo mismo:

$$(t^3y)^2 = (t^2x)^3 + t^6.$$

Si llamamos $x' = t^2x$ e $y' = t^3y$, observamos que: $(x, y) \in E$ si, y sólo si $(x', y') \in E'$; donde E' es la curva elíptica dada por la ecuación:

$$E' \,:\, y^2 = x^3 + t^6.$$

Esto nos dice que tenemos una aplicación:

$$\begin{array}{rcl} E & \longrightarrow & E' \\ (x, y) & \longrightarrow & (t^2x, t^3y) \end{array}$$

No es nada difícil ver que esta aplicación es en realidad un isomorfismo. De manera que, si partimos de la curva E', si bien aparece la indeterminada t en su ecuación, se puede eliminar con un cambio de coordenadas. Dicho de otra forma, E' es isomorfa a una curva elíptica definida sobre $\mathbb{Q}$, que es justamente E.

La hipótesis de que la curva elíptica E definida sobre $\mathbb{Q}(t)$ no se descomponga es realmente necesaria para que valga el Teorema de Mordell-Weil. Si no se tiene, puede no ser cierto. Esto es sencillo de ver en el caso de curvas definidas sobre $\overline{\mathbb{Q}}(t)$. En efecto, si tomamos por ejemplo la curva E de recién y la miramos en $\overline{\mathbb{Q}}(t)$, tenemos que cada punto de $E(\overline{\mathbb{Q}})$ es a su vez un punto de $E(\overline{\mathbb{Q}}(t))$. Pero como claramente $E(\overline{\mathbb{Q}})$ no puede ser finitamente generado, en consecuencia, $E(\overline{\mathbb{Q}}(t))$ tampoco.

Proposición 3.1.12. *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(t)$. Supongamos que la curva E no se descompone. Entonces:*

$$\{P \in E(k) \,:\, h_E(P) \leq C\},$$

es un conjunto finito para cualquier constante C.

Demostración: Ver [10], Capítulo III, Teorema 5.4. □

Lo mismo vale en el caso general $k = \mathbb{Q}(\mathcal{C})$.

Con todos estos ingredientes podemos dar con todo detalle el enunciado del teorema.

Teorema 3.1.13. (*Teorema de Mordell-Weil sobre* $\mathbb{Q}(t)$). *Sea E una curva elíptica sobre $k = \mathbb{Q}(t)$. Supongamos que la curva E no se descompone. Entonces el grupo $E(k)$ es finitamente generado.*

Demostración: Ver [10], Capítulo III, Teorema 6.1. □

Se tiene el mismo resultado en el caso general $k = \mathbb{Q}(\mathcal{C})$.

Obviamente, las consecuencias de este teorema son las mismas que teníamos en el caso anterior. Esto es, gracias al teorema de estructura, podemos tener una identificación del tipo:

$$E(k) \simeq \mathbb{Z}^r \oplus T.$$

3.1.3. Altura Canónica.

Para terminar de trazar el paralelo con el caso K un cuerpo de números nos falta hablar de la altura canónica. La construcción de la altura canónica sí que es esencialmente copiarnos del caso anterior. El lema que nos garantizará la buena definición es el siguiente:

Lema 3.1.14. *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(t)$ y consideremos su función de altura h_E. Dado $P \in E(\overline{k})$, el límite:*

$$\frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h_E([2^n]\, P),$$

existe.

Demostración: Ver [10], Capítulo III, Teorema 4.3. □

De este modo podemos dar la definición.

Definición 3.1.15. Sea E una curva elíptica definida sobre $k = \mathbb{Q}(t)$. La *altura canónica* de E es la función:

$$\hat{h}_E \,:\, E(\overline{k}) \longrightarrow \mathbb{R},$$

definida por:

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

La altura canónica en curvas sobre $\mathbb{Q}(t)$ también satisface las propiedades análogas a las que satisface la del caso cuerpo de números; y se resumen en el siguiente resultado:

Teorema 3.1.16. *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(t)$. Sean h_E su función de altura y $\hat{h}_E$ su altura canónica.*

a) $\hat{h}_E(P) = \frac{1}{2}h_E(P) + O(1),\ \forall P \in E(\overline{k})$.

b) $\hat{h}_E([m]\,P) = m^2\hat{h}_E(P),\ \forall P \in E(\overline{k}),\ \forall m \in \mathbb{Z}$.

c) $\hat{h}_E(P+Q) + \hat{h}_E(P-Q) = 2\hat{h}_E(P) + 2\hat{h}_E(Q),\ \forall P, Q \in E(\overline{k})$.

d) $\hat{h}_E$ es una forma cuadrática en $E(\overline{k})$. En otras palabras, $\hat{h}_E$ es par y la aplicación:

$$\langle\ ,\ \rangle : E(\overline{k}) \times E(\overline{k}) \longrightarrow \mathbb{R}$$
$$\langle P, Q\rangle = \hat{h}_E(P+Q) - \hat{h}_E(P) - \hat{h}_E(Q)$$

es una forma bilineal.

e) Supongamos que la curva E no se descompone. Sea $P \in E(\overline{k})$. Entonces $\hat{h}_E(P) \geq 0$ y:

$$\hat{h}_E(P) = 0 \Longleftrightarrow P \text{ es un punto de torsión.}$$

f) Si $\hat{h}'_E : E(\overline{k}) \longrightarrow \mathbb{R}$ es otra función que satisface a) y existe $m \in \mathbb{Z}$, $m \geq 2$, tal que $\hat{h}_E([m]\,P) = m^2\hat{h}_E(P),\ \forall P \in E(\overline{k})$; entonces $\hat{h}'_E = \hat{h}_E$.

Demostración: Ver [10] Capítulo III, Teorema 4.3. □

Se tienen los mismos resultados en el caso general $k = \mathbb{Q}(\mathcal{C})$.

Las observaciones que podemos hacer son exactamente las mismas que hicimos para la altura canónica sobre cuerpos de números. La técnica para identificar puntos de torsión es idéntica; y también el procedimiento para encontrar cotas inferiores para el rango. Esto lo vamos a usar explícitamente más adelante.

3.2. Superficies

Ahora empezaremos a ver a las curvas elípticas sobre $\mathbb{Q}(t)$ con una perspectiva diferente; y así surgirán muchos otros condimentos.

Tal como habíamos comentado, cuando uno tiene una curva elíptica sobre $\mathbb{Q}(t)$, si tratamos a la indeterminada t como una variable más podemos pensar que tenemos una superficie sobre $\mathbb{Q}$. Antes de ir a los detalles, volvamos a considerar el ejemplo que teníamos:

$$E\ :\ y^2 = x^3 - t^2x + t^2.$$

E es una curva elíptica definida sobre el cuerpo $k = \mathbb{Q}(t)$. Esto es, es la variedad proyectiva irreducible de dimensión 1 en el plano proyectivo $\mathbb{P}^2(\overline{k})$, determinada por la ecuación afín que dimos. En tal caso, x e y son las variables y t es un escalar del cuerpo.

Ahora bien, si pensamos que t es otra variable con el mismo rol de x y de y, la ecuación afín que define a E consta de 3 variables; de manera que E se convierte en una variedad proyectiva (irreducible) que vive dentro del espacio proyectivo $\mathbb{P}^3(\overline{\mathbb{Q}})$, y ahora de dimensión 2.

3.2.1. Superficies Elípticas

Es natural llamar *superficies* a las variedades de dimensión 2. Esa nueva perspectiva que vimos en el último ejemplo no termina siendo un simple juego interesante de ver las cosas de otra forma, sino que va a ser la clave para todo el desarrollo que vamos a hacer a partir de ahora y nos va a permitir disponer de herramientas muy poderosas para obtener información de E.

A partir de ese mismo ejemplo que vimos, uno puede intuir que hay una cierta correspondencia entre las curvas elípticas definidas sobre $\mathbb{Q}(t)$ y una cierta familia de variedades proyectivas de dimensión 2, o superficies. En efecto la hay, y para ello vamos a especificar cuál es esa familia de superficies que están en correspondencia con las curvas elípticas sobre $\mathbb{Q}(t)$. Esa familia es la que le da el nombre al título de esta sección: son las *Superficies Elípticas.* Una definición intuitiva sería tratar de extender lo que hicimos con el ejemplo particular al caso general, y decir que las superficies elípticas son aquellas que provienen de interpretar a una curva elíptica sobre $\mathbb{Q}(t)$ como una variedad de dimensión 2. Pues en efecto, detalle más detalle menos, esa es la esencia de la definición.

Pasemos al aspecto formal. Vamos a dar la definición para el caso general $k = \mathbb{Q}(\mathcal{C})$; sin embargo, como insistimos siempre, sólo nos vamos a dedicar a trabajar con el caso $k = \mathbb{Q}(t)$.

Definición 3.2.1. Sea $\mathcal{C}$ una curva no singular sobre $\overline{\mathbb{Q}}$. Una *superficie elíptica sobre* $\mathcal{C}$ consiste en:

a) Una superficie irreducible $\mathcal{E}$, es decir, una variedad proyectiva irreducible de dimensión 2.

b) Un morfismo de variedades:

$$\pi : \mathcal{E} \longrightarrow \mathcal{C},$$

tal que para casi todo $p \in \mathcal{C}(\overline{\mathbb{Q}})$ (es decir, para todos salvo finitos) la fibra:

$$\mathcal{E}_p = \pi^{-1}(p),$$

es una curva elíptica sobre $\overline{\mathbb{Q}}$.

c) Una sección:

$$\sigma_0 : \mathcal{C} \longrightarrow \mathcal{E}.$$

(Ver Figura 3.1). Recordemos que una sección es un morfismo $\sigma : \mathcal{C} \longrightarrow \mathcal{E}$ tal que $\pi \circ \sigma = id_{\mathcal{C}}$. La sección σ_0 es aquella que recorrerá los puntos origen $\mathcal{O}$ de cada una de las curvas elípticas $\mathcal{E}_p$, para casi todos los $p \in \mathcal{C}(\overline{\mathbb{Q}})$.

Uno puede ser más formal aún si toma como definición de curva elíptica aquella que comentamos que involucra el concepto de género. De este modo, en el ítem b) se pide que la fibra $\mathcal{E}_p$ sea una curva de género 1. Sin embargo no nos queremos meter con esa perspectiva.

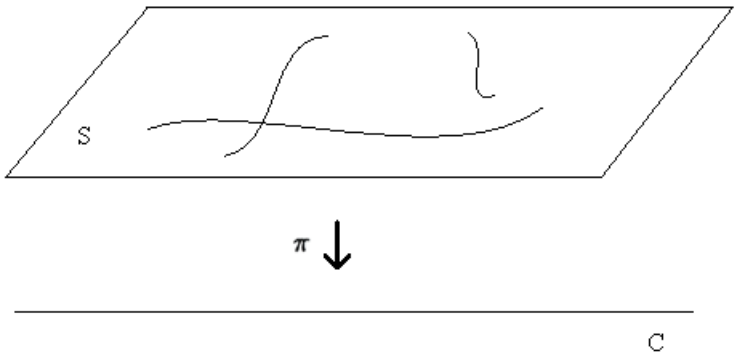


Figura 3.1: Superficie elíptica

El caso que vamos a trabajar es, como dijimos, $\mathcal{C} = \mathbb{P}^1$; con lo que $\mathbb{Q}(\mathcal{C}) = \mathbb{Q}(t)$.

Observación 3.2.2. Las superficies elípticas resultan ser un caso particular de una familia más general llamada Superficies Fibradas. Luego vamos a generalizar y trabajar con ellas.

La definición resulta mucho más clara cuando vemos un ejemplo. Volvamos sobre el ejemplo de siempre. Afirmamos que:

$$\mathcal{E} \,:\, y^2 = x^3 - t^2 x + t^2,$$

es una superficie elíptica sobre $\mathcal{C} = \mathbb{P}^1$.

En efecto, es una variedad proyectiva irreducible de dimensión 2. La tenemos escrita en su ecuación afín pero podemos homogenizarla. Antes de eso, por cuestiones de comodidad, no vamos a pensar a nuestra superficie viviendo en el espacio proyectivo $\mathbb{P}^3$; sino que la vamos a pensar inmersa en el espacio $\mathbb{P}^2 \times \mathbb{P}^1$. En este espacio los elementos son pares de la forma:

$$([X : Y : Z]\,; [T : U]);$$

donde la identificación coordenadas homogéneas-afines es:

$$x = \frac{X}{Z};\; y = \frac{Y}{Z};\; t = \frac{T}{U}.$$

Con esta convención, la ecuación homogénea de $\mathcal{E}$ resulta ser:

$$\mathcal{E} \,:\, \frac{Y^2}{Z^2} = \frac{X^3}{Z^3} - \frac{T^2}{U^2}\frac{X}{Z} + \frac{T^2}{U^2}.$$

Y si limpiamos denominadores:

$$\mathcal{E} \,:\, U^2 Y^2 Z = U^2 X^3 - T^2 X Z^2 + T^2 Z^3.$$

Con el trabajo que hicimos es bastante claro cuál es el morfismo

$$\begin{array}{rccc} \pi\ : & \mathcal{E} & \longrightarrow & \mathbb{P}^1 \\ & ([X:Y:Z]\,;[T:U]) & \longrightarrow & [T:U] \end{array}$$

Habría que verificar que para casi todo $p=[T:U]\in\mathbb{P}^1$ la fibra $\mathcal{E}_p$ es una curva elíptica sobre $\overline{\mathbb{Q}}$. Pero esto no es nada difícil. Por cómo está definido π, que es simplemente proyectar en la segunda componente, hay que verificar que para casi toda especialización del punto $p=[T:U]$ se obtiene una curva elíptica sobre $\overline{\mathbb{Q}}$. Es decir, que:

$$\mathcal{E}_p\ :\ U^2Y^2Z=U^2X^3-T^2XZ^2+T^2Z^3,$$

es una curva elíptica no singular para casi todas las elecciones de $p=[T:U]$.

Por ejemplo, tomemos $p=[t:1]$, de modo que queda:

$$\mathcal{E}_t\ :\ Y^2Z=X^3-t^2XZ^2+t^2Z^3,$$

con ecuación afín:

$$\mathcal{E}_t\ :\ y^2=x^3-t^2x+t^2.$$

Esta será una curva elíptica sobre $\overline{\mathbb{Q}}$ si el discriminante Δ es no nulo. Tenemos:

$$\Delta=16t^4(4t^2-27).$$

De este modo concluimos que $\mathcal{E}_t$ es una curva elíptica para todo t salvo para:

$$t=0,\ t=\frac{3}{2}\sqrt{3},\ t=-\frac{3}{2}\sqrt{3}.$$

También es fácil de verificar que para $p_\infty=[1:0]$ tampoco se obtiene una curva elíptica, pues la ecuación queda:

$$\mathcal{E}_\infty\ :\ 0=-XZ^2+Z^3.$$

Hemos visto entonces que salvo para 4 puntos $p\in\mathbb{P}^1$ la fibra $\mathcal{E}_p$ es una curva elíptica sobre $\overline{\mathbb{Q}}$. Por último, hay varias secciones que podrían hacer las veces de σ_0; sin embargo suele tomarse:

$$\sigma_0([T:U])=([0:1:0]\,;[T:U]).$$

Es sencillo de comprobar que σ_0 es efectivamente una sección. Es natural considerar esa sección particular. Recordemos que σ_0 recorre los puntos origen de las curvas elípticas $\mathcal{E}_p$; y como ya vimos, en general se toma como punto origen de una curva elíptica al punto $\mathcal{O}=[0:1:0]$.

Como estamos viendo, dada una curva elíptica E sobre $\overline{\mathbb{Q}(t)}$, uno puede construirse una superficie elíptica $\mathcal{E}$ asociada. Es natural preguntarse si esa correspondencia es recíproca, y además si involucra alguna relación algebraica entre las variedades E y $\mathcal{E}$. En efecto las dos preguntas tienen respuesta afirmativa. La siguiente proposición formaliza esta idea.

Proposición 3.2.3. *a) Sea E una curva elíptica sobre $\overline{\mathbb{Q}(\mathcal{C})}$ de ecuación:*

$$E \,:\, Y^2Z = X^3 + AX^2Z + BXZ^2 + CZ^3,$$

con $A, B, C \in \overline{\mathbb{Q}(\mathcal{C})}$. Sea $\mathcal{E}$ la superficie de $\mathbb{P}^2 \times \mathcal{C}$ dada por:

$$\mathcal{E} \,:\, Y^2Z = X^3 + A(p)X^2Z + B(p)XZ^2 + C(p)Z^3,$$

con $\pi : \mathcal{E} \longrightarrow \mathcal{C}$, $\pi([X : Y : Z]\,; p) = p$ y $\sigma_0 : \mathcal{C} \longrightarrow \mathcal{E}$, $\sigma_0(p) = ([0 : 1 : 0]\,; p)$. Entonces $(\mathcal{E}, \pi, \sigma_0)$ es una superficie elíptica sobre $\mathcal{C}$.

b) Sea $\mathcal{E}'$ una superficie elíptica sobre $\mathcal{C}$. Entonces $\mathcal{E}'$ es birracionalmente equivalente a la superficie elíptica $\mathcal{E}$ definida en el ítem a) para alguna elección de A, B y C; y la curva elíptica E está unívocamente determinada por $\mathcal{E}$ salvo isomorfismos.

Demostración: Ver [10], Capítulo III, Proposición 3.8. □

Como siempre, la aclaración es que sólo nos vamos a abocar al caso $\mathcal{C} = \mathbb{P}^1$.

Teniendo esta correspondencia podemos trazar paralelos entre las curvas elípticas sobre $\mathbb{Q}(t)$ y las superficies elípticas asociadas. Concretamente, una primera idea surge de mirar nuestro ejemplo. Tenemos la curva sobre $\mathbb{Q}(t)$ de ecuación afín:

$$E \,:\, y^2 = x^3 - t^2x + t^2.$$

Como habíamos observado, hay algunos puntos de E que se encuentran sin mucho esfuerzo. Tenemos, por ejemplo, los puntos de coordenadas afines:

$$(t, t);\ (t, -t);\ (0, t);\ (0, -t);\ (1, 1);\ (1, -1),$$

cuyas coordenadas homogéneas son:

$$[t : t : 1]\,;\ [t : -t : 1]\,;\ [0 : t : 1]\,;\ [0 : -t : 1]\,;\ [1 : 1 : 1]\,;\ [1 : -1 : 1]\,.$$

Ahora, si pensamos en la superficie elíptica $\mathcal{E}$ de $\mathbb{P}^2 \times \mathbb{P}^1$ asociada, ¿qué interpretación tendrán estos puntos? La interpretación es muy precisa, pues esos puntos se corresponden con *secciones* de $\mathbb{P}^1$ en $\mathcal{E}$. Concretamente tenemos las secciones $\sigma_i : \mathbb{P}^1 \longrightarrow \mathcal{E}$:

$$\begin{aligned}
\sigma_1([T : U]) &= ([T : T : U]\,; [T : U]) \\
\sigma_2([T : U]) &= ([T : -T : U]\,; [T : U]) \\
\sigma_3([T : U]) &= ([0 : T : U]\,; [T : U]) \\
\sigma_4([T : U]) &= ([0 : -T : U]\,; [T : U]) \\
\sigma_5([T : U]) &= ([1 : 1 : 1]\,; [T : U]) \\
\sigma_6([T : U]) &= ([1 : -1 : 1]\,; [T : U])
\end{aligned}$$

De este modo vemos que los puntos de E están en correspondencia con secciones de $\mathcal{E}$. Esto nos permite hacernos el siguiente planteo. Sabemos que hay una operación suma entre los puntos de E que hace de $E(\overline{k})$ un grupo abeliano. ¿Cómo se traduce esa operación en las secciones correspondientes de $\mathcal{E}$? Del modo más natural. Podemos *sumar* secciones aprovechando la operación de grupo en las fibras $\mathcal{E}_p$.

Concretamente, supongamos que tenemos dos secciones σ_1 y σ_2 de $\mathcal{E}$. Donde $\mathcal{E}$ es una superficie elíptica sobre $\mathcal{C}$. Sea $p \in \mathcal{C}$ tal que la fibra $\mathcal{E}_p$ es una curva elíptica definida sobre $\overline{\mathbb{Q}}$. Tenemos que $\sigma_1(p)$ y $\sigma_2(p)$ son puntos de $\mathcal{E}$ cuyas primeras componentes son puntos de la curva elíptica $\mathcal{E}_p$; por lo que podemos sumarlas según la operación de grupo en $\mathcal{E}_p$. De esta manera podemos definir:

$$(\sigma_1 + \sigma_2)(p) = \sigma_1(p) + \sigma_2(p).$$

Donde la suma del miembro derecho de la igualdad es sumar las primeras componentes en $\mathcal{E}_p$ y dejar fijas las segundas. De un modo similar definimos:

$$(-\sigma_1)(p) = -\sigma_1(p);$$

donde el inverso aditivo del miembro derecho de la igualdad es el inverso aditivo de la primera componente según la operación de grupo en $\mathcal{E}_p$ y dejar fija la segunda.

De esta manera bastante natural es que podemos darle una estructura de grupo al conjunto de secciones de $\mathcal{E}$; aprovechando la estructura en cada fibra $\mathcal{E}_p$ que sea una curva elíptica.

Ahora bien, esta definición sólo tiene sentido precisamente en los puntos $p \in \mathcal{C}$ tales que $\mathcal{E}_p$ es una curva elíptica; pues en el resto no tenemos definida una suma. Sin embargo esto no es impedimento para la construcción que uno quiere hacer. La razón por la cual esto no nos obstaculiza es la siguiente. Dadas secciones σ_1 y σ_2, podemos definir la función $\sigma_1 + \sigma_2$ que está definida sólo en los puntos $p \in \mathcal{C}$ tales que $\mathcal{E}_p$ es una curva elíptica. Ocurre que, así definida, $\sigma_1 + \sigma_2 : \mathcal{C} \longrightarrow \mathcal{E}$ es una **función racional**. Dado que asumimos que $\mathcal{C}$ es no singular, tenemos que necesariamente $\sigma_1 + \sigma_2$ resulta ser un **morfismo**. En otras palabras, se puede extender $\sigma_1 + \sigma_2$ a aquellos puntos $p \in \mathcal{C}$ en los que no estaba definida. Lo mismo para $-\sigma_1$.

Los detalles de esto y el resultado que se obtiene los encontramos en la siguiente proposición.

Proposición 3.2.4. *Sea $\mathcal{E}$ una superficie elíptica sobre $\mathcal{C}$. Notemos:*

$$\mathcal{E}(\mathcal{C}) = \{ \text{ Secciones } \sigma \, : \, \mathcal{C} \longrightarrow \mathcal{E} \} .$$

Sean $\sigma_1, \sigma_2 \in \mathcal{E}(\mathcal{C})$.

a) Las funciones:

$$\begin{aligned} (\sigma_1 + \sigma_2)(p) &= \sigma_1(p) + \sigma_2(p) \\ (-\sigma_1)(p) &= -\sigma_1(p) \end{aligned}$$

definidas en los puntos $p \in \mathcal{C}$ tales que $\mathcal{E}_p$ es una curva elíptica; se extienden a elementos de $\mathcal{E}(\mathcal{C})$.

b) Las operaciones $(\sigma_1, \sigma_2) \longmapsto \sigma_1 + \sigma_2$ *y* $\sigma \longmapsto -\sigma$ *definidas en a) hacen de* $\mathcal{E}(\mathcal{C})$ *un grupo abeliano.*

c) Sea E la curva elíptica sobre $\overline{\mathbb{Q}(\mathcal{C})}$ *asociada a* $\mathcal{E}$*. Entonces se tiene un isomorfismo de grupos:*

$$\begin{aligned} E(\overline{\mathbb{Q}(\mathcal{C})}) \ : \longrightarrow \ & \mathcal{E}(\mathcal{C}) \\ P \longmapsto \ & \sigma_P \end{aligned}$$

Donde, si $P = [X(p) : Y(p) : Z(p)] \in E(\overline{\mathbb{Q}(\mathcal{C})})$*, con* $X(p), Y(p), Z(p) \in \overline{\mathbb{Q}(\mathcal{C})}$*, se define* $\sigma_P : \mathcal{C} \longrightarrow \mathcal{E}$ *como:*

$$\sigma_P(p) = ([X(p) : Y(p) : Z(p)] \, ; p).$$

Demostración: Ver [10], Capítulo III, Proposición 3.10. □

Como siempre, aclaramos que sólo vamos a trabajar con $\mathcal{C} = \mathbb{P}^1$.

Miremos cómo es la estructura de grupo de $\mathcal{E}(\mathcal{C})$ en nuestro ejemplo de siempre. Tenemos la superficie $\mathcal{E}$ dada afinmente por:

$$\mathcal{E} \ : \ y^2 = x^3 - t^2 x + t^2.$$

Consideremos las secciones:

$$\sigma_1([T : U]) = ([T : T : U] \, ; [T : U])$$

$$\sigma_3([T : U]) = ([0 : T : U] \, ; [T : U])$$

y calculemos $\sigma_1 + \sigma_3$. Para ello consideramos los puntos $p = [T : U]$ tales que $\mathcal{E}_p$ es una curva elíptica. Recordemos que si miramos aquellos de la forma $p = [t : 1]$, nos servían todos salvo para $t = 0$, $t = \pm\frac{3}{2}\sqrt{3}$. Considerando entonces la familia de esos t *buenos*, hagamos el cálculo. La curva elíptica $\mathcal{E}_t$ es la de ecuación afín:

$$\mathcal{E}_t \ : \ y^2 = x^3 - t^2 x + t^2.$$

Y los puntos que queremos sumar son las primeras componentes de $\sigma_1(p)$ y $\sigma_3(p)$; o sea, los puntos afines:

$$Q_1 = (t, t)$$

$$Q_2 = (0, t)$$

Recordando las fórmulas explícitas para la ley de grupo que vimos en el capítulo anterior, nos queda que:

$$Q_1 + Q_2 = (t, t) + (0, t) = (-t, -t).$$

Es decir:

$$(\sigma_1 + \sigma_3)([t : 1]) = ([-t : -t : 1] \, ; [t : 1]).$$

Y volviendo a coordenadas homogéneas:

$$(\sigma_1 + \sigma_3)([T : U]) = (\left[-\frac{T}{U} : -\frac{T}{U} : 1\right] ; \left[\frac{T}{U} : 1\right]) = ([-T : -T : U] \, ; [T : U]).$$

O sea, $\sigma_1 + \sigma_3 = \tau$, donde:

$$\tau([T:U]) = ([-T:-T:U]\,;[T:U]).$$

También podemos calcular $-\sigma_1$. Para ello tenemos que hallar el inverso aditivo de $Q_1 = (t,t)$. Pero sabemos que el inverso aditivo se encuentra simplemente cambiando de signo la segunda coordenada:

$$-Q_1 = (t,-t).$$

Luego tenemos:

$$(-\sigma_1)([t:1]) = ([t:-t:1]\,;[t:1]).$$

O sea, escribiendo en coordenadas homogéneas:

$$(-\sigma_1)([T:U]) = ([T:-T:U]\,;[T:U]).$$

3.3. Geometría de las Superficies Fibradas

Las siguientes construcciones que haremos son nociones que no son exclusivas de las superficies elípticas, sino de objetos más generales; por lo que vamos a generalizar un poco y veremos a las superficies elípticas como casos particulares.

Hasta acá hemos trabajado con las superficies elípticas; que son variedades proyectivas irreducibles de dimensión 2 con un morfismo de proyección asociado.

Como hemos anticipado, las superficies elípticas son casos particulares de lo que se llaman *Superficies Fibradas*. En efecto, una Superficie Fibrada $\mathcal{S}$ es una variedad proyectiva irreducible de dimensión 2 junto con un morfismo de proyección hacia una curva no singular:

$$\pi : \mathcal{S} \longrightarrow \mathcal{C}.$$

Cuando uno le agrega condiciones a las fibras $\pi^{-1}(p)$ aparecen los casos particulares, como las superficies elípticas.

Sobre las superficies elípticas hay muchos aspectos geométricos que son interesantes en sí y que nos van a ser de gran utilidad para lo que viene. Sin embargo estos aspectos geométricos no son exclusivos de las superficies elípticas en particular, sino de todas las superficies fibradas. Es por esto que en esta sección trataremos las características geométricas de todas las superficies fibradas; y más adelante volveremos sobre las superficies elípticas, cuando queramos hacer construcciones que sí son propias de ellas.

3.3.1. Divisores sobre Superficies Fibradas

Ya trabajamos con el concepto de Divisor sobre las curvas. Llegó el momento de extender esa noción a las Superficies; y lo vamos a hacer de un modo bastante natural.

Esta primera parte, en realidad, puede hacerse sobre cualquier superficie, no necesariamente fibrada; es decir, sobre cualquier variedad proyectiva irreducible de dimensión 2. Sin embargo, dado que en breve sí necesitaremos que la superficie sea fibrada, vamos a suponer que lo es. Al fin y al cabo no nos estamos restringiendo mucho.

En las curvas, habíamos definido el grupo de sus divisores como el $\mathbb{Z}$-módulo libre generado por sus puntos. El paralelo se traza aquí del siguiente modo. Dada una superficie fibrada $\mathcal{S}$, en lugar de sus puntos, vamos a considerar todas las curvas irreducibles contenidas en ella. El grupo de los divisores de $\mathcal{S}$ será entonces el $\mathbb{Z}$-módulo libre generado por esas curvas. Así como aquella vez consideramos curvas no singulares, ahora también vamos a tener que pedirle a la superficie $\mathcal{S}$ que sea no singular.

Definición 3.3.1. Sea $\mathcal{S}$ una superficie fibrada no singular. Es decir, una variedad proyectiva irreducible de dimensión 2, no singular y con un morfismo de proyección hacia una curva no singular. Definimos el *grupo de divisores de* $\mathcal{S}$ como el $\mathbb{Z}$-módulo libre generado por las curvas irreducibles contenidas en $\mathcal{S}$. Es decir:

$$\mathcal{D}iv(\mathcal{S}) = \left\{ \sum_{\Gamma \subseteq \mathcal{S}} n_\Gamma(\Gamma) \ : \ n_\Gamma \in \mathbb{Z},\, n_\Gamma = 0 \textit{ para casi toda } \Gamma \subseteq \mathcal{S} \textit{ irreducible} \right\}.$$

Cuando trabajamos con curvas, aprovechando que el anillo de coordenadas localizado en un punto no singular es un anillo de valuación discreta, a cada función no nula f del cuerpo de funciones le asociamos un divisor. Ahora vamos a hacer algo similar, pero para eso necesitamos tener la noción de valuación sobre una curva irreducible $\Gamma \subseteq \mathcal{S}$.

Cuando trabajamos con una curva, dado un punto P de ella, habíamos definido el anillo local en P como la localización del anillo de coordenadas de la curva en el ideal maximal asociado a P; y la interpretación era que constaba de las funciones del cuerpo de funciones de la curva definidas en P. Tratemos de extender esto a superficies. Dada una curva irreducible $\Gamma \subseteq \mathcal{S}$, por ser Γ irreducible, su ideal asociado $I(\Gamma)$ es un ideal primo del anillo de polinomios. En particular es un ideal primo del anillo de coordenadas $\overline{\mathbb{Q}}\,[\mathcal{S}]$. Podemos entonces localizar $\overline{\mathbb{Q}}\,[\mathcal{S}]$ en $I(\Gamma)$. De aquí surge la definición:

Definición 3.3.2. Sea $\mathcal{S}$ una superficie fibrada no singular y sea $\Gamma \subseteq \mathcal{S}$ una curva irreducible. Si $I(\Gamma)$ es el ideal asociado a la variedad Γ, definimos el *anillo local de* $\mathcal{S}$ en Γ como la localización de $\overline{\mathbb{Q}}\,[\mathcal{S}]$ en $I(\Gamma)$ y lo notamos $\mathcal{O}_\Gamma$.

Aquí también hay una interpretación similar a la que hicimos con el anillo local de una curva en un punto. En este caso, son las funciones de $\overline{\mathbb{Q}}(\mathcal{S})$ definidas en **algún punto** de Γ.

Teniendo esta interpretación podemos dar una definición alternativa. Veamos primero cómo es el anillo local de una superficie en un punto. Dado un punto $P \in \mathcal{S}$, el anillo local de $\mathcal{S}$ en P es hacer exactamente lo mismo que se hizo en curvas. Si llamamos:

$$\mathcal{M}_P = \left\{ f \in \overline{\mathbb{Q}}\,[\mathcal{S}] \ : \ f(P) = 0 \right\},$$

es fácil verificar, tal como lo hicimos en las curvas, que $\mathcal{M}_P$ es un ideal maximal del anillo de coordenadas $\overline{\mathbb{Q}}\,[\mathcal{S}]$. Podemos entonces localizar en ese ideal, y a la localización la llamamos el

anillo local de $\mathcal{S}$ en P. A ese anillo local lo vamos a notar $\mathcal{O}_P$, y consistirá en las funciones de $\overline{\mathbb{Q}}(\mathcal{S})$ definidas en P. Afirmamos entonces que:

$$\mathcal{O}_\Gamma = \bigcup_{P \in \Gamma} \mathcal{O}_P.$$

Esto ahora es bastante claro a partir de las interpretaciones de uno y otro.

En curvas, si el punto P en el que estábamos localizando era no singular, el anillo local resultaba un anillo de valuación discreta. Aquí, dado que asumimos a nuestra superficie $\mathcal{S}$ no singular, también tenemos un resultado similar.

Proposición 3.3.3. *Sea $\mathcal{S}$ una superficie fibrada no singular y $\Gamma \subseteq \mathcal{S}$ una curva irreducible. Entonces $\mathcal{O}_\Gamma$ es un anillo de valuación discreta.*

Demostración: Ver [10], Capítulo III, Sección 7. □

Teniendo este resultado es que podemos asociarle a cada función no nula de $\overline{\mathbb{Q}}(\mathcal{S})$ un divisor. En efecto, podemos definir el morfismo de valuación en cada curva Γ.

Definición 3.3.4. Sea $\mathcal{S}$ una superficie fibrada no singular y sea $\Gamma \subseteq \mathcal{S}$ una curva irreducible. La *valuación* en Γ es la función:

$$\begin{array}{rcl} ord_\Gamma : \overline{\mathbb{Q}}\,[\mathcal{S}] & \longrightarrow & \mathbb{N}_0 \cup \{\infty\} \\ f & \longmapsto & ord_\Gamma(f) \end{array}$$

Donde:

$$ord_\Gamma(f) = máx\left\{d \in \mathbb{Z} \,:\, f \in I(\Gamma)^d\right\},$$

y donde $I(\Gamma)$ nota el ideal de Γ.

Convenimos $ord_\Gamma(0) = \infty$.

Hacemos la extensión natural de ord_Γ a $\overline{\mathbb{Q}}\,(\mathcal{S})$ definiendo:

$$ord_\Gamma\left(\frac{f}{g}\right) = ord_\Gamma(f) - ord_\Gamma(g).$$

De este modo tenemos $ord_\Gamma : \overline{\mathbb{Q}}\,(\mathcal{S}) \longrightarrow \mathbb{Z} \cup \{\infty\}$.

La definición es buena gracias a la Proposición 3.3.3.

Algunas de las propiedades que satisface la valuación son las mismas que enumeramos en la Observación 1.3.10 cuando trabajamos con curvas.

Contando con la valuación ahora sí podemos asociar a cada función no nula del cuerpo de funciones de $\mathcal{S}$ un divisor. Más aún, tenemos un morfismo de grupos.

Proposición 3.3.5. *Sea $\mathcal{S}$ una superficie fibrada no singular. La siguiente aplicación es un morfismo de grupos:*

$$\begin{array}{ccc} \overline{\mathbb{Q}}(\mathcal{S})^{\times} & \longrightarrow & \mathcal{D}iv(\mathcal{S}) \\ f & \longrightarrow & div(f) \end{array}$$

Donde:

$$div(f) = \sum_{\Gamma \subseteq \mathcal{S}} ord_{\Gamma}(f)(\Gamma).$$

Demostración: Es inmediato a partir de las propiedades de ord_{Γ} listadas en la Observación 1.3.10. □

Antes de hacer ejemplos veamos algunas definiciones más. Al igual que en el caso de curvas, a los divisores de la forma $div(f)$ para alguna $f \in \overline{\mathbb{Q}}(\mathcal{S})^{\times}$ los llamamos *principales.* Considerando el subgrupo de los divisores principales, podemos dividir a $\mathcal{D}iv(\mathcal{S})$ por él; lo que es lo mismo que definir una relación de equivalencia dada por:

$$D_1 \sim D_2 \Longleftrightarrow D_1 - D_2 \text{ es principal.}$$

Esto es exactamente lo mismo que hicimos en el caso curvas. Al grupo cociente también lo vamos a llamar el grupo de Picard de $\mathcal{S}$ y lo notamos:

$$\mathcal{P}ic(\mathcal{S}) = \mathcal{D}iv(\mathcal{S})/\sim .$$

Observemos ahora lo siguiente. Dada una curva irreducible $\Gamma \subseteq \mathcal{S}$; consideremos el morfismo de proyección:

$$\pi : \mathcal{S} \longrightarrow \mathcal{C}.$$

Podemos restringir π a la curva Γ obteniendo así un morfismo de curvas:

$$\pi|_{\Gamma} : \Gamma \longrightarrow \mathcal{C}.$$

Recordando el Teorema 1.3.16 sabemos que $\pi|_{\Gamma}$ es o bien constante o bien suryectivo. Pues bien, de acuerdo a las dos posibilidades es que vamos a clasificar a nuestras curvas irreducibles $\Gamma \subseteq \mathcal{S}$.

Definición 3.3.6. Sea $\mathcal{S}$ una superficie fibrada no singular con morfismo de proyección $\pi : \mathcal{S} \longrightarrow \mathcal{C}$. Sea $\Gamma \subseteq \mathcal{S}$ una curva irreducible.

Si $\pi|_{\Gamma} : \Gamma \longrightarrow \mathcal{C}$ es constante decimos que Γ es una curva *fibral* de $\mathcal{S}$.

Si $\pi|_{\Gamma} : \Gamma \longrightarrow \mathcal{C}$ es suryectivo decimos que Γ es una curva *horizontal* de $\mathcal{S}$.

Los nombres son bastante razonables, pues si $\pi|_{\Gamma}$ es constante, digamos $\pi|_{\Gamma}(P) = p$, $\forall P \in \Gamma$, tenemos que $\Gamma \subseteq \mathcal{S}_p = \pi^{-1}(p)$. O sea, Γ está contenida en una de las fibras.

Y si $\pi|_{\Gamma}$ es suryectivo, la palabra horizontal es muy coherente con la idea geométrica de lo que ocurre. (Ver Figura 3.2).

Las definiciones de curvas fibrales y horizontales se extienden naturalmente a los divisores:

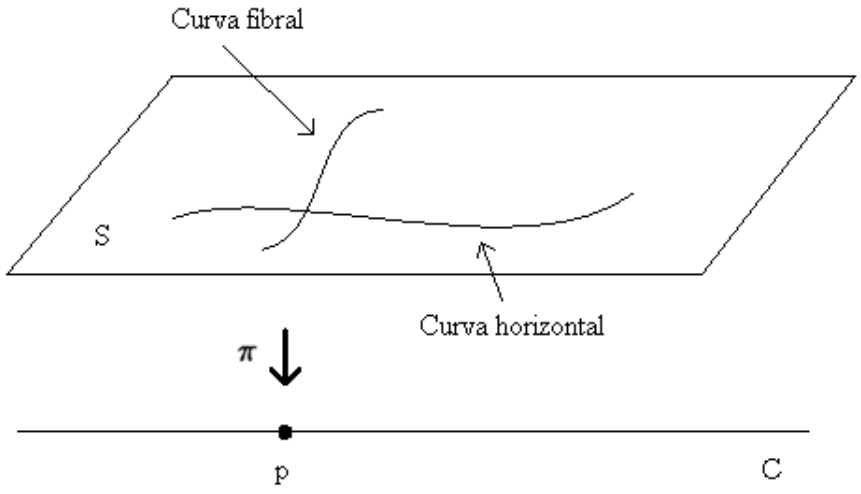


Figura 3.2: Curvas fibrales y horizontales

Definición 3.3.7. Sea $\mathcal{S}$ una superficie fibrada no singular. Sea $D \in \mathcal{D}iv(\mathcal{S})$. D se dice *divisor fibral* si todas sus componentes son fibrales; y se dice *divisor horizontal* si todas sus componentes son horizontales. Donde, si:

$$D = \sum_{i=1}^{r} n_{\Gamma_i}(\Gamma_i),$$

con $n_{\Gamma_i} \neq 0$; $\Gamma_1, \Gamma_2, ..., \Gamma_r$ son las componentes de D.

Considerando el morfismo $\pi : \mathcal{S} \longrightarrow \mathcal{C}$ de una superficie fibrada, podemos construir un morfismo en el sentido inverso entre sus grupos de divisores.

Fijemos un punto $p \in \mathcal{C}$. Dado que asumimos que $\mathcal{C}$ es no singular, el anillo local de $\mathcal{C}$ en p es un anillo de valuación discreta, por lo que tiene sentido considerar un uniformizador local $u_p \in \overline{mathbbQ}[\mathcal{C}]_P \subseteq \overline{\mathbb{Q}}(\mathcal{C})$. De este modo podemos construir la siguiente función:

$$u_p \circ \pi \ : \ \mathcal{S} \longrightarrow \overline{\mathbb{Q}}.$$

Claramente $u_p \circ \pi$ es un elemento de $\overline{\mathbb{Q}}(\mathcal{S})$, el cuerpo de funciones de $\mathcal{S}$. Por lo tanto podemos calcular su orden sobre curvas $\Gamma \subseteq \mathcal{S}$. Aquí la definición precisa.

Definición 3.3.8. Sea $\mathcal{S}$ una superficie fibrada no singular con morfismo de proyección $\pi : \mathcal{S} \longrightarrow \mathcal{C}$. Se define el morfismo $\pi^* : \mathcal{D}iv(\mathcal{C}) \longrightarrow \mathcal{D}iv(\mathcal{S})$ asociado a π del siguiente modo:

$$\pi^*(\sum_{p \in \mathcal{C}} n_p(p)) = \sum_{p \in \mathcal{C}} n_p(\sum_{\Gamma \subseteq \mathcal{S}_p} ord_\Gamma(u_p \circ \pi)(\Gamma)).$$

Notar que, por la definición de uniformizador local, el número $ord_\Gamma(u_p \circ \pi)$ siempre será positivo sobre cualquier curva Γ contenida en la fibra $\mathcal{S}_p$.

Ahora sí vamos a desarrollar un ejemplo para poder visualizar estas cosas. Vamos a considerar la siguiente superficie fibrada. $\mathcal{S}$ será una superficie que vamos a mirar dentro de $\mathbb{P}^2 \times \mathbb{P}^1$; con $\overline{K} = \overline{\mathbb{Q}}$. En este espacio diremos que los puntos son de la forma $([X : Y : Z] ; [T : U])$. La ecuación que define a $\mathcal{S}$ es:

$$\mathcal{S} \, : \, F(X, Y, Z, T, U) = X^2U + Y^2U + XYT + XZT + YZU - 2Z^2U = 0.$$

Va a ser cómodo mirar a $\mathcal{S}$ en la afinización $Z = U = 1$. Así nos queda:

$$\mathcal{S} \, : \, x^2 + y^2 + xyt + xt + y - 2 = 0.$$

No es difícil verificar que F es irreducible, por lo que el ideal $(F) \subseteq \overline{\mathbb{Q}}\,[X, Y, Z, T, U]$ es primo. Además, con técnicas que ya hicimos, y que volveremos a hacer, también se puede comprobar que el ideal que define a la variedad $\mathcal{S}$ es exactamente (F); y en consecuencia $\mathcal{S}$ es una variedad irreducible.

Definimos el morfismo de proyección como $\pi : \mathcal{S} \longrightarrow \mathbb{P}^1$, $\pi\left([X : Y : Z] ; [T : U]\right) = [T : U]$.

Observemos que $\mathcal{S}$ también puede ser interpretada como una curva sobre $\overline{\mathbb{Q}(t)}$; más aún, definida sobre $\mathbb{Q}(t)$. De la misma forma que hicimos antes cuando establecimos la correspondencia entre curvas elípticas sobre $\overline{\mathbb{Q}(t)}$ y superficies elípticas, pues aquí también $\mathcal{S}$ puede ser pensada como una curva (ya no elíptica) sobre $\mathbb{Q}(t)$.

Antes de ponernos a buscar ejemplos de divisores en $\mathcal{S}$, lo primero que tenemos que hacer, que no es un detalle menor, es verificar que $\mathcal{S}$ es una superficie no singular. Recordemos que para ello tenemos que, dado un punto $P \in \mathcal{S}$, encontrar una afinización de $\mathcal{S}$ tal que P pertenezca a ella, y verificar que la variedad afín que se obtiene es no singular en P. Como estamos trabajando en $\mathbb{P}^2 \times \mathbb{P}^1$, las afinizaciones posibles son 6. A saber:

$$X = T = 1;\ X = U = 1;\ Y = T = 1;\ Y = U = 1;\ Z = T = 1;\ Z = U = 1.$$

Deberíamos entonces verificar que las 6 variedades afines resultantes son no singulares. O sea, que las derivadas parciales de los polinomios:

$$F(1, Y, Z, 1, U);\ F(1, Y, Z, T, 1);\ F(X, 1, Z, 1, U);$$

$$F(X, 1, Z, T, 1);\ F(X, Y, 1, 1, U);\ F(X, Y, 1, T, 1);$$

no son simultáneamente nulas en cada punto de la superficie. Para esto basta verificar que las 5 derivadas parciales de $F(X, Y, Z, T, U)$ no son simultáneamente nulas en cada punto de $\mathcal{S}$.

Veamos entonces. Tenemos el sistema:

$$\begin{aligned}
\frac{\partial F}{\partial X}(X,Y,Z,T,U) = & \quad 2XU + YT + TZ = 0 \quad (1)\\
\frac{\partial F}{\partial Y}(X,Y,Z,T,U) = & \quad 2YU + XT + ZU = 0 \quad (2)\\
\frac{\partial F}{\partial Z}(X,Y,Z,T,U) = & \quad XT + YU - 4ZU = 0 \quad (3)\\
\frac{\partial F}{\partial T}(X,Y,Z,T,U) = & \quad XY + XZ = 0 \quad (4)\\
\frac{\partial F}{\partial U}(X,Y,Z,T,U) = & \quad X^2 + Y^2 + YZ - 2Z^2 = 0 \quad (5)
\end{aligned}$$

De (4), $XY + XZ = 0 \Rightarrow X(Y+Z) = 0 \Rightarrow X = 0$ *o* $Y = -Z$.

1. Si $X = 0$, de (2), $2YU + ZU = 0 \Rightarrow U(2Y+Z) = 0 \Rightarrow U = 0$ *o* $Z = -2Y$.

   - Si $U = 0$, de (1), $YT + TZ = 0 \Rightarrow T(Y+Z) = 0$. Como $U = 0$, entonces $T \neq 0$; luego, $Y = -Z$. Entonces, de (5), $Y^2 - Y^2 - 2Y^2 = 0 \Rightarrow Y = 0$. Entonces $Z = -Y = 0$. Pero entonces $X = Y = Z = 0$: Absurdo.
   - Si $Z = -2Y$, de (5), $Y^2 - 2Y^2 - 8Y^2 = 0 \Rightarrow Y = 0 \Rightarrow Z = -2Y = 0$. Con lo cual, otra vez, $X = Y = Z = 0$: Absurdo.

2. Si $Y = -Z$, de (1), $2XU = 0 \Rightarrow X = 0$ *o* $U = 0$.

   - Si $X = 0$, volvemos al caso anterior, que vimos que es imposible.
   - Si $U = 0$, de (3), $XT = 0 \Rightarrow X = 0$ *o* $T = 0$. Pero, de nuevo, el caso $X = 0$ ya lo hicimos; y como $U = 0$, $T \neq 0$. Por lo tanto, tampoco es posible este caso.

Luego, el sistema no tiene solución en $\mathbb{P}^2 \times \mathbb{P}^1$; en particular, no tiene solución para puntos de $\mathcal{S}$; por lo que $\mathcal{S}$ es no singular.

Notemos que en $\mathcal{S}$ tenemos algunas secciones evidentes:

$$\begin{aligned}
\sigma_1([T:U]) &= ([0:1:1]\,;[T:U])\\
\sigma_2([T:U]) &= ([0:-2:1]\,;[T:U])\\
\sigma_3([T:U]) &= ([T:-2U:U]\,;[T:U])
\end{aligned}$$

Precisamente estas secciones se corresponden con curvas irreducibles de $\mathcal{S}$. Sea $\Gamma_1 \subseteq \mathcal{S}$ dada por las ecuaciones:

$$\Gamma_1 : \begin{cases} X & = 0 \\ Y - Z & = 0 \end{cases}$$

En efecto $\Gamma_1 \subseteq \mathcal{S}$ y es irreducible. Para verificar que es irreducible afirmamos que el ideal homogéneo que define a Γ_1 es:

$$I(\Gamma_1) = (X, Y - Z).$$

Es claro que el ideal del miembro derecho está incluido en $I(\Gamma_1)$. Para ver la otra inclusión tomemos cualquier $f \in I(\Gamma_1)$ y escribamos:

$$f(X, Y, Z, T, U) = Xq_1 + (Y - Z)q_2 + R(Z, T, U).$$

Como $f \in I(\Gamma_1)$ se tiene que:

$$0 = f(0, Z, Z, T, U) = R(Z, T, U), \ \forall Z \in \bar{\mathbb{Q}} \ \ y \ \forall [T : U] \in \mathbb{P}^1.$$

Luego $R = 0$, por lo que $f \in (X, Y - Z)$.

Podíamos hacer esto de otra forma, que es la siguiente. Si consideramos las dos proyecciones de $\mathcal{S}$, a la primera y a la segunda coordenada; tenemos que:

$$\pi_1(\Gamma_1) = [0 : 1 : 1]\,,$$

y:

$$\pi_2(\Gamma_1) = \mathbb{P}^1.$$

Aprovechando esta particularidad resulta que:

$$\Gamma_1 = \pi_1^{-1}([0 : 1 : 1]).$$

Luego:

$$I(\Gamma_1) = \pi_1^{-1}(I([0 : 1 : 1]) = \pi_1^{-1}((X, Y - Z)) = (X, Y - Z).$$

Es claro que $I([0 : 1 : 1]) = (X, Y - Z)$ porque ahora se trata del ideal de un punto de una superficie. O sea, con este razonamiento de mirar las proyecciones, pudimos reducirnos al caso de mirar el ideal de un punto, que es bastante más sencillo. Sin embargo, pudimos hacerlo sólo porque Γ_1 tiene esa particularidad de proyectarse en un punto. Con cualquier curva arbitraria no vamos a poder hacer lo mismo.

Ahora sólo nos falta verificar que $I(\Gamma_1)$ es un ideal primo de $\overline{\mathbb{Q}}[X, Y, Z, T, U]$. Pero esto es sencillo. Por comodidad, trabajemos en la afinización $Z = U = 1$. Podemos hacer esto, pues Γ_1 está contenida casi toda en esa afinización, ya que sólo se pierde el punto $([0 : 1 : 1]\,; [1 : 0])$; con lo cual, el comportamiento de Γ_1 basta mirarlo en ese abierto afín. Allí tenemos:

$$\frac{\overline{\mathbb{Q}}[x, y, t]}{I(\Gamma_1)} = \frac{\overline{\mathbb{Q}}[x, y, t]}{(x, y - 1)} \simeq \overline{\mathbb{Q}}[t]\,;$$

y este último anillo es un dominio íntegro. Luego, efectivamente $\Gamma_1 \subseteq \mathcal{S}$ es una curva irreducible. Además, por cómo la construimos, resulta precisamente que:

$$\Gamma_1 = Im(\sigma_1) = \sigma_1(\mathbb{P}^1).$$

Análogamente, se tienen:

$$\Gamma_2 = Im(\sigma_2) \;\; y \;\; \Gamma_3 = Im(\sigma_3);$$

donde:

$$\Gamma_2 \; : \; \begin{cases} X & = 0 \\ Y + 2Z & = 0 \end{cases}$$

Para obtener el ideal que define a Γ_3 hay que tener un poco más de cuidado. Observando que, para Γ_3, $X = T$, $Z = U$ e $Y + 2Z = 0$; uno está tentado a decir que Γ_3 está dada por:

$$\Gamma_3 \; : \; \begin{cases} X - T & = 0 \\ Y + 2Z & = 0 \\ Z - U & = 0 \end{cases}$$

Pero el primero y el tercero de esos polinomios no son homogéneos en $\mathbb{P}^2 \times \mathbb{P}^1$. Hay que ajustar este detalle y lo podemos hacer multiplicando a sus coeficientes por variables adecuadas. Afirmamos así que:

$$\Gamma_3 \; : \; \begin{cases} XU - ZT & = 0 \\ Y + 2Z & = 0 \\ ZT - XU & = 0 \end{cases}$$

Como la tercera ecuación es la misma que la primera, podemos suprimirla:

$$\Gamma_3 \; : \; \begin{cases} XU - ZT & = 0 \\ Y + 2Z & = 0 \end{cases}$$

Observemos que, justamente, como los σ_i son secciones, tenemos que:

$$\pi \circ \sigma_i = id_{\mathbb{P}^1}.$$

En particular, $\pi|_{\Gamma_i} \; : \; \Gamma_i \longrightarrow \mathbb{P}^1$ es un morfismo suryectivo. Por lo tanto las curvas Γ_i que encontramos son curvas **horizontales** de $\mathcal{S}$.

Encontrar curvas fibrales es, en cierta forma, más sencillo. Basta con fijar un punto $p = [T : U] \in \mathbb{P}^1$ y ver cómo queda la fibra $\mathcal{S}_p$. Por ejemplo, tomemos $p_0 = [0 : 1]$. En tal caso, la fibra $\mathcal{S}_{p_0}$ consta de los puntos de ecuación:

$$\mathcal{S}_{p_0} \; : \; F(X, Y, Z, 0, 1) = X^2 + Y^2 + YZ - 2Z^2 = 0.$$

$\mathcal{S}_{p_0}$ es una variedad proyectiva de $\mathbb{P}^2$. De un modo similar al que hicimos ya un par de veces, se puede verificar que el ideal que la define es efectivamente:

$$I(\mathcal{S}_{p_0}) = (F(X, Y, Z, 1, 0));$$

y dado que $F(X,Y,Z,1,0)$ es un polinomio homogéneo irreducible (esto también es fácil de comprobar), $I(\mathcal{S}_{p_0})$ es un ideal primo de $\overline{\mathbb{Q}}[X,Y,Z]$; por lo que $\mathcal{S}_{p_0}$ es una variedad irreducible.

Geométricamente, si afinizamos $\mathcal{S}_{p_0}$ respecto de alguna de las variables, lo que obtenemos es una cónica en el plano.

En definitiva, en este caso, la fibra $\mathcal{S}_{p_0}$ ya es en sí misma una curva irreducible de $\mathcal{S}$. Tenemos entonces, en particular, que $\Gamma_4 = \mathcal{S}_{p_0}$ es una curva **fibral** de $\mathcal{S}$. Pues ocurre que:

$$\pi|_{\Gamma_4} \,:\, \Gamma_4 \longrightarrow \mathbb{P}^1,$$

es constante. Precisamente, $\pi|_{\Gamma_4}(P) = [0:1],\ \forall P \in \Gamma_4$.

Busquemos más curvas fibrales. Miremos ahora la fibra de $p_\infty = [1:0]$. En este caso nos queda que la fibra $\mathcal{S}_{p_\infty}$ está dada por la ecuación:

$$\mathcal{S}_{p_\infty} \,:\, XY + XZ = 0.$$

Aquí es más sencilla aún la cuenta. Claramente $\mathcal{S}_{p_\infty}$ no es irreducible. Tenemos:

$$\mathcal{S}_{p_\infty} \,:\, XY + XZ = X(Y+Z) = 0.$$

O sea, $\mathcal{S}_{p_\infty}$ consta de la unión de los conjuntos $\{X=0\}$ y $\{Y+Z=0\}$. Geométricamente, $\mathcal{S}_{p_\infty}$ es la unión de 2 rectas; que son justamente sus componentes irreducibles. Tenemos precisamente que:

$$\Gamma_5 \,:\, X = 0 \quad y \quad \Gamma_6 \,:\, Y + Z = 0,$$

son curvas **fibrales** de $\mathcal{S}$. Concretamente:

$$\pi|_{\Gamma_5}(P) = [1:0],\ \forall P \in \Gamma_5 \quad y \quad \pi|_{\Gamma_6}(P) = [1:0],\ \forall P \in \Gamma_6.$$

Ya tenemos varios ejemplos tanto de curvas horizontales como de curvas fibrales. Con ellas podemos construir ejemplos de divisores de $\mathcal{D}iv(\mathcal{S})$. Lo que vamos a hacer ahora es calcular $div(G)$ para algún elemento de $\overline{\mathbb{Q}}(\mathcal{S})$. Recordemos que los elementos de $\overline{\mathbb{Q}}(\mathcal{S})$ pueden verse como cocientes de polinomios homogéneos de igual grado. Pongamos un ejemplo sencillo entonces. Sea $G(X,Y,Z,T,U) \in \overline{\mathbb{Q}}(\mathcal{S})$ la siguiente función:

$$G(X,Y,Z,T,U) = \frac{Y+2Z}{Z}.$$

Tenemos que calcular $ord_\Gamma(G)$ para todas las curvas $\Gamma \subseteq \mathcal{S}$ irreducibles. Para ello busquemos aquellas curvas $\Gamma \subseteq \mathcal{S}$ a lo largo de las cuales G tenga ceros o polos. Es decir, buscamos las curvas $\Gamma \subseteq \mathcal{S}$ irreducibles tales que:

$$G|_\Gamma \equiv 0 \ \ o \ \ G|_\Gamma \equiv \infty.$$

Veamos:

$$G(X,Y,Z,T,U) = 0 \Rightarrow Y + 2Z = 0 \Rightarrow Y = -2Z.$$

Los puntos de $\mathcal{S}$ que verifican $Y = -2Z$ son puntos de la forma $([X : -2Z : Z]\,;[T : U])$; y que satisfacen la ecuación:

$$X^2U + 4Z^2U - 2XZT + XZT - 2Z^2U - 2Z^2U = 0.$$

Pero luego de simplificar $4Z^2U$ con $-2Z^2U - 2Z^2U$, queda simplemente:

$$X^2U - XZT = 0 \Leftrightarrow X(XU - ZT) = 0.$$

Entonces $X = 0$ o $XU - ZT = 0$.

En el caso $X = 0$, como tenemos que $Y = -2Z$, tenemos la familia de puntos:

$$\{([0 : -2 : 1]\,;[T : U])\}\,.$$

Esto no es otra cosa que la curva horizontal Γ_2 que encontramos antes.

En el otro caso nos quedan las condiciones:

$$\begin{cases} XU - ZT &= 0 \\ Y + 2Z &= 0 \end{cases}$$

Esto es exactamente la curva Γ_3.

Ahora planteemos que el denominador de G sea 0. Es decir: $Z = 0$. Tenemos en este caso que los puntos de $\mathcal{S}$ que satisfacen esta condición son los que surgen de la ecuación:

$$X^2U + Y^2U + XYT = 0.$$

Es decir:

$$U(X^2 + Y^2) + XYT = 0.$$

Este es un polinomio irreducible y es muy claro cuál es la curva en cuestión si suponemos $U \neq 0$ y $XY \neq 0$:

$$\frac{T}{U} = -\frac{X^2 + Y^2}{XY}.$$

O sea:

$$t = -\frac{X^2 + Y^2}{XY}.$$

Nos queda la familia de puntos:

$$\left\{\left([X : Y : 0]\,;\left[-\frac{X^2 + Y^2}{XY} : 1\right]\right)\right\} = \left\{\left([X : Y : 0]\,;\left[-Y^2 - X^2 : XY\right]\right)\right\}.$$

Esta es una nueva curva irreducible que llamaremos Γ_7. Notemos que Γ_7 es una curva horizontal de $\mathcal{S}$.

Antes de seguir, observemos un detalle. Cuando hicimos la correspondencia entre curvas elípticas E sobre $\overline{\mathbb{Q}(t)}$ y superficies elípticas $\mathcal{E}$, dijimos que los **puntos** de E se correspondían con

secciones de $\mathcal{E}$. Para las superficies fibradas en general esto no deja de ser cierto. En nuestro ejemplo, si llamamos C a la curva sobre $\overline{\mathbb{Q}(t)}$ asociada a $\mathcal{S}$; la sección σ_1, que es la que determina la curva horizontal Γ_1 de $\mathcal{S}$, se corresponde con el punto $[T : -2U : U]$ de C; la sección σ_2, que es la que determina la curva horizontal Γ_2 de $\mathcal{S}$, se corresponde con el punto $[0 : 1 : 1]$ de C; etc. Miremos qué pasa con la curva horizontal Γ_7. Nos había quedado la ecuación:

$$X^2U + Y^2U + XYT = 0.$$

Si afinizamos en $Y = U = 1$, queda:

$$x^2 + 1 + xt = 0.$$

Ese polinomio es irreducible en $\overline{\mathbb{Q}}[x, t]$; pero si pensamos esto en el contexto de C; es decir, trabajando sobre el cuerpo $\overline{\mathbb{Q}(t)}$; ocurre que hay dos soluciones:

$$x = \frac{-t + \sqrt{t^2 - 4}}{2} \quad y \quad x = \frac{-t - \sqrt{t^2 - 4}}{2}.$$

De este modo obtenemos dos puntos de C, que son:

$$P_1 = \left[\frac{-t + \sqrt{t^2 - 4}}{2} : 1 : 0\right] \quad y \quad P_2 = \left[\frac{-t - \sqrt{t^2 - 4}}{2} : 1 : 0\right].$$

¿Qué nos dice esto? ¿Que la sección Γ_7 está en correspondencia con dos puntos distintos de C? No! Justamente esto no puede ocurrir, y la sencilla razón es que Γ_7 **no** corresponde a ninguna sección de $\mathcal{S}$. Si bien Γ_7 es una curva horizontal, pues $\pi|_{\Gamma_7}$ es suryectiva; no existe ninguna sección σ de $\mathcal{S}$ tal que $Im(\sigma) = \Gamma_7$. Podríamos decir que Γ_7 es una curva irreducible en la superficie $\mathcal{S}$ definida sobre $\overline{\mathbb{Q}}$; pero cuando vemos a la superficie como una curva C sobre $\overline{\mathbb{Q}(t)}$; la curva Γ_7 se *separa* en dos puntos.

Sigamos con nuestro cálculo. Tenemos ahora sí todas las posibles curvas en las cuales el orden de G puede ser no nulo. Pues, en cualquier otra, ni $Y + 2Z$ ni Z pertenecen al ideal I_Γ por cuanto $ord_\Gamma(G) = 0$. En definitiva tenemos que:

$$ord(G) = \sum_{\Gamma \subseteq \mathcal{S}} ord_\Gamma(G)(\Gamma) = n_2(\Gamma_2) + n_3(\Gamma_3) + n_7(\Gamma_7).$$

Donde $n_i = ord_{\Gamma_i}(G)$. Sólo nos falta calcular los números enteros n_2, n_3 y n_7.

Empecemos por n_2. Tenemos que:

$$I_{\Gamma_2} = (X, Y + 2Z).$$

Consideremos la función que define a la superficie $\mathcal{S}$:

$$F(X, Y, Z, T, U) = X^2U + Y^2U + XYT + XZT + YZU - 2Z^2U.$$

Afinicemos en Z y en U, así obtenemos:

$$f(x, y, t) = x^2 + y^2 + xyt + xt + y - 2.$$

El ideal que define a Γ_2 en este espacio afín es $(x, y+2)$. Mirando la ecuación $f(x,y,t)=0$ y haciendo algunas operaciones algebraicas obtenemos:

$$f(x,y,t)=0 \Leftrightarrow x^2+y^2+xyt+xt+y-2=0 \Leftrightarrow x(x-t)=(-xt-y-1)(y+2);$$

donde la última es una igualdad en el anillo de coordenadas $\overline{\mathbb{Q}}[\mathcal{S}]$. Pero si consideramos la localización $\mathcal{O}_{\Gamma_2}$, como claramente $x-t \notin (x, y+2)$, resulta que $x-t$ es una unidad en $\mathcal{O}_{\Gamma_2}$. De modo que:

$$x=\left(\frac{-xt-y-1}{x-t}\right)(y+2) \ \ en\, \mathcal{O}_{\Gamma_2}.$$

En particular, $x \in (y+2)\mathcal{O}_{\Gamma_2}$. Por lo tanto, el ideal que define a Γ_2 es simplemente $(y+2)$. O sea, $y+2$ es un uniformizador local. Volviendo a coordenadas homogéneas, tenemos entonces que $I_{\Gamma_2}\mathcal{O}_{\Gamma_2}=(Y+2Z)\mathcal{O}_{\Gamma_2}$. Por otro lado, es evidente que $Z \notin (Y+2Z)$. Con todo esto es claro que:

$$n_2=ord_{\Gamma_2}(G)=ord_{\Gamma_2}\left(\frac{Y+2Z}{Z}\right)=1.$$

Calculemos ahora n_3. Volvamos a trabajar en el afín $Z=U=1$. De nuevo, podemos hacerlo ya que sólo perdemos un punto de Γ_3 que no está en esa afinización, que es el $([1:0:0]\,;[1:0])$. El ideal que define a Γ_3 es $I_{\Gamma_3}=(XU-ZT, Y+2Z)$; y trabajando en la afinización queda $(x-t, y+2)$. Aprovechando la misma cuenta que hicimos antes, tenemos que la ecuación $f(x,y,t)=0$ puede escribirse como:

$$x(x-t)=(-xt-y-1)(y+2);$$

y esta igualdad es en el anillo de coordenadas $\overline{\mathbb{Q}}[\mathcal{S}]$. Pero, como antes, consideremos ahora la localización $\mathcal{O}_{\Gamma_3}$; y en este caso se tiene que $x \notin (x-t, y+2)$, por lo que es una unidad en $\mathcal{O}_{\Gamma_3}$. Así que:

$$x-t=\left(\frac{-xt-y-1}{x}\right)(y+2)\ en\, \mathcal{O}_{\Gamma_3}.$$

Con lo cual, $x-t \in (y+2)\mathcal{O}_{\Gamma_3}$; de modo que, volviendo a coordenadas homogéneas, $I_{\Gamma_3}\mathcal{O}_{\Gamma_3}=(Y+2Z)\mathcal{O}_{\Gamma_3}$.

De nuevo, $Z \notin (Y+2Z)$; así que concluimos que:

$$n_3=ord_{\Gamma_3}(G)=ord_{\Gamma_3}\left(\frac{Y+2Z}{Z}\right)=1.$$

Sólo nos falta calcular n_7. Recordemos que la curva Γ_7 está dada por:

$$\Gamma_7\ :\ \left\{\left([X:Y:0]\,;\left[-Y^2-X^2:XY\right]\right)\right\}.$$

Aquí nos va a convenir trabajar en el afín $Y=U=1$. Allí tenemos:

$$\Gamma_7\ :=\left\{\left([x:1:0]\,;\left[\frac{-1-x^2}{x}:1\right]\right)\right\}.$$

No es difícil ver que el ideal que define a Γ_7 en esta afinización es: $(z, x^2 + 1 + xt)$. Hagamos el procedimiento análogo a lo que hicimos con Γ_2 y Γ_3. Miremos la ecuación que define a $\mathcal{S}$ en este espacio afín; esto es:

$$f(x, z, t) = x^2 + 1 + xt + xzt + z - 2z^2.$$

Considerando la ecuación $f(x, z, t) = 0$ y operando algebraicamente obtenemos:

$$f(x, z, t) = 0 \Leftrightarrow x^2 + 1 + xt = z(2z - 1 - xt).$$

De modo que, como hicimos antes, se tiene que $x^2 + 1 + xt \in (z)\mathcal{O}_{\Gamma_7}$; y por lo tanto $I_{\Gamma_7}\mathcal{O}_{\Gamma_7} = (Z)\mathcal{O}_{\Gamma_7}$.

Dado que $Y + 2Z \notin (Z)$ llegamos a que:

$$n_7 = ord_{\Gamma_7}(G) = ord_{\Gamma_7}(\frac{Y + 2Z}{Z}) = -1.$$

Nos queda entonces que:

$$div(G) = (\Gamma_2) + (\Gamma_3) - (\Gamma_7).$$

Observemos que $deg(div(G)) \neq 0$, y no tenía por qué serlo; pues eso es una propiedad que se daba en las curvas, en las superficies ya no necesariamente. Pero podemos hacer una observación interesante. Recordemos que podíamos ver a nuestra superficie $\mathcal{S}$ como una curva C sobre $\overline{k} = \overline{\mathbb{Q}(t)}$. Miremos también a nuestra función G como un elemento de $\overline{k}(C)$, el cuerpo de funciones de C. Debería ser cierto que, en el grupo $\mathcal{D}iv(C)$; $div(G) = 0$. Esto va a ser efectivamente cierto y lo podemos ver fácilmente. Si repitiéramos la cuenta pero en el contexto de C, veríamos que la función G tiene un cero en los puntos:

$$P_1 = [0 : -2 : 1] \;\; y \;\; P_2 = [T : -2U : U]\,;$$

que son justamente los que se corresponden con las secciones que determinan a Γ_2 y a Γ_3 respectivamente. La cosa cambia cuando miramos los puntos en donde G tiene polos. Resulta que aparecen dos puntos, que son:

$$P_3 = \left[\frac{-t + \sqrt{t^2 - 4}}{2} : 1 : 0\right] \;\; y \;\; P_4 = \left[\frac{-t - \sqrt{t^2 - 4}}{2} : 1 : 0\right].$$

Estos son justamente los dos puntos en los que se separa la curva Γ_7 cuando la miramos sobre la curva C. Va a resultar entonces que:

$$div(G) = (P_1) + (P_2) - (P_3) - (P_4).$$

Para terminar de ilustrar esta parte, mostremos un ejemplo de algún divisor de la forma $\pi^*(D)$ para $D \in \mathcal{D}iv(\mathbb{P}^1)$. Tenemos un ejemplo a mano aprovechando todo lo que ya hicimos. Definamos $D \in \mathcal{D}iv(\mathbb{P}^1)$ como:

$$D = (p_0) + (p_\infty);$$

donde $p_0 = [0:1]$ y $p_\infty = [1:0]$. Tenemos entonces que:

$$\pi^*(D) = \sum_{\Gamma \subseteq \mathcal{S}_{p_0}} ord_\Gamma(u_{p_0} \circ \pi)(\Gamma) + \sum_{\Gamma \subseteq \mathcal{S}_{p_\infty}} ord_\Gamma(u_{p_\infty} \circ \pi)(\Gamma).$$

Donde u_{p_0},$u_{p_\infty} \in \overline{\mathbb{Q}}(\mathbb{P}^1)$ son uniformizadores locales de los anillos locales de $\mathbb{P}^1$ en p_0 y p_∞ respectivamente. Claramente podemos tomar:

$$u_{p_0} = \frac{T}{U} \ y \ u_{p_\infty} = \frac{U}{T}.$$

Recordando que $\pi([X:Y:Z];[T:U]) = [T:U]$, nos queda:

$$(u_{p_0} \circ \pi)([X:Y:Z];[T:U]) = \frac{T}{U} \ y \ (u_{p_\infty} \circ \pi)([X:Y:Z];[T:U]) = \frac{U}{T}.$$

Pero el cálculo de $ord_\Gamma(\frac{T}{U})$ y $ord_\Gamma(\frac{U}{T})$ es bien sencillo. Recordemos primero que en $\mathcal{S}_{p_0}$ hay sólo una curva irreducible, que es justamente toda la fibra $\mathcal{S}_{p_0}$; que habíamos llamado Γ_4. Es la curva dada por:

$$X^2 + Y^2 + YZ - 2Z^2 = 0.$$

En $\mathcal{S}_{p_\infty}$ hay dos curvas, que son las rectas $\Gamma_5 : X = 0$ y $\Gamma_6 : Y + Z = 0$. De este modo:

$$\pi^*(D) = n_4(\Gamma_4) + n_5(\Gamma_5) + n_6(\Gamma_6).$$

Donde $n_4 = ord_{\Gamma_4}(\frac{T}{U})$ y $n_i = ord_{\Gamma_i}(\frac{U}{T})$, $i = 5, 6$.

Haciendo un desarrollo análogo al que hicimos antes, podemos verificar rápidamente que $n_4 = n_5 = n_6 = 1$. La razón de fondo de esta cuenta es que las curvas Γ_4, Γ_5 y Γ_6 aparecen con multiplicidad 1 en la ecuación que define a la superficie $\mathcal{S}$. Esto es en definitiva lo que usamos. En conclusión nos queda que:

$$\pi^*(D) = (\Gamma_4) + (\Gamma_5) + (\Gamma_6).$$

3.3.2. Intersección

En esta parte vamos a trabajar con una noción geométrica que va a se crucial para las construcciones que vamos a hacer luego. Hasta aquí hemos construido el grupo abeliano $\mathcal{D}iv(\mathcal{S})$ asociado a una superficie fibrada no singular $\mathcal{S}$. Lo que nos interesa hacer ahora es construir una forma bilineal simétrica:

$$\mathcal{D}iv(\mathcal{S}) \times \mathcal{D}iv(\mathcal{S}) \longrightarrow \mathbb{Z}.$$

Esta forma bilineal va a ser un objeto abstracto que tendrá una interpretación geométrica muy precisa y va a ser muy útil para las construcciones que queremos hacer más adelante.

Recordemos que los elementos de $\mathcal{D}iv(\mathcal{S})$ son combinaciones lineales finitas de curvas irreducibles $\Gamma \subseteq \mathcal{S}$. De manera que, para definir la forma bilineal aplicada a un par $(D_1, D_2) \in \mathcal{D}iv(\mathcal{S}) \times \mathcal{D}iv(\mathcal{S})$, basta hacerlo para sus componentes y extender por linealidad. Es decir, vamos a ver

cómo se define la forma bilineal aplicada a un par de la forma (Γ_1, Γ_2) y luego extenderemos por linealidad a cualquier par de divisores.

Consideremos entonces dos curvas irreducibles Γ_1 y Γ_2. El número entero asociado a (Γ_1, Γ_2), que lo vamos a notar $\Gamma_1.\Gamma_2$; representará la cantidad de intersecciones entre Γ_1 y Γ_2 contadas con su multiplicidad. Para ello pensemos que nuestras curvas irreducibles Γ_1 y Γ_2 son distintas. Asumiendo esto, las curvas se van a intersecar en finitos puntos. Por lo tanto nos basta mirar qué pasa en cada uno de esos puntos y después sumar. Es decir, vamos a definir el índice de intersección en cada P; y lo notaremos $(\Gamma_1.\Gamma_2)_P$; que representará la multiplicidad con la que Γ_1 y Γ_2 se cortan en P. Después sumaremos sobre todos los puntos de $\Gamma_1 \cap \Gamma_2$. Concretamente estamos diciendo que:

$$\Gamma_1.\Gamma_2 = \sum_{P \in \Gamma_1 \cap \Gamma_2} (\Gamma_1.\Gamma_2)_P.$$

Si Γ_1 y Γ_2 no se intersecan vamos a definir obviamente: $\Gamma_1.\Gamma_2 = 0$.

Sólo bastaría definir $(\Gamma_1.\Gamma_2)_P$. Lo que queremos es que este número represente la multiplicidad, o el orden de contacto con el que se intersecan Γ_1 y Γ_2 en P. Intuitivamente, queremos que si Γ_1 y Γ_2 se cortan *transversalmente* en P; entonces $(\Gamma_1.\Gamma_2)_P = 1$. A partir de esto es que surge la idea para la definición general. Supongamos que $f_1,\ f_2 \in \overline{\mathbb{Q}}(\mathcal{S})^\times$ son funciones definidas en P que determinan a Γ_1 y a Γ_2 respectivamente. Esto es, $f_1,\ f_2 \in \mathcal{O}_P$, $ord_{\Gamma_i}(f_i) = 1$ y $ord_{\Gamma}(f_i) = 0$ para cualquier otra curva irreducible $\Gamma \subseteq \mathcal{S}$. Como $f_1(P) = f_2(P) = 0$, entonces $f_1,\ f_2 \in \mathcal{M}_P$, el ideal maximal en P; y si Γ_1 y Γ_2 se cortan transversalmente, en el anillo local $\mathcal{O}_P$ podemos pensar, intuitivamente, que son elementos bien distintos. De esto surge la idea de considerar el ideal $(f_1, f_2) \subseteq \mathcal{M}_P$ y ver cuán lejos está esa inclusión de ser una igualdad. Cuanto más cerca esté, es porque f_1 y f_2 se comportan distinto alrededor de P. Es así que uno quiere que, si se cortan transversalmente, el índice de intersección sea 1, y se dé la igualdad. Formalizando estas ideas es como surge la definición.

Consideremos el cociente:

$$\mathcal{O}_P/(f_1, f_2).$$

Este cociente tiene estructura de $\overline{\mathbb{Q}}$-espacio vectorial, por lo que podemos considerar su dimensión. Pues bien, definiremos:

$$(\Gamma_1.\Gamma_2)_P = dim_{\overline{\mathbb{Q}}}\left(\mathcal{O}_P/(f_1, f_2)\right).$$

Notemos que, si $(f_1, f_2) = \mathcal{M}_P$, efectivamente $(\Gamma_1.\Gamma_2)_P = 1$, pues la hipótesis de que $\mathcal{S}$ es no singular es la que nos asegura que:

$$dim_{\overline{\mathbb{Q}}}(\mathcal{O}_P/\mathcal{M}_P) = 1$$

Empecemos con un ejemplo sencillo. Tomemos $\mathcal{S} = \mathbb{P}^2$, las curvas:

$$\Gamma_1 : X = 0 \ y \ \Gamma_2 : Y = 0.$$

Γ_1 y Γ_2 no son más que dos copias de $\mathbb{P}^1$, que, en el plano afín $Z = 0$, son los ejes coordenados. Sea $P = [0:0:1]$, que afinizando en Z, sus coordenadas afines son $P = (0,0)$. Tenemos que

Γ_1 y Γ_2 se cortan en P. Y se cortan de una manera transversal. Elijamos funciones f_1 y f_2 que determinen a Γ_1 y a Γ_2 y veamos si efectivamente el ideal (f_1, f_2) es igual al ideal maximal $\mathcal{M}_P$. En efecto, podemos trabajar en el afín $Z = 0$ y allí podemos tomar:

$$f_1(x, y) = x \;\; y \;\; f_2(x, y) = y.$$

Además tenemos:

$$\mathcal{M}_P = (x, y).$$

De manera que, en efecto, $(f_1, f_2) = \mathcal{M}_P$. Luego, $(\Gamma_1.\Gamma_2)_P = 1$.

Generalicemos un poco ahora y veamos que, en efecto, si la intersección entre las curvas es transversal, entonces $(\Gamma_1.\Gamma_2)_P = 1$. Vamos a hacerlo en el caso en que Γ_1 y Γ_2 se intersecan transversalmente en el punto afín $P = (0, 0)$ y son no singulares en ese punto. Este caso es representativo, pues, mediante una simple traslación se puede llevar el razonamiento a cualquier otro punto.

Lema 3.3.9. *Sea $\mathcal{S}$ una superficie no singular y sean $\Gamma_1, \Gamma_2 \subseteq \mathcal{S}$ curvas irreducibles que se intersecan en el punto $P = [0 : 0 : 1]$ y son no singulares en ese punto. Sean f_1, $f_2 \in \mathcal{M}_P$ funciones que determinan a Γ_1 y a Γ_2 respectivamente. Supongamos que la intersección en P es transversal; es decir, las rectas tangentes a Γ_1 y Γ_2 en P son distintas. Entonces:*

$$(\Gamma_1.\Gamma_2)_P = dim_{\overline{\mathbb{Q}}}(\mathcal{O}_P/(f_1, f_2)) = 1.$$

Demostración: Podemos trabajar en el afín $Z = 1$. Queremos ver que $(f_1, f_2) = \mathcal{M}_P = (x, y)$. Sólo hace falta probar que $\mathcal{M}_P \subseteq (f_1, f_2)$. Escribamos:

$$\Gamma_1 \; : \; f_1(x, y) = xg_{11}(x, y) + yg_{12}(x, y) + ax + by = 0.$$

$$\Gamma_2 \; : \; f_2(x, y) = xg_{21}(x, y) + yg_{22}(x, y) + cx + dy = 0.$$

Con $g_{11}, g_{12}, g_{21}, g_{22} \in \mathcal{M}_P$.

Dado que estamos asumiendo que Γ_1 y Γ_2 son no singulares en $P = (0, 0)$, necesariamente $(a, b) \neq (0, 0)$ y $(c, d) \neq (0, 0)$. Más aún, es fácil ver que las rectas tangentes a Γ_1 y Γ_2 en P son respectivamente:

$$R_1 \; : \; ax + by = 0.$$

$$R_2 \; : \; cx + dy = 0.$$

Si suponemos que la intersección es transversal, entonces $R_1 \neq R_2$. Y esto es decir que:

$$ad - bc \neq 0.$$

Supongamos, sin perder generalidad, que $d \neq 0$; pues si $d = 0$, entonces $b \neq 0$ y se sigue un razonamiento análogo al que vamos a hacer. Miramos el cociente:

$$\mathcal{O}_P/(f_1, f_2)\,;$$

y allí tenemos que:

$$y = -\frac{xg_{21}(x,y) + yg_{22}(x,y) + cx}{d}.$$

Mirando la ecuación de Γ_1 nos queda que:

$$xg_{11}(x,y) + yg_{12}(x,y) + ax - b\left(\frac{xg_{21}(x,y) + yg_{22}(x,y) + cx}{d}\right) = 0.$$

Multiplicando por d y agrupando los términos tenemos:

$$x(dg_{11}(x,y) - bg_{21}(x,y) + (ad - bc)) = y(bg_{22}(x,y) - dg_{12}(x,y)).$$

Pero como $g_{11}, g_{21} \in \mathcal{M}_P$ y $ad - bc \neq 0$, entonces:

$$dg_{11}(x,y) - bg_{21}(x,y) + (ad - bc) \notin \mathcal{M}_P,$$

con lo cual es una unidad en $\mathcal{O}_P$. Por lo tanto $x = k(x,y)y$ en $\mathcal{O}_P/(f_1, f_2)$. Donde:

$$k(x,y) = \frac{bg_{22}(x,y) - dg_{12}(x,y)}{dg_{11}(x,y) - bg_{21}(x,y) + (ad - bc)} \in \mathcal{O}_P.$$

Más aún, $k(x,y) \in \mathcal{M}_P$. Reemplazando en la ecuación de Γ_2 nos queda:

$$k(x,y)yg_{21}(k(x,y)y, y) + yg_{22}(k(x,y)y, y) + ck(x,y)y + dy = 0.$$

O sea,

$$y(k(x,y)g_{21}(k(x,y)y, y) + g_{22}(k(x,y)y, y) + ck(x,y) + d) = 0.$$

Como $k(x,y)g_{21}(k(x,y)y, y) + g_{22}(k(x,y)y, y) + ck(x,y) \in \mathcal{M}_P$ y $d \neq 0$, el factor que multiplica a y no está en $\mathcal{M}_P$; de modo que es una unidad en $\mathcal{O}_P$. Luego, $y = 0$. Esto es, $y = 0$ en $\mathcal{O}_P/(f_1, f_2)$; por lo que $y \in (f_1, f_2)$. Y en consecuencia:

$$x = k(x,y)y \in (f_1, f_2).$$

Por lo tanto, efectivamente $\mathcal{M}_P = (x,y) \subseteq (f_1, f_2)$. □

La técnica que usamos para la demostración también puede usarse para calcular el índice de intersección en el caso en que las rectas tangentes coinciden.

Vamos a mostrar ahora un ejemplo en donde la intersección tiene orden mayor a 1 y vamos a hacerlo usando directamente la definición. En $\mathbb{P}^2$ consideremos las curvas de ecuación afín:

$$\begin{aligned} \Gamma_1 : f_1(x,y) &= x^4 + x^3 - y = 0 \\ \Gamma_2 : f_2(x,y) &= 2x^5y^2 - 3x^3 + y = 0 \end{aligned}$$

Ambas se intersecan en el punto afín $P = (0,0)$. Tenemos $\mathcal{M}_P = (x,y)$ y queremos calcular:

$$(\Gamma_1.\Gamma_2)_P = dim_{\overline{\mathbb{Q}}}(\mathcal{O}_P/(f_1, f_2)).$$

Aquí,

$$\mathcal{O}_P = \overline{\mathbb{Q}}\,[x,y]_{(0,0)} = \left\{ \frac{f}{g} \in \overline{\mathbb{Q}}(x,y) \,:\, g(0,0) \neq 0 \right\}.$$

Entonces queremos mirar la dimensión como $\overline{\mathbb{Q}}$-espacio vectorial de:

$$\frac{\overline{\mathbb{Q}}\,[x,y]_{(0,0)}}{(f_1,f_2)}.$$

Tenemos:

$$\frac{\overline{\mathbb{Q}}\,[x,y]_{(0,0)}}{(f_1,f_2)} = \frac{\overline{\mathbb{Q}}\,[x,y]_{(0,0)}}{(x^4+x^3-y, 2x^5y^2-3x^3+y)} = \frac{\overline{\mathbb{Q}}\,[x]_0}{(2x^5(x^4+x^3)^2-3x^3+(x^4+x^3))} =$$

$$\frac{\overline{\mathbb{Q}}\,[x]_0}{(x^3(2x^2(x^4+x^3)^2+x-2))} = \frac{\overline{\mathbb{Q}}\,[x]_0}{(x^3)} \simeq \overline{\mathbb{Q}} + \overline{\mathbb{Q}}x + \overline{\mathbb{Q}}x^2.$$

La última igualdad es porque $2x^2(x^4+x^3)^2+x-2$ es una unidad en $\overline{\mathbb{Q}}\,[x]_0$.

Concluimos así que:

$$(\Gamma_1.\Gamma_2)_P = dim_{\overline{\mathbb{Q}}}(\mathcal{O}_P/(f_1,f_2)) = dim_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}} + \overline{\mathbb{Q}}x + \overline{\mathbb{Q}}x^2) = 3.$$

Ahora sí ya podemos extender todo esto de manera lineal y definir así el valor de $D_1.D_2$. El único comentario que nos falta hacer es que uno quiere que esta forma bilineal sea compatible con la relación de equivalencia que tenemos definida en $\mathcal{D}iv(\mathcal{S})$. Recordemos que $D_1 \sim D_2 \Leftrightarrow D_1 - D_2$ es principal. Para que las cosas se comporten como uno quisiera, es natural pedir que si tenemos $D, D_1, D_2 \in \mathcal{D}iv(\mathcal{S})$ tales que $D_1 \sim D_2$; entonces $D.D_1 = D.D_2$. El siguiente teorema nos asegura que la construcción que hicimos efectivamente se comporta así:

Teorema 3.3.10. *Sea $\mathcal{S}$ una superficie fibrada no singular. Existe una única forma bilineal simétrica:*

$$\begin{array}{ccc} \mathcal{D}iv(\mathcal{S}) \times \mathcal{D}iv(\mathcal{S}) & \longrightarrow & \mathbb{Z} \\ (D_1, D_2) & \longrightarrow & D_1.D_2 \end{array}$$

tal que extiende linealmente a la definición de $\Gamma_1.\Gamma_2$ que dimos arriba para $\Gamma_1 \neq \Gamma_2$; y tal que, dados $D, D_1, D_2 \in \mathcal{D}iv(\mathcal{S})$:

$$D_1 \sim D_2 \Rightarrow D.D_1 = D.D_2.$$

Demostración: Ver [10], Capítulo III, Teorema 7.2. □

A esta forma bilineal la vamos a llamar *índice de intersección.*

El interrogante natural que uno se plantea en este punto es el siguiente. Sabemos calcular el índice de intersección entre dos curvas irreducibles distintas. ¿Qué ocurre cuando las curvas son iguales? Es decir, ¿cómo se calcula $\Gamma^2 = \Gamma.\Gamma$? Justamente, la compatibilidad con la relación de equivalencia en $\mathcal{D}iv(\mathcal{S})$ nos va a dar la respuesta. En efecto, supongamos que tenemos una función $f \in \overline{\mathbb{Q}}(\mathcal{S})^\times$ tal que (Γ) sea una de las componentes de $div(f)$. Digamos:

$$div(f) = n(\Gamma) + n_1(\Gamma_1) + n_2(\Gamma_2) + \cdots + n_r(\Gamma_r).$$

Entonces:

$$(-n)(\Gamma) \sim (-n)(\Gamma) + div(f).$$

Por lo tanto:

$$(-n)\Gamma^2 = (\Gamma).(-n)(\Gamma) = (\Gamma).((-n)(\Gamma) + div(f)) = (\Gamma).(n_1(\Gamma_1) + \cdots + n_r(\Gamma_r))$$
$$= n_1(\Gamma).(\Gamma_1) + \cdots + n_r(\Gamma).(\Gamma_r).$$

Y estos últimos los podemos calcular, pues $\Gamma \neq \Gamma_i$.

Finalmente se tiene:

$$\Gamma^2 = -\frac{1}{n}(n_1(\Gamma).(\Gamma_1) + \cdots + n_r(\Gamma).(\Gamma_r)).$$

Observemos que, en consecuencia, Γ^2 es un número racional que no tiene por qué ser positivo.

Antes de presentar algunas propiedades interesantes que satisface el índice de intersección hagamos algunos ejemplos. Retomemos el mismo ejemplo que teníamos:

$$\mathcal{S} \,:\, F(X,Y,Z,T,U) = X^2U + Y^2U + XYT + XZT + YZU - 2Z^2U.$$

Habíamos encontrado varias curvas irreducibles contenidas en $\mathcal{S}$. Calculemos algunos índices de intersección. Tenemos:

$$\begin{aligned}
\Gamma_1 &= \{([0:1:1]\,;[T:U])\}\,.\\
\Gamma_2 &= \{([0:-2:1]\,;[T:U])\}\,.\\
\Gamma_3 &= \{([T:-2U:U]\,;[T:U])\}\,.\\
\Gamma_4 &= \left\{([X:Y:Z]\,;[0:1]) \,:\, X^2+Y^2+YZ-2Z^2=0\right\}.\\
\Gamma_5 &= \{([0:Y:Z]\,;[1:0])\}\,.\\
\Gamma_6 &= \{([X:Z:-Z]\,;[1:0])\}\,.\\
\Gamma_7 &= \left\{\left([X:Y:0]\,;\left[-Y^2-X^2:XY\right]\right)\right\}.
\end{aligned}$$

Claramente $\Gamma_1 \cap \Gamma_2 = \emptyset$, por lo que $\Gamma_1.\Gamma_2 = 0$. También se tiene $\Gamma_1 \cap \Gamma_3 = \emptyset$. Así que también $\Gamma_1.\Gamma_3 = 0$.

Ahora, $\Gamma_2 \cap \Gamma_3 = \{([0:-2:1]\,;[0:1])\}$. Llamemos P a ese punto y calculemos $(\Gamma_2.\Gamma_3)_P$. Para eso veamos si la intersección es transversal o no. Ver esto es sencillo; pues podemos parametrizar las curvas y calcular el vector tangente de cada una de ellas en P. Trabajemos en el afín $Z = U = 1$. Así estamos simplemente en el espacio afín $\overline{\mathbb{Q}}^3$ donde las coordenadas son (x, y, t). Podemos parametrizar allí nuestras curvas del siguiente modo:

$$\Gamma_2 \,:\, \sigma_2(t) = (0, -2, t).$$

$$\Gamma_3 \,:\, \sigma_3(t) = (t, -2, t).$$

Tenemos que $P = (0, 2, 0) = \sigma_2(0) = \sigma_3(0)$. De manera que nos interesa comparar los vectores tangentes $\sigma_2'(0)$ y $\sigma_3'(0)$. Resulta que:

$$\sigma_2'(0) = (0, 0, 1) \;\; y \;\; \sigma_3'(0) = (1, 0, 1).$$

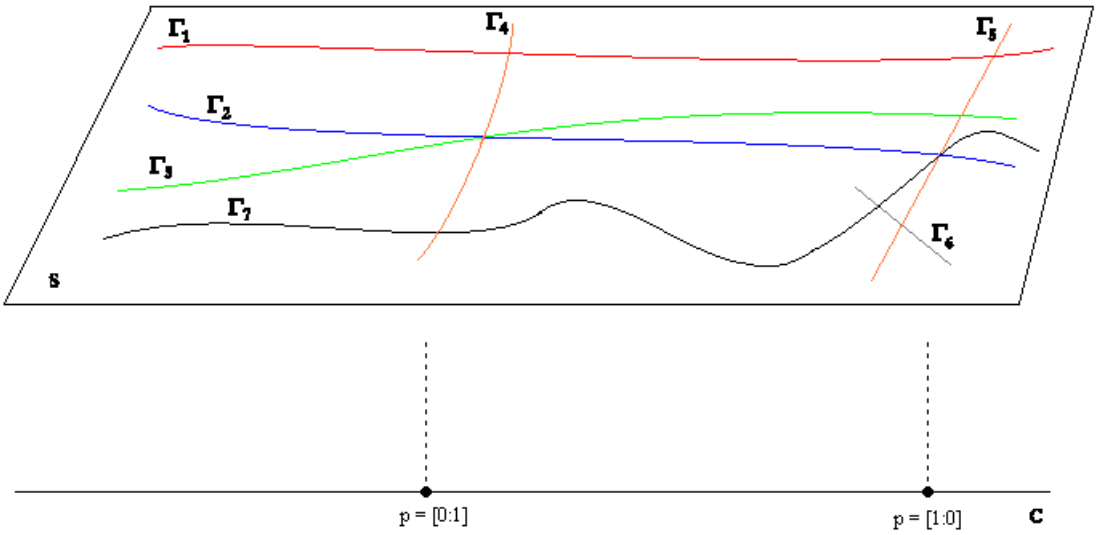


Figura 3.3: Superficie $\mathcal{S}$

Como $\sigma_2'(0) \neq \sigma_3'(0)$, las curvas se intersecan transversalmente. Luego $\Gamma_2.\Gamma_3 = (\Gamma_2.\Gamma_3)_P = 1$.

Haciendo cuentas similares; o sea, parametrizando, podemos verificar que Γ_1, Γ_2 y Γ_3 cortan una vez a la curva fibral Γ_4 y lo hacen transversalmente. Así que $\Gamma_1.\Gamma_4 = \Gamma_2.\Gamma_4 = \Gamma_3.\Gamma_4 = 1$. Más aún, Γ_2 y Γ_3 cortan a Γ_4 en el mismo punto $P = ([0:-2:1]\,;[0:1])$.

Claramente Γ_4 no se interseca con Γ_5 ni con Γ_6; pues son curvas fibrales contenidas en fibras distintas.

También es fácil de ver que Γ_1, Γ_2 y Γ_3 cortan a Γ_5 en un punto transversalmente, y que no cortan a Γ_6.

Con Γ_7 ocurre algo curioso. Esta interseca transversalmente tanto a Γ_5 como a Γ_6 en los puntos $([0:1:0]\,;[1:0])$ y $([1:0:0]\,;[1:0])$ respectivamente. Lo curioso es que corte a dos curvas fibrales distintas contenidas en la misma fibra. Pero en realidad este hecho deja de sorprender si recordamos que Γ_7 no es una sección. Si lo fuera sería imposible que esto pasara.

El diagrama de la superficie $\mathcal{S}$ podemos imaginarlo como se ve en la Figura 3.3.

Calculemos ahora el índice de intersección de una curva consigo misma. Sigamos con el ejemplo de la superficie $\mathcal{S}$ de siempre ya que podemos aprovechar las cuentas que ya hicimos. Tratemos de calcular por ejemplo $\Gamma_2^2 = \Gamma_2.\Gamma_2$; donde, recordemos, $\Gamma_2 = \{([0:-2:1]\,;[T:U])\}$. Habíamos considerado la función $G(X,Y,Z,T,U) \in \overline{\mathbb{Q}}(\mathcal{S})$ definida por:

$$G(X,Y,Z,T,U) = \frac{Y+2Z}{Z}.$$

Y vimos que:

$$div(G) = (\Gamma_2) + (\Gamma_3) - (\Gamma_7).$$

De modo que la función G nos sirve para calcular Γ_2^2. En efecto, se tiene:

$$\Gamma_2^2 = (\Gamma_2).(\Gamma_2) = (\Gamma_2).((\Gamma_2) - div(G)) = (\Gamma_2).(-(\Gamma_3) + (\Gamma_7)) =$$

$$-(\Gamma_2).(\Gamma_3) + (\Gamma_2).(\Gamma_7) = -1 + 0 = -1.$$

Pues ya habíamos visto que $(\Gamma_2).(\Gamma_3) = 1$; y es fácil verificar que $\Gamma_2 \cap \Gamma_7 = \emptyset$.

Claramente podemos aprovechar la misma función G para calcular Γ_3^2 o Γ_7^2. Por ejemplo veamos cuánto da Γ_3^2. Es fácil verificar que $\Gamma_3 \cap \Gamma_7 = \{([1:0:0]\,;[1:0])\}$ y que la intersección es transversal. Por lo que $\Gamma_3.\Gamma_7 = 1$. Entonces:

$$\Gamma_3^2 = (\Gamma_3).(\Gamma_3) = (\Gamma_3).((\Gamma_3) - div(G)) = (\Gamma_3).(-(\Gamma_2) + (\Gamma_7)) =$$

$$-(\Gamma_3).(\Gamma_2) + (\Gamma_3).(\Gamma_7) = -1 + 1 = 0.$$

Análogamente podemos ver que $\Gamma_7^2 = 1$.

A continuación vamos a ver algunas propiedades que satisface el índice de intersección y que vamos a necesitar. Algunas van a parecer un poco técnicas, pero tal vez más adelante se entienda mejor la idea geométrica.

Proposición 3.3.11. *Sea $\mathcal{S}$ una superficie fibrada no singular con morfismo de proyección $\pi : \mathcal{S} \longrightarrow \mathcal{C}$. Sean $\delta \in \mathcal{D}iv(\mathcal{C})$ y $D \in \mathcal{D}iv(\mathcal{S})$ un divisor fibral. Entonces:*

$$D.\pi^*(\delta) = 0.$$

Demostración: Vamos a demostrarlo en el caso $\mathcal{C} = \mathbb{P}^1$, que es el que nos interesa. El caso general es un poco más delicado y diremos al final cuál es la parte en la que hay que tener un poco más de cuidado.

Por la linealidad de '$.$' y de π^* basta ver el caso $D = (\Gamma)$ y $\delta = (p)$; para $\Gamma \subseteq \mathcal{S}$ una curva irreducible y $p \in \mathbb{P}^1$. Como D es un divisor fibral, Γ es una curva fibral; digamos $\Gamma \subseteq \mathcal{S}_\tau$ para algún $\tau \in \mathbb{P}^1$. Además, por la definición de π^*, tenemos que $\pi^*(p) \subseteq \mathcal{S}_p$. Tenemos entonces dos posibilidades que son: $\tau \neq p$ o $\tau = p$.

Si $\tau \neq p$, entonces es claro que $\Gamma \cap \pi^*(p) = \emptyset$. Por la simple razón de que están incluidos en fibras distintas. Luego: $(\Gamma).\pi^*(p) = 0$.

Supongamos que $\tau = p$. Sin pérdida de generalidad podemos suponer que p es de la forma $p = [t:1]$. Sea $F \in \mathbb{Q}(\mathbb{P}^1)^\times$ la función $F([T:U]) = \frac{T - tU}{U}$. Entonces se tiene:

$$div(F) = (p) - (p_\infty);$$

donde $p_\infty = [1:0]$. Luego:

$$\pi^*(p_\infty) = \pi^*((p) - div(F)) = \pi^*(p) - \pi^*(div(F)).$$

Ahora, usando la definición de π^*, se tiene:

$$\pi^*(div(F)) = \pi^*((p) - (p_\infty)) = \sum_{\Lambda \subseteq \mathcal{S}_p} ord_\Lambda(u_p \circ \pi)\Lambda - \sum_{\Lambda \subseteq \mathcal{S}_{p_\infty}} ord_\Lambda(u_{p_\infty} \circ \pi)\Lambda;$$

donde u_p y u_{p_∞} son uniformizadores locales en p y en p_∞ respectivamente. Pero justamente podemos tomar $u_p = F$ y $u_{p_\infty} = \frac{1}{F}$. De modo que nos queda:

$$\sum_{\Lambda \subseteq \mathcal{S}_p} ord_\Lambda(u_p \circ \pi)\Lambda - \sum_{\Lambda \subseteq \mathcal{S}_{p_\infty}} ord_\Lambda(u_{p_\infty} \circ \pi)\Lambda = \sum_{\Lambda \subseteq \mathcal{S}_p} ord_\Lambda(F \circ \pi)\Lambda - \sum_{\Lambda \subseteq \mathcal{S}_{p_\infty}} ord_\Lambda(\frac{1}{F} \circ \pi)\Lambda =$$

$$\sum_{\Lambda \subseteq \mathcal{S}_p} ord_\Lambda(F \circ \pi)\Lambda + \sum_{\Lambda \subseteq \mathcal{S}_{p_\infty}} ord_\Lambda(F \circ \pi)\Lambda = div(F \circ \pi) \in \mathcal{D}iv(\mathcal{S}).$$

La última igualdad se tiene dado que, claramente, las únicas curvas que pueden aparecer como componentes del divisor de $F \circ \pi$ en $\mathcal{D}iv(\mathcal{S})$ son las contenidas en las fibras $\mathcal{S}_p$ y $\mathcal{S}_{p_\infty}$.

Hemos visto entonces que:

$$\pi^*(p_\infty) = \pi^*(p) - div(F \circ \pi).$$

Pero como $p_\infty \neq \tau$, reduciéndonos al primer caso, tenemos:

$$(\Gamma).\pi^*(p_\infty) = 0.$$

Luego:

$$0 = (\Gamma).\pi^*(p_\infty) = (\Gamma).(\pi^*(p) - div(F \circ \pi)) = (\Gamma).\pi^*(p) - (\Gamma).div(F \circ \pi).$$

Pero, por definición, $div(F \circ \pi)$ es un divisor principal. Es decir $div(F \circ \pi) \sim 0$. Por lo que:

$$(\Gamma).div(F \circ \pi) = (\Gamma).0 = 0;$$

de donde:

$$(\Gamma).\pi^*(p) = 0.$$

En el caso general de cualquier curva $\mathcal{C}$ no singular; hay que tener un poco más de cuidado al elegir la función auxiliar F que hemos considerado; pues no es tan sencillo asegurar la existencia de una tal función que nos permita hacer el razonamiento que hicimos. □

El segundo resultado es el siguiente.

Proposición 3.3.12. *Sea $\mathcal{S}$ una superficie fibrada no singular con morfismo de proyección $\pi : \mathcal{S} \longrightarrow \mathcal{C}$. Sea $D \in \mathcal{D}iv(\mathcal{S})$ un divisor fibral. Entonces:*

a) $D^2 = D.D \leq 0$.

b) $D^2 = 0 \Leftrightarrow D \in \pi^*(\mathcal{D}iv(\mathcal{C}) \otimes \mathbb{Q})$. Es decir, $D^2 = 0$ si, y sólo si, existe un divisor $\delta \in \mathcal{D}iv(\mathcal{C})$ tal que $aD = b\pi^*(\delta)$ para ciertos enteros no nulos a y b.

Demostración: a) Escribamos $D = D_1 + D_2 + \cdots + D_n$; con $D_i \subseteq \mathcal{S}_{p_i}$, para algún $p_i \in \mathcal{C}$. Como $p_i \neq p_j$ si $i \neq j$, es claro que $D_i.D_j = 0$ si $i \neq j$. De modo que tenemos:

$$D^2 = D_1^2 + D_2^2 + \cdots + D_n^2.$$

Por lo tanto basta probar el resultado en el caso $D \subseteq \mathcal{S}_p$.

Digamos que la fibra $\mathcal{S}_p$ es unión de las componentes irreducibles $\Gamma_0, \Gamma_1, ..., \Gamma_r$; y escribamos:

$$D = \sum_{i=0}^{r} a_i(\Gamma_i) \quad y \quad F = \pi^*(p) = \sum_{i=0}^{r} n_i(\Gamma_i); \ \ con\, n_i > 0.$$

Entonces:

$$D^2 = \sum_{i,j=0}^{r} a_i a_j(\Gamma_i).(\Gamma_j).$$

Si $i \neq j$, entonces $(\Gamma_i).(\Gamma_j) \geq 0$. Por lo tanto tenemos:

$$\sum_{i,j=0}^{r} (a_i - a_j)^2(\Gamma_i).(\Gamma_j) = \sum_{i,j=0, i\neq j}^{r} (a_i - a_j)^2(\Gamma_i).(\Gamma_j) \geq 0.$$

Entonces:

$$0 \leq \sum_{i,j=0}^{r} \left(\frac{a_i}{n_i} - \frac{a_j}{n_j}\right)^2 n_i(\Gamma_i).n_j(\Gamma_j) = \sum_{i,j=0}^{r} \frac{a_i^2}{n_i^2} n_i(\Gamma_i).n_j(\Gamma_j) - 2\sum_{i,j=0}^{r} \frac{a_i}{n_i}\frac{a_j}{n_j} n_i(\Gamma_i).n_j(\Gamma_j) +$$

$$\sum_{i,j=0}^{r} \frac{a_j^2}{n_j^2} n_i(\Gamma_i).n_j(\Gamma_j).$$

Pero, por la Proposición 3.3.11:

$$\sum_{i,j=0}^{r} \frac{a_i^2}{n_i^2} n_i(\Gamma_i).n_j(\Gamma_j) = \underbrace{\left(\sum_{i=0}^{r} \frac{a_i^2}{n_i^2} n_i(\Gamma_i)\right)}_{Fibral} . \underbrace{\left(\sum_{j=0}^{r} n_j(\Gamma_j)\right)}_{\pi^*(p)} = 0.$$

Luego:

$$0 \leq -2\sum_{i,j=0}^{r} \frac{a_i}{n_i}\frac{a_j}{n_j} n_i(\Gamma_i).n_j(\Gamma_j) = -2\sum_{i,j=0}^{r} a_i a_j(\Gamma_i).(\Gamma_j) = -2D^2.$$

Por lo tanto:

$$D^2 \leq 0.$$

b) La implicación ($\Leftarrow$) es evidente a partir de la Proposición 3.3.11. Veamos que vale ($\Rightarrow$) :

Por lo que hicimos en a), tenemos que:

$$-2D^2 = \sum_{i,j=0}^{r} \left(\frac{a_i}{n_i} - \frac{a_j}{n_j}\right)^2 n_i(\Gamma_i).n_j(\Gamma_j).$$

Entonces, si $D^2 = 0$, necesariamente $\frac{a_i}{n_i} = \frac{a_j}{n_j}$ para todos $i \neq j$ tales que $(\Gamma_i).(\Gamma_j) > 0$. Es decir, si $\Gamma_i \cap \Gamma_j \neq \emptyset$, entonces $\frac{a_i}{n_i} = \frac{a_j}{n_j}$.

Ahora, es un hecho conocido que las fibras de una superficie fibrada son conexas. Entonces, dadas Γ_i y Γ_j arbitrarias, existen Γ_{l_k} tales que:

$$\Gamma_i = \Gamma_{l_0}, \Gamma_{l_1}, ..., \Gamma_{l_m} = \Gamma_j;$$

con $\Gamma_{l_k} \cap \Gamma_{l_{k+1}} \neq \emptyset$. De modo que:

$$\frac{a_i}{n_i} = \frac{a_{l_0}}{n_{l_0}} = \frac{a_{l_1}}{n_{l_1}} = \cdots = \frac{a_{l_m}}{n_{l_m}} = \frac{a_j}{n_j}.$$

Es decir, $\frac{a_i}{n_i} = \frac{a_j}{n_j} = a \in \mathbb{Q}$, $\forall i, j$.

Luego:

$$D = \sum_{i=0}^{r} a_i(\Gamma_i) = \sum_{i=0}^{r} \frac{a_i}{n_i} n_i(\Gamma_i) = a \sum_{i=0}^{r} n_i(\Gamma_i) = a\pi^*(p) \in \pi^*(\mathcal{D}iv(\mathcal{C}) \otimes \mathbb{Q}).$$

□

Observación 3.3.13. Siguiendo con la notación de la demostración anterior, podemos razonar lo siguiente. Situémonos en la fibra $\mathcal{S}_p$; donde tenemos las componentes irreducibles $\Gamma_0, \Gamma_1, ..., \Gamma_r$. Consideremos la *matriz de incidencia*:

$$I = (\Gamma_i.\Gamma_j)_{0 \leq i,j \leq r}\,.$$

Entonces lo que dice la Proposición 3.3.12 puede ser reinterpretado de la siguiente manera. La forma cuadrática:

$$\begin{array}{rcl} \mathbb{Q}^{r+1} & \longrightarrow & \mathbb{Q} \\ a & \mapsto & a^t I a \end{array}$$

es semi-definida negativa y tiene como núcleo el espacio 1-dimensional generado por el vector $(n_0, ..., n_r)$. En particular, $det(I) = 0$, pero $det(I_{ii}) \neq 0$ $\forall i$; donde I_{ii} es el menor que se obtiene al tachar la i-ésima fila y la i-ésima columna.

La última proposición que necesitamos es la siguiente.

Proposición 3.3.14. *Sea $\mathcal{S}$ una superficie fibrada no singular con morfismo de proyección $\pi : \mathcal{S} \longrightarrow \mathcal{C}$ y sea $D \in \mathcal{D}iv(\mathcal{S})$ tal que:*

$$D.\pi^*(p) = 0 \text{ para todo } p \in \mathcal{C}.$$

Entonces existe un divisor fibral $\Phi_D \in \mathcal{D}iv(\mathcal{S}) \otimes \mathbb{Q}$ tal que:

$$(D + \Phi_D).F = 0 \ \ \forall F \in \mathcal{D}iv(\mathcal{S}) \ divisor\ fibral.$$

Además, si Φ'_D es otro divisor con la misma propiedad, se tiene que:

$$\Phi_D - \Phi'_D \in \pi^*(\mathcal{D}iv(\mathcal{C}) \otimes \mathbb{Q}).$$

Demostración: Dado $p \in \mathcal{C}$, llamemos $\Gamma_{p_0}, \Gamma_{p_1}, ..., \Gamma_{p_{r_p}}$ a las componentes irreducibles de la fibra $\mathcal{S}_p$. Buscamos un divisor Φ de la forma:

$$\Phi_D = \sum a_\Gamma(\Gamma).$$

Dado $p \in \mathcal{C}$ fijo, llamemos $\Phi_{D,p}$ a la componente de Φ en la fibra $\mathcal{S}_p$. Es decir:

$$\Phi_{D,p} = \sum_{i=0}^{r_p} a_{p_i}(\Gamma_{p_i}).$$

Notemos que $r_p = 0$ para casi todo $p \in \mathcal{S}$. Vamos a definir $a_{p_0} = 0$ y para aquellos $p \in \mathcal{C}$ tales que $r_p \geq 1$, planteamos:

$$\sum_{i=1}^{r_p} a_{p_i}(\Gamma_{p_i}).(\Gamma_{p_j}) = -D.(\Gamma_{p_j}) \ \ \forall\, 1 \leq j \leq r_p.$$

Este es un sistema lineal de ecuaciones con r_p ecuaciones y las incógnitas $a_{p_1}, ..., a_{p_{r_p}}$. Matricialmente:

$$\left(\Gamma_{p_i}.\Gamma_{p_j}\right) . \begin{pmatrix} a_{p_1} \\ \vdots \\ a_{p_{r_p}} \end{pmatrix} = -D. \begin{pmatrix} \Gamma_{p_1} \\ \vdots \\ \Gamma_{p_{r_p}} \end{pmatrix}.$$

Por la Observación 3.3.13, la matriz $\left(\Gamma_{p_i}.\Gamma_{p_j}\right)$ tiene determinante no nulo; pues resulta de tachar la primera fila y la primera columna a la matriz de incidencia correspondiente a la fibra $\mathcal{S}_p$. Luego, el sistema tiene una solución $(a_{p_1}, ..., a_{p_{r_p}}) \in \mathbb{Q}^{r_p}$. Definimos entonces:

$$\Phi_D = \sum_{p \in \mathcal{C}} \sum_{i=0}^{r_p} a_{p_i}(\Gamma_{p_i}),$$

y afirmamos que funciona.

En primer lugar, como $r_p = 0$ para casi todo $p \in \mathcal{C}$, y definimos $a_{p_0} = 0$, la suma es finita; por lo que Φ_D está bien definido. Para verificar que Φ_D en efecto funciona, por linealidad, basta ver que:

$$(D + \Phi_D).(\Gamma) = 0,$$

para toda curva fibral irreducible $\Gamma \subseteq \mathcal{S}$. Consideremos tres casos:

1) Si $r_p = 0$, entonces $\Gamma = \Gamma_{p_0} = \pi^*(p)$. Entonces, usando la Proposición 3.3.11 y la hipótesis que tenemos, resulta:

$$(D + \Phi_D).(\Gamma) = D.\pi^*(p) + \Phi_D.\pi^*(p) = 0.$$

2) Si $r_p \geq 1$ y $\Gamma = \Gamma_{p_j}$ para $j \geq 1$, entonces por cómo elegimos los a_{p_i} tenemos efectivamente que:

$$(D + \Phi_D).(\Gamma) = D.(\Gamma_{p_j}) + \sum_{p \in \mathcal{C}} \sum_{i=0}^{r_p} a_{p_i}(\Gamma_{p_i}).(\Gamma_{p_j}) = 0.$$

3) Supongamos por último que $r_p \geq 1$ y $\Gamma = \Gamma_{p_0}$. Digamos $\pi^*(p) = \sum_{i=0}^{r_p} n_i.(\Gamma_{p_i})$. Entonces, volviendo a usar la Proposición 3.3.11 y el caso 2) se tiene:

$$0 = (D + \Phi_D).\pi^*(p) = \sum_{i=0}^{r_p} n_i(D + \Phi_D).(\Gamma_{p_i}) = n_0(D + \Phi_D).(\Gamma_{p_0}) = n_0(D + \Phi_D).(\Gamma).$$

De donde:

$$(D + \Phi_D).(\Gamma) = 0.$$

Luego, en cualquiera de los casos, el divisor Φ_D que construimos funciona.

Veamos la unicidad. Si Φ'_D es otro divisor con la misma propiedad y tomamos cualquier divisor fibral F tenemos:

$$(\Phi_D - \Phi'_D).F = (D + \Phi_D).F - (D + \Phi'_D).F = 0.$$

En particular, tomando $F = (\Phi_D - \Phi'_D)$, que es fibral, obtenemos:

$$(\Phi_D - \Phi'_D)^2 = 0.$$

Luego, por la Proposición 3.3.12, $\Phi_D - \Phi'_D \in \pi^*(\mathcal{D}iv(\mathcal{C}) \otimes \mathbb{Q})$. □

Dimos las Proposiciones 3.3.11, 3.3.12 y 3.3.14 en el caso general de cualquier superficie fibrada, aunque, como siempre, sólo vamos a trabajar el caso $\mathcal{C} = \mathbb{P}^1$.

Antes de seguir veamos con algunos ejemplos cómo se aplican estos resultados. La Proposición 3.3.11 puede ser muy útil a la hora de querer calcular el índice de intersección de una curva fibral consigo misma. Ya habíamos visto un método para ello, que requería usar de manera auxiliar un divisor principal. Otra manera es la siguiente. Supongamos que queremos calcular Γ_5^2, donde $\Gamma_5 \subseteq \mathcal{S}$ es la curva que trabajamos antes con el ejemplo de siempre. Esto es:

$$\Gamma_5 \,:\, \{([0 : Y : Z]\,; [1 : 0])\}\,.$$

La Proposición 3.3.11 nos dice que $(\Gamma_5).\pi^*(\delta) = 0$ para cualquier divisor $\delta \in \mathcal{D}iv(\mathbb{P}^1)$. Tomemos simplemente:

$$\delta = (p_\infty) = ([1 : 0]).$$

Recordemos que ya calculamos $\pi^*(p_\infty)$. Nos dio:

$$\pi^\star(p_\infty) = (\Gamma_5) + (\Gamma_6).$$

Podemos entonces razonar del siguiente modo:

$$0 = (\Gamma_5).\pi^*(p_\infty) = (\Gamma_5).((\Gamma_5) + (\Gamma_6)) = \Gamma_5^2 + (\Gamma_5).(\Gamma_6) = \Gamma_5^2 + 1.$$

En efecto, Γ_5 y Γ_6 son dos rectas que se cortan en un punto, y obviamente lo hacen de manera transversal, por ser rectas. De modo que $(\Gamma_5).(\Gamma_6) = 1$. En conclusión nos quedó que:

$$\Gamma_5^2 = -1.$$

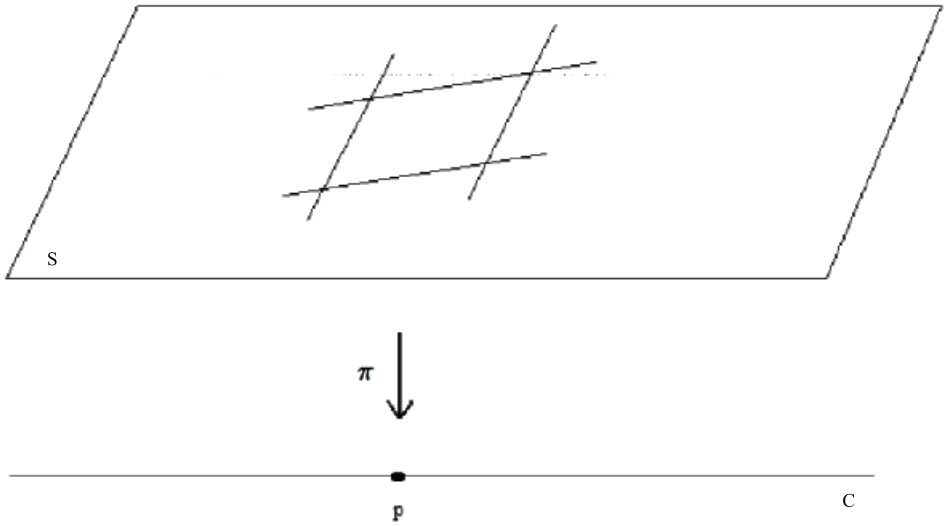


Figura 3.4: Fibra de $\mathcal{S}$ en p.

De un modo simétrico podemos concluir que $\Gamma_6^2 = -1$.

Veamos ahora con un ejemplo la construcción que se hace en la Proposición 3.3.12. Consideremos nuestra superficie de siempre y calculemos la matriz de incidencia I de la Observación 3.3.13 en una fibra particular. De las fibras que ya analizamos, la que resultará más interesante para el caso es $\mathcal{S}_{p_\infty}$, pues en ella encontramos más de una componente irreducible. Con todos los cálculos que ya hicimos podemos construir nuestra matriz I:

$$I = \begin{pmatrix} \Gamma_5^2 & \Gamma_5.\Gamma_6 \\ \Gamma_6.\Gamma_5 & \Gamma_6^2 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Y como vemos, efectivamente se tiene que $det(I) = 0$ y que $I_{ii} \neq 0$, $i = 0, 1$.

Por último, vamos a mostrar con un ejemplo la construcción del divisor Φ_D de la Proposición 3.3.14. Vamos a considerar para esto otro ejemplo para que resulte más interesante. Supongamos que tenemos una superficie fibrada $\mathcal{S}$ y una fibra $\mathcal{S}_p$ tal que consta de 4 componentes irreducibles $\Gamma_0, \Gamma_1, \Gamma_2$ y Γ_3 que se cortan transversalmente con la forma de un cuadrilátero, como muestra la Figura 3.4.

Tendremos en este caso que:

$$\pi^*(p) = (\Gamma_0) + (\Gamma_1) + (\Gamma_2) + (\Gamma_3),$$

y

$$\Gamma_i.\Gamma_j = \begin{cases} 1 & \text{si } \Gamma_i \cap \Gamma_j \neq \emptyset \\ 0 & \text{si } \Gamma_i \cap \Gamma_j = \emptyset \end{cases}$$

Para calcular Γ_i^2 podemos usar, como hicimos antes, la Proposición 3.3.11; así, por ejemplo:

$$0 = (\Gamma_0).\pi^*(p) = (\Gamma_0).((\Gamma_0) + (\Gamma_1) + (\Gamma_2) + (\Gamma_3)) = \Gamma_0^2 + 1 + 0 + 1;$$

por lo tanto, $\Gamma_0^2 = -2$. Simétricamente obtenemos $\Gamma_i^2 = -2$ para $i = 1, 2, 3$.

Nos queda entonces que la matriz de incidencia es:

$$I = (\Gamma_i.\Gamma_j)_{0\leq i,j\leq 3} = \begin{pmatrix} -2 & 1 & 0 & 1 \\ 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \\ 1 & 0 & 1 & -2 \end{pmatrix}.$$

Supongamos ahora que tenemos un divisor $D \in \mathcal{D}iv(\mathcal{S})$ tal que $D.\pi^*(p) = 0$. Por ejemplo, que D satisfaga que:

$$D.\Gamma_0 = -1,\ D.\Gamma_1 = 1,\ D.\Gamma_2 = D.\Gamma_3 = 0.$$

Geométricamente, podemos imaginar que D es de la forma $D = (\Lambda_1) - (\Lambda_0)$; donde Λ_0 y Λ_1 son secciones de $\mathcal{S}$ que cortan respectivamente a Γ_0 y a Γ_1 en un punto de manera transversal. Calculemos la componente de Φ_D correspondiente a la fibra $\mathcal{S}_p$. Notemos a esa componente $\Phi_{D,p}$. Planteamos entonces:

$$\Phi_{D,p} = a_1(\Gamma_1) + a_2(\Gamma_2) + a_3(\Gamma_3);$$

y queremos que:

$$(D + \Phi_{D,p}).\Gamma_i = 0,\ \ i = 1, 2, 3.$$

Resolviendo este sistema lineal obtenemos que $a_1 = \frac{3}{4}$, $a_2 = \frac{1}{2}$ y $a_3 = \frac{1}{4}$. Proponemos entonces:

$$\Phi_{D,p} = \frac{3}{4}(\Gamma_1) + \frac{1}{2}(\Gamma_2) + \frac{1}{4}(\Gamma_3).$$

Se verifica fácilmente que, en efecto, $(D+\Phi_{D,p}).\Gamma_i = 0$ para $i = 0, 1, 2, 3$; por lo que la componente $\Phi_{D,p}$ de Φ_D que encontramos sirve. No es difícil generalizar esto al caso en el que se tiene un n-ágono en vez de un cuadrilátero.

Hasta aquí las propiedades más importantes que queríamos presentar de las superficies fibradas en general. Las próximas construcciones van a ser específicas para superficies elípticas. Pero hagamos la siguiente observación. Recordemos el ejemplo de superficie elíptica con el que hemos trabajado; aquella de ecuación afín:

$$\mathcal{E} : y^2 = x^3 - t^2x + t^2.$$

Uno podría estar tentado a tomar este nuevo ejemplo e intentar encontrar curvas irreducibles, divisores, calcular índices de intersección, etc. Si embargo hay un problema que no podemos dejar pasar por alto y es que esta superficie **es singular**. Efectivamente el punto $(x, y, t) = (0, 0, 0)$ es un punto singular; pues basta con observar que, si llamamos $f(x, y, z) = y^2 - x^3 + t^2x - t^2$,

tenemos:

$$\begin{cases} \dfrac{\partial f}{\partial x}(x,y,t) = & -3x^2 + t^2 \\ \dfrac{\partial f}{\partial y}(x,y,t) = & 2y \\ \dfrac{\partial f}{\partial t}(x,y,t) = & 2tx - 2t \end{cases}$$

Por lo que:

$$\frac{\partial f}{\partial x}(0,0,0) = \frac{\partial f}{\partial y}(0,0,0) = \frac{\partial f}{\partial t}(0,0,0) = 0.$$

Uno puede desanimarse y decir que con esta superficie no podemos hacer nada y buscar un ejemplo *mejor*. Sin embargo sí hay algo que podemos hacer. Hay un procedimiento muy conocido para *resolver singularidades* que consiste en conseguir una superficie no singular que sea birracionalmente equivalente a la que teníamos. Este método lo mostramos a grandes rasgos a continuación.

3.3.3. Blowing Up

Hemos visto que si uno tiene un morfismo birracional entre dos curvas proyectivas no singulares, automáticamente resulta ser un isomorfismo. Esto deja de ser cierto cuando las dimensiones de las variedades son mayores. Un típico ejemplo de esto es el morfismo birracional conocido como *Blow Up*. Este morfismo aparece cuando uno tiene una variedad que es singular y pretende obtener otra que no lo sea, y sea birracionalmente equivalente a la primera.

Notemos que, claramente, el Blow Up no va a ser un isomorfismo; pues una de las superficies es singular y la otra no; pero el hecho que sea un morfismo birracional va a bastarnos para los objetivos que perseguimos.

Empezaremos mostrando cómo se construye el Blow Up en un punto con un ejemplo. Supongamos que estamos en el plano proyectivo $\mathbb{P}^2$. Vamos a construir una variedad que sea birracionalmente equivalente a $\mathbb{P}^2$ de la siguiente manera. Consideremos el producto $\mathbb{P}^2 \times \mathbb{P}^1$, y la variedad $V \subseteq \mathbb{P}^2 \times \mathbb{P}^1$ definida por:

$$V = \left\{ ([X_0 : X_1 : X_2] ; [Y_0 : Y_1]) \in \mathbb{P}^2 \times \mathbb{P}^1 \ : \ X_0 Y_1 = X_1 Y_0 \right\}.$$

Definimos el morfismo $\Pi : V \longrightarrow \mathbb{P}^2$ simplemente como la proyección a la primera coordenada. A ese morfismo Π lo llamamos el Blow Up de $\mathbb{P}^2$ centrado en el punto $\xi = [0 : 0 : 1]$.

Miremos el comportamiento de esta construcción. En primer lugar, si tomamos $[X_0 : X_1 : X_2] \neq \xi$, y miramos la ecuación $X_0 Y_1 = X_1 Y_0$; es fácil ver que esto implica necesariamente que $[Y_0 : Y_1] = [X_0 : X_1]$; de manera que el morfismo $\Pi^{-1} : \mathbb{P}^2 - \{\xi\} \longrightarrow V$ definido por:

$$\Pi^{-1}([X_0 : X_1 : X_2]) = ([X_0 : X_1 : X_2] ; [X_0 : X_1]),$$

satisface efectivamente que $\Pi \circ \Pi^{-1} = id_{\mathbb{P}^2 - \{\xi\}}$.

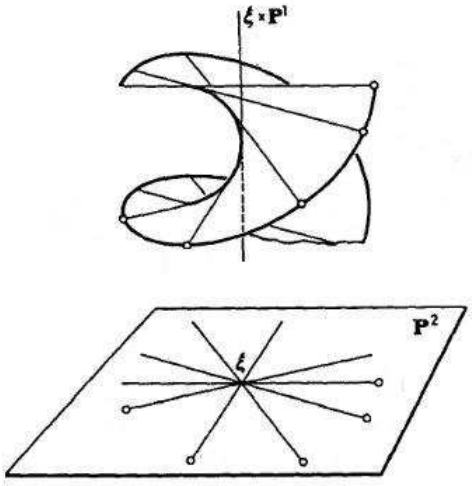


Figura 3.5: Blow Up del plano proyectivo en el origen.

Analicemos ahora qué pasa con el punto ξ. Resulta que si miramos la ecuación que define a V, si $[X_0 : X_1 : X_2] = \xi$; ésta se satisface para cualquier punto $[Y_0 : Y_1] \in \mathbb{P}^1$. De modo que, si queremos extender la definición de Π^{-1} al punto ξ, tendríamos un problema, pues:

$$\Pi^{-1}(\{\xi\}) = \{\xi\} \times \mathbb{P}^1.$$

Pero esto no nos preocupa demasiado. Lo que queremos destacar es que el morfismo Π tiene una vuelta si lo restringimos al abierto $V - (\{\xi\} \times \mathbb{P}^1)$. Es decir:

$$\Pi|_{V-(\{\xi\}\times\mathbb{P}^1)} : V - (\{\xi\} \times \mathbb{P}^1) \longrightarrow \mathbb{P}^2 - \{\xi\},$$

es un **isomorfismo**. Y si extendemos Π^{-1} a ξ de algún modo, resulta que $\Pi^{-1} : \mathbb{P}^2 \longrightarrow V$ es una función racional que satisface:

$$\Pi \circ \Pi^{-1} = id_{\mathbb{P}^2}.$$

Esto nos dice que Π es un morfismo birracional de V en $\mathbb{P}^2$; pues es un morfismo y tiene una vuelta Π^{-1} que es una función racional. Pero **no es un isomorfismo**; pues Π^{-1} no puede extenderse a $\mathbb{P}^2$ de manera que resulte un morfismo. Precisamente, fuera del punto ξ hay una relación de uno a uno entre los puntos de $\mathbb{P}^2$ y los de V; sólo en ξ no se da esa correspondencia, sino que sobre ξ hay toda una recta que se proyecta.

La idea de la construcción se aclara mucho cuando uno mira un gráfico representativo. (Ver Figura 3.5).

Veamos ahora cómo se aplica esto para, dada una variedad singular, conseguir otra no singular y que sea birracionalmente equivalente. Consideremos la curva singular $\mathcal{C}$ contenida en $\mathbb{P}^2$ dada por la ecuación:

$$\mathcal{C} : Y^2Z = X^3 + X^2Z.$$

Habíamos visto que $\mathcal{C}$ es singular en el punto $P = [0 : 0 : 1]$; que, afinizando en Z, es el punto $P = (0, 0)$. Lo que vamos a hacer es mirar el efecto que le produce el Blow Up en P que ya

construimos a la curva $\mathcal{C}$. Es decir, vamos a mirar la variedad $W \subseteq V$ que es la preimagen de $\mathcal{C}$ por el morfismo de proyección Π. O sea, $W = \Pi^{-1}(\mathcal{C})$. Para que la notación sea compatible, a los puntos de V vamos a llamarlos $([X : Y : Z] ; [T : U])$. Tenemos que W está dada por:

$$W : \begin{cases} Y^2Z - X^3 - X^2Z & = 0 \\ XU - YT & = 0 \end{cases}$$

Trabajemos en el espacio afín $Z = T = 1$ para que se entienda la idea geométrica. Aquí, la variedad W está dada por:

$$W : \begin{cases} y^2 - x^3 - x^2 & = 0 \\ xu - y & = 0 \end{cases}$$

No es difícil ver que el ideal de $\overline{\mathbb{Q}}[x, y, u]$ asociado a W es exactamente $I(W) = (y^2 - x^3 - x^2, xu - y)$. Pero resulta que $I(W)$ no es un ideal primo. Más precisamente, con un poco de trabajo, podemos ver que hay dos ideales primos que lo contienen, que son:

$$\wp_1 = (x, y) \;\; y \;\; \wp_2 = (x - (u^2 - 1), y - u(u^2 - 1));$$

que se corresponden con las dos variedades irreducibles que son las componentes de W.

Si pensamos esto desde el punto de vista geométrico tiene mucho sentido. Miremos la curva $\mathcal{C}$ en el plano $\mathbb{P}^2$ y pensemos cómo es su preimagen W. Si tomamos un punto de $\mathcal{C}$ distinto de $p = (0, 0)$; la relación es uno a uno. Consideremos el conjunto contenido en V que se obtiene al tomar la preimagen de $\mathcal{C} - \{(0, 0)\}$. Para que ese conjunto sea una variedad, hay que tomar su clausura (su clausura topológica con la topología Zariski). Así obtenemos una curva. Por otro lado, la preimagen de $p = (0, 0)$ es toda una recta. Resulta precisamente que esa curva y esa recta que se obtienen al tomar la preimagen de toda la curva $\mathcal{C}$ son las dos componentes de W que se corresponden con $\wp_2$ y $\wp_1$ respectivamente.

¿Cuál será la variedad no singular que estamos buscando que sea birracionalmente equivalente a $\mathcal{C}$? Claramente la respuesta va a ser esa curva asociada al ideal primo $\wp_2$. A esa curva la llamamos $\mathcal{C}'$ y efectivamente es birracionalmente equivalente a $\mathcal{C}$. La razón de esto es que el morfismo de proyección Π restringido a $\mathcal{C}'$ es un morfismo que tiene una función racional inversa. Precisamente, la curva $\mathcal{C}$ se *levanta* a $\mathcal{C}'$ de manera biyectiva en todos los puntos salvo en el $(0, 0)$; en donde se levanta a dos puntos distintos: $(0, 0, 1)$ y $(0, 0, -1)$.

Insistamos con la idea geométrica que es la que ilumina todo este razonamiento. La curva $\mathcal{C}$, originalmente, pasaba dos veces por $(0, 0)$. Esto es lo que provoca que ese punto sea singular. Cuando hacemos el Blow Up, lo que hacemos es levantar esa curva y mirarla ahora en el espacio; y conseguimos así que esas dos veces en las que $\mathcal{C}$ pasaba por $(0, 0)$ se conviertan en dos puntos distintos. Logramos *separar* esos dos puntos que coincidían. Ahora obtenemos una curva en un espacio de dimensión mayor que, salvo en dos de sus puntos, al proyectarla sobre $\mathbb{P}^2$, hay una correspondencia biunívoca con los puntos de $\mathcal{C}$. No sólo correspondencia biunívoca, sino que, más fuerte aún, isomorfismo. En consecuencia las dos curvas son birracionalmente equivalentes.

Otra forma de verlo es decir que a la curva $\mathcal{C}$ le agregamos una coordenada extra que es la *pendiente*. De modo que, como antes pasaba dos veces por el punto P; ahora eso no ocurre, ya que cada vez que pasa por P lo hace con una pendiente diferente. (Ver Figura 3.6).

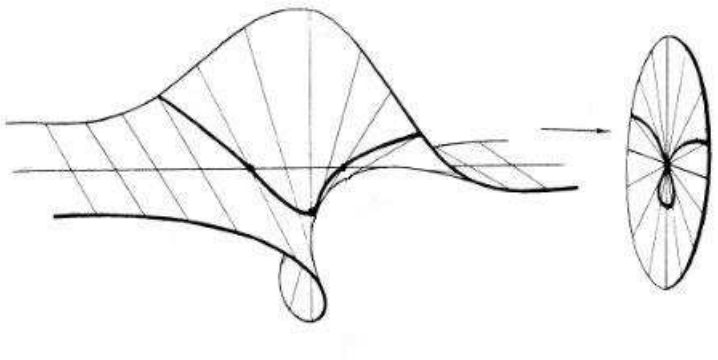


Figura 3.6: Efecto del Blow Up en la curva $\mathcal{C}$.

Volvamos a coordenadas homogéneas para ver cómo queda la curva $\mathcal{C}'$ que construimos:

$$x - (u^2 - 1) = \frac{X}{Z} - \left(\frac{U^2}{T^2} - 1\right).$$

Limpiando denominadores queda:

$$XT^2 - Z(U^2 - T^2).$$

Análogamente,

$$y - u(u^2 - 1) = \frac{Y}{Z} - \frac{U}{T}\left(\frac{U^2}{T^2} - 1\right).$$

Y limpiando denominadores queda:

$$YT^3 - ZU(U^2 - T^2).$$

O sea, nos queda:

$$\mathcal{C}' : \begin{cases} XT^2 - Z(U^2 - T^2) & = 0 \\ YT^3 - ZU(U^2 - T^2) & = 0 \end{cases}$$

Sólo falta verificar que $\mathcal{C}'$ es no singular; lo cual es creíble a partir del dibujo. Pero también es claro si hacemos la cuenta explícita. Habría que verificar que $\mathcal{C}'$ es no singular en todas las afinizaciones posibles. Hagamos sólo una ya que las demás son análogas. Vale la pena hacer al menos una para que veamos cómo es que logramos que esa singularidad que teníamos ha sido salvada en $\mathcal{C}'$. Tomemos la parte afín que trabajamos antes: $Z = T = 1$. Aquí tenemos:

$$\mathcal{C}' : \begin{cases} f_1(x, y, u) = x - (u^2 - 1) & = 0 \\ f_2(x, y, u) = y - u(u^2 - 1) & = 0 \end{cases}$$

Veamos cómo queda la matriz de las derivadas parciales de f_1 y f_2 :

$$\begin{pmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} & \frac{\partial f_1}{\partial u} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} & \frac{\partial f_2}{\partial u} \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2u \\ 0 & 1 & -3u^2 + 1 \end{pmatrix}.$$

Sólo hay que verificar que esta matriz tiene rango 2 en cualquier punto (x, y, u); pero esto es inmediato, ya que claramente las filas son linealmente independientes. En general, si nos quedan f_1 y f_2 lineales en x y en y respectivamente, la no singularidad está asegurada.

Esto que hicimos fue sólo un caso particular de Blow Up. Por supuesto que lo mismo puede hacerse si tomamos como centro otro punto de $\mathbb{P}^2$; con una simple traslación. También podemos trabajar en un espacio de dimensión mayor. Aquí una de las generalizaciones:

Definición 3.3.15. Dados los espacios proyectivos $\mathbb{P}^n$ y $\mathbb{P}^{n-1}$, sea $V \subseteq \mathbb{P}^n \times \mathbb{P}^{n-1}$ la variedad dada por:

$$V = \left\{ ([X_0 : \cdots : X_n] ; [Y_0 : \cdots : Y_{n-1}]) \in \mathbb{P}^n \times \mathbb{P}^{n-1} \, : \, X_i Y_j = X_j Y_i \, : \, i, j = 0, 1, ..., n-1 \right\}.$$

Al morfismo $\Pi \, : \, V \longrightarrow \mathbb{P}^n$, que es la proyección a la primera coordenada, lo llamamos el *Blow Up* de $\mathbb{P}^n$ centrado en el punto $\xi = [0 : \cdots : 0 : 1] \in \mathbb{P}^n$.

El resultado que se obtiene al generalizar lo que hicimos es el siguiente.

Proposición 3.3.16. *Con las notaciones de la Definición 3.3.15,* Π *es un morfismo birracional entre las variedades* V *y* $\mathbb{P}^n$.

Como vimos, la técnica del Blow Up nos permite pensar que, dada una curva cualquiera $\mathcal{C}$, siempre podemos conseguir una curva no singular $\mathcal{C}'$ tal que sea birracionalmente equivalente a $\mathcal{C}$. No es difícil convencerse de esto. Pues supongamos que $\mathcal{C}$ tiene más de una singularidad. Como la cantidad será siempre finita, repitiendo el proceso esas finitas veces uno siempre puede conseguirse la curva $\mathcal{C}'$. Más aún, resulta que la curva $\mathcal{C}'$ es única salvo isomorfismos. La unicidad es clara a partir de lo siguiente. Si tenemos dos curvas $\mathcal{C}'$ y $\mathcal{C}''$ no singulares y birracionalmente equivalentes a $\mathcal{C}$; en particular serán birracionalmente equivalentes entre sí. Pero como son no singulares, necesariamente son isomorfas. En definitiva, lo que es cierto es que:

Dada una curva cualquiera $\mathcal{C}$, *existe una curva* $\mathcal{C}'$ *no singular tal que es birracionalmente equivalente a* $\mathcal{C}$; *y* $\mathcal{C}'$ *resulta ser única salvo isomorfismos.*

El Blow Up también pude aplicarse para resolver singularidades de superficies y esto nos lleva a definir nuevas nociones que veremos a continuación.

3.3.4. Minimalidad de Superficies

Como dijimos, dada una curva $\mathcal{C}$, existe siempre una "única" curva $\mathcal{C}'$ no singular y birracionalmente equivalente a $\mathcal{C}$. Cuando uno trabaja con superficies la cosa no es muy distinta; pero hay que tener un poco más de cuidado. Es cierto que, dada una superficie $\mathcal{S}$, con la técnica del Blow Up, uno puede conseguirse una superficie $\mathcal{S}'$ no singular y birracionalmente equivalente a $\mathcal{S}$; y, por cierto, esto no es para nada trivial de demostrar. Sin embargo la unicidad ya no es cierta. La razón es que uno podría continuar haciendo el método Blow Up aunque la superficie $\mathcal{S}'$ ya

sea no singular, y obtener una superficie $\mathcal{S}''$ que también será no singular y birracionalmente equivalente a $\mathcal{S}$, pero **no isomorfa**. Intuitivamente, queremos decir que la unicidad la tenemos si no hicimos ningún Blow Up de más. Es decir, queremos aplicarle la técnica del Blow Up a la superficie $\mathcal{S}$ tantas veces como sea necesario para resolver sus singularidades; pero no excedernos.

¿Por qué uno puede excederse en superficies y no en curvas? Es decir, ¿por qué al hacer Blow Up de más en curvas no es problema porque ya quedan todas isomorfas, mientras que en superficies no ocurre eso? No vamos a dar un argumento general, pero sí podemos seguir aprovechando el ejemplo que hicimos. Cuando le hicimos el Blow Up a $\mathbb{P}^2$ en $\xi = [0:0:1]$, vimos que la curva $\mathcal{C}$ se levantaba a una variedad que tenía dos componentes. Sólo una de ellas es la que nos interesaba y a la que llamamos $\mathcal{C}'$. La otra era toda la recta que estaba sobre ξ. Pero supongamos que queremos ver en qué se transforma toda la superficie $\mathbb{P}^2$. La variedad a la que se levanta $\mathbb{P}^2$ es justamente la variedad de $\mathbb{P}^2 \times \mathbb{P}^1$ que llamamos V, que puede verse que es irreducible. Y como vimos, V es birracionalmente equivalente a $\mathbb{P}^2$ pero no son isomorfas. Podríamos decir que el Blow Up que le hicimos a $\mathbb{P}^2$ estuvo de más; pues $\mathbb{P}^2$ ya es una superficie no singular. Tal vez con este ejemplo sencillo se visualice que lo que ocurre en curvas no es lo mismo que lo que ocurre en superficies.

Sin embargo podemos tener una noción de unicidad para las superficies si pedimos, justamente, que no se hayan aplicado Blow Up innecesarios. Es así como surge una noción de minimalidad para superficies que es la siguiente.

Definición 3.3.17. Una superficie $\mathcal{S}$ se dice *relativamente minimal* si satisface las siguientes propiedades:

a) $\mathcal{S}$ es una superficie no singular

b) Si $\mathcal{S}'$ es otra superficie no singular y $\phi : \mathcal{S} \longrightarrow \mathcal{S}'$ es un morfismo birracional, entonces ϕ es un isomorfismo.

La definición es para una superficie cualquiera, no necesariamente fibrada.

La noción intuitiva de superficie relativamente minimal es justamente lo que decíamos antes. En el ejemplo que tenemos ocurre que la superficie $\mathbb{P}^2$ es en efecto relativamente minimal. Esto es cierto y una forma de verlo es que no se puede proyectar $\mathbb{P}^2$ en la dirección de una recta contenida en él de manera que la proyección resulte ser un morfismo birracional. Podemos verificar sin embargo que la variedad V no es relativamente minimal. Pues se tiene el morfismo birracional $\Pi : V \longrightarrow \mathbb{P}^2$ que no es un isomorfismo. Justamente V no es relativamente minimal ya que se obtuvo al aplicarle un Blow Up a una superficie que ya era no singular.

La pregunta natural que uno se hace es si dada cualquier superficie $\mathcal{S}$ siempre podemos encontrar una superficie $\mathcal{S}'$ que sea birracionalmente equivalente a $\mathcal{S}$ y que sea relativamente minimal. Esto es efectivamente cierto. El resultado, muy fuerte por cierto, es el siguiente:

Teorema 3.3.18. *Toda superficie $\mathcal{S}_0$ es birracionalmente equivalente a una superficie $\mathcal{S}$ relativamente minimal. Si $\mathcal{S}_0$ es no singular, entonces existe un morfismo birracional $\phi : \mathcal{S}_0 \longrightarrow \mathcal{S}$.*

Demostración: Ver [10], Capítulo III, Teorema 7.7. □

3.4. Geometría de las Superficies Elípticas

Hay una noción de minimalidad para superficies fibradas que vamos a ver en esta parte. Si bien es un concepto aplicable a cualquier superficie fibrada, cuando la superficie es elíptica se pueden decir más cosas; de manera que vamos a trabajar directamente con superficies elípticas.

En esta sección volveremos entonces sobre las superficies elípticas y veremos que varios de los conceptos que vimos para superficies fibradas en general adquieren más riqueza aún. Veremos propiedades geométricas de las superficies elípticas haciendo uso de la estructura algebraica que ya vimos que tienen.

Hasta ahora, lo que hicimos con las superficies elípticas $\mathcal{E}$ fue ver que están en correspondencia con las curvas elípticas E definidas sobre $\overline{\mathbb{Q}(t)}$; y vimos la relación que hay entre los puntos de E y las secciones de $\mathcal{E}$. Todo lo que vino después fue mostrar propiedades geométricas de las superficies fibradas en general que, obviamente, también se aplican a las superficies elípticas. El problema de esa parte es que, para definir todas esas nociones, se requiere que la superficie fibrada sea no singular. Supongamos que queremos mostrar un ejemplo de superficie elíptica no singular dada por una ecuación de la forma:

$$\mathcal{E} \,:\, Y^2Z = X^3 + AX^2Z + BXZ^2 + CZ^3;$$

donde $A, B, C \in \mathbb{Q}(\mathbb{P}^1)$. Por ahora, el único ejemplo que vimos no servía porque era singular. Pero no es que hayamos hecho una mala elección. Ocurre que, lamentablemente, nunca vamos a conseguirnos tal ejemplo por la forma que tiene la ecuación. Siempre algún punto singular va a aparecer. Pero esto no va a ser una traba definitiva. Usando la técnica del Blow Up que presentamos antes vamos a poder resolver las singularidades y obtener así el ejemplo deseado. Va a surgir aquí la noción de minimalidad para superficies elípticas, que es la que presentamos a continuación.

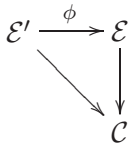
3.4.1. Modelo Minimal

La idea de la minimalidad va a ser muy similar a la que ya vimos, sólo que ahora hay que tener en consideración al morfismo de proyección que trae consigo la superficie elíptica. Concretamente, dada una superficie elíptica $\mathcal{E}$ con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathcal{C}$; nos van a interesar las superficies elípticas $\mathcal{E}'$ con morfismo de proyección $\pi' : \mathcal{E}' \longrightarrow \mathcal{C}$; y las funciones racionales entre ambas que vamos a considerar serán aquellas que conmuten con las proyecciones π y π'.

Definición 3.4.1. Una superficie elíptica $\mathcal{E}$ con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathcal{C}$ se llama una *superficie elíptica minimal* si satisface las siguientes propiedades:

a) $\mathcal{E}$ es una superficie no singular.

b) Sea $\mathcal{E}'$ una superficie elíptica no singular con morfismo de proyección $\pi' : \mathcal{E}' \longrightarrow \mathcal{C}$; y sea $\phi : \mathcal{E}' \longrightarrow \mathcal{E}$ una función birracional tal que $\pi' = \pi \circ \phi$. Entonces ϕ se extiende a un morfismo (por lo tanto, morfismo birracional).



Notar la diferencia con el concepto anterior de superficie relativamente minimal. Antes, si uno tenía un **morfismo birracional** $\phi : \mathcal{S} \longrightarrow \mathcal{S}'$, resultaba que tenía que ser un **isomorfismo**. Ahora, si uno tiene una **función birracional** $\phi : \mathcal{E}' \longrightarrow \mathcal{E}$, resulta que tiene que ser un **morfismo birracional**.

De vuelta, la pregunta natural que surge es si cualquier superficie elíptica será birracionalmente equivalente a una superficie elíptica minimal. El siguiente teorema nos asegura esto para superficies elípticas no singulares:

Teorema 3.4.2. *Sea $\mathcal{E}$ una superficie elíptica no singular con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathcal{C}$. Entonces existe una superficie elíptica minimal $\mathcal{E}^{min}$ con morfismo de proyección $\pi^{min} : \mathcal{E}^{min} \longrightarrow \mathcal{C}$, y un morfismo birracional $\phi : \mathcal{E} \longrightarrow \mathcal{E}^{min}$ tal que $\pi = \pi^{min} \circ \phi$.*

Demostración: Ver [10], Capítulo III, Teorema 8.4. □

Observación 3.4.3. Uno se pregunta qué pasará entonces con las superficies elípticas que son singulares. Pero con todo lo que ya tenemos podemos ocuparnos de ellas también. Supongamos que $\mathcal{E}$ es una superficie elíptica cualquiera con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathcal{C}$. Por el Teorema 3.3.18, mirando a $\mathcal{E}$ como una superficie cualquiera (no fibrada) sabemos que existe una superficie relativamente minimal $\mathcal{E}'$ que es birracionalmente equivalente a $\mathcal{E}$. Más aún, tenemos un morfismo birracional $\phi : \mathcal{E}' \longrightarrow \mathcal{E}$. Pero entonces resulta que, si consideramos el morfismo $\pi \circ \phi : \mathcal{E}' \longrightarrow \mathcal{C}$; se tiene que $\mathcal{E}'$ también es una superficie elíptica sobre $\mathcal{C}$. Es cierto que casi todas las fibras van a ser curvas elípticas porque ϕ es un isomorfismo en un abierto de $\mathcal{E}'$. Podemos entonces aplicarle el Teorema 3.4.2 a $\mathcal{E}'$ y tenemos que $\mathcal{E}'$ es birracionalmente equivalente a una superficie elíptica minimal $\mathcal{E}^{min}$. Transitivamente resulta que $\mathcal{E}$ es birracionalmente equivalente a $\mathcal{E}^{min}$.

Esto nos permite concluir que:

Cualquier superficie elíptica, singular o no, es birracionalmente equivalente a una superficie elíptica minimal.

A partir de todos estos resultados tenemos un corolario bastante inmediato pero que nos va a ser de mucha utilidad.

Proposición 3.4.4. *Sea $\mathcal{E}$ una superficie elíptica minimal con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathcal{C}$; y sea $\tau : \mathcal{E} \longrightarrow \mathcal{E}$ una función birracional tal que $\pi \circ \tau = \pi$. Entonces τ es un morfismo.*

Demostración: Basta con tomar $\mathcal{E}' = \mathcal{E}$ y $\phi = \tau$ en la Definición 3.4.1. □

Lo que vamos a hacer ahora es tratar de conseguir explícitamente un ejemplo de superficie elíptica minimal. Recordemos el ejemplo que venimos trabajando, la curva E sobre $k = \mathbb{Q}(t)$ dada por la ecuación afín:

$$E \,:\, y^2 = x^3 - t^2x + t^2.$$

Habíamos visto que la superficie elíptica asociada $\mathcal{E}$ era singular, por ejemplo en el punto de coordenadas afines $(x, y, t) = (0, 0, 0)$. Pero podemos ver que, en realidad, hay muchas otras singularidades. Si consideramos la ecuación homogénea:

$$\mathcal{E} \,:\, Y^2ZU^2 = X^3U^2 - T^2XZ^2 + T^2Z^3,$$

y afinizamos en $Y = T = 1$, nos queda:

$$\mathcal{E} \,:\, zu^2 = x^3u^2 - xz^2 + z^3.$$

Es fácil verificar que las tres derivadas parciales en esta afinización se anulan sobre toda la recta dada por $z = u = 0$. Esto es, hay toda una recta de puntos singulares sobre $\mathcal{E}$; lo cual hace sospechar que el proceso para resolver todas las singularidades de $\mathcal{E}$ no va a ser sencillo. Sin embargo, podemos hacer un recurso que va a facilitarnos mucho las cuentas. Intuitivamente, la razón por la cual la superficie $\mathcal{E}$ tiene tantas singularidades es que el mínimo grado con el que aparece la variable t es 2. Por esto, las derivadas parciales se anulan. Pero haciendo una sencilla operación algebraica podemos ver lo siguiente. Volvamos a considerar la ecuación afín de antes y dividamos a ambos lados por t^2. Esto es:

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

Que es lo mismo que:

$$\left(\frac{y}{t}\right)^2 = t\left(\frac{x}{t}\right)^3 - t\left(\frac{x}{t}\right) + 1.$$

Si llamamos $y' = \frac{y}{t}$ y $x' = \frac{x}{t}$, nos queda la ecuación:

$$y'^2 = tx'^3 - tx' + 1.$$

Lo que hicimos fue un simple cambio de coordenadas y resulta así que:

$$y^2 = x^3 - t^2x + t^2 \Leftrightarrow y'^2 = tx'^3 - tx' + 1.$$

Pero si pensamos esto en el contexto de la curva E sobre $\mathbb{Q}(t)$; la transformación:

$$(x, y) \longmapsto \left(\frac{x}{t}, \frac{y}{t}\right),$$

es un **isomorfismo** sobre $\mathbb{Q}(t)$. En efecto, multiplicar por $\frac{1}{t}$ está bien definido en $\mathbb{Q}(t)$; pues es un elemento del cuerpo; y claramente tiene inverso. De manera que estamos ante dos curvas que son **isomorfas** sobre $\mathbb{Q}(t)$:

$$E \,:\, y^2 = x^3 - t^2x + t^2 \quad y \quad E' \,:\, y^2 = tx^3 - tx + 1.$$

Sin embargo, las superficies elípticas asociadas a una y otra ya no serán iguales. De hecho, la superficie elíptica asociada a E' es la de ecuación homogénea:

$$\mathcal{E}' \,:\, Y^2ZU = TX^3 - TXZ^2 + Z^3U.$$

Es fácil verificar, que en $\mathcal{E}'$ sólo hay un punto singular, que es $P = ([0:1:0]\,;[1:0])$. De manera que no va a ser tan costoso hacer el proceso de desingularización.

El comentario que podemos hacer es que hay un sustento teórico que justifica que $\mathcal{E}'$ tenga muchas menos singularidades que $\mathcal{E}$. Este hecho tiene que ver con la relación directa que hay entre la no singularidad de una variedad y la propiedad de su anillo de coordenadas de ser *íntegramente cerrado*. Un dominio íntegro A se dice íntegramente cerrado si satisface lo siguiente: si un elemento x del cuerpo de fracciones de A es raíz de un polinomio mónico con coeficientes en A, entonces $x \in A$. (Por ejemplo, $\mathbb{Z}$ lo es). Lo que hicimos, al pasar de $\mathcal{E}$ a $\mathcal{E}'$, fue lograr que la nueva superficie sea tal que su anillo de coordenadas es íntegramente cerrado; por lo que las singularidades son muchas menos.

Para resolver las singularidades de $\mathcal{E}'$ sólo tenemos que hacer entonces un Blow Up centrado en ese único punto singular. De todas maneras la construcción del Blow Up requiere de muchas cuentas, no sólo para definirlo; recordemos que además, una vez que se aplica, hay que encontrar la componente irreducible de esa variedad nueva que resulta ser la que es birracionalmente equivalente a $\mathcal{E}'$. Con ayuda del programa Singular hicimos esta cuenta y obtuvimos la variedad $\mathcal{E}^{min} \subseteq \mathbb{P}^2 \times \mathbb{P}^1 \times \mathbb{P}^2$, con coordenadas $([X:Y:Z]\,;[T:U]\,;[\alpha:\beta:\gamma])$ dada por las ecuaciones:

$$\mathcal{E}^{min} \,:\, \begin{cases} Y^2ZU - TX^3 + TXZ^2 - Z^3U = 0 \\ \alpha Z - \beta X = 0 \\ \alpha UY - \gamma XT = 0 \\ \beta UY - \gamma ZT = 0 \\ Z^2\beta\gamma + XY\alpha^2 - XY\beta^2 - Y^2\beta\gamma = 0 \\ Z^3\gamma + X^2Y\alpha - XYZ\beta - Y^2Z\gamma = 0 \\ XZ\beta^2\gamma + XY\alpha^3 - XY\alpha\beta^2 - Y^2\alpha\beta\gamma = 0 \\ X^2\beta^3\gamma + XY\alpha^4 - XY\alpha^2\beta^2 - Y^2\alpha^2\beta\gamma = 0 \end{cases}$$

Tenemos que $\mathcal{E}^{min}$ es una superficie birracionalmente equivalente a $\mathcal{E}'$, donde el morfismo birracional está dado por:

$$\Pi \,:\, \mathcal{E}^{min} \longrightarrow \mathcal{E}'$$
$$([X:Y:Z]\,;[T:U]\,;[\alpha:\beta:\gamma]) \mapsto ([X:Y:Z]\,;[T:U])$$

Usamos la notación $\mathcal{E}^{min}$ porque efectivamente es una superficie elíptica minimal. Con el Blow Up conseguimos que sea no singular; y se verifica también que es minimal, pues no se puede proyectar en ninguna dirección mediante un morfismo birracional.

Tenemos así una superficie elíptica minimal $\mathcal{E}^{min} \subseteq \mathbb{P}^2 \times \mathbb{P}^1 \times \mathbb{P}^2$, con morfismo de proyección $\pi^{min} \,:\, \mathcal{E}^{min} \longrightarrow \mathbb{P}^1$ dado por:

$$\pi^{min}([X:Y:Z]\,;[T:U]\,;[\alpha:\beta:\gamma]) = [T:U]\,.$$

Casi toda fibra $\mathcal{E}_q^{min}$ es una curva elíptica. Veamos cuáles son las fibras que no lo son. Para los puntos tales que $U \neq 0$, la fibra $\mathcal{E}_q^{min}$ es isomorfa a la fibra $\mathcal{E}'_q$; por lo que podemos mirar simplemente la ecuación de $\mathcal{E}'$ y ver para qué puntos $q \in \mathbb{P}^1$ se tiene que la fibra no es una curva elíptica. Para puntos de la forma $q = [t : 1]$, la ecuación afinizando en Z es:

$$\mathcal{E}' \, : \, y^2 = tx^3 - tx + 1.$$

Recordemos que es isomorfa a la curva $y^2 = x^3 - t^2x + t^2$. Y vimos que ésta es una curva elíptica salvo para $t = 0$, $t = \frac{3}{2}\sqrt{3}$ y $t = -\frac{3}{2}\sqrt{3}$. Para esos mismos valores entonces la fibra $\mathcal{E}_q^{min}$ no es una curva elíptica. El caso $t = 0$ tiene además la particularidad de que la fibra es reducible. Analicemos esto porque nos va a interesar mucho. La fibra $\mathcal{E}_0^{min}$ es isomorfa a $\mathcal{E}'_0$, y ésta, con la ecuación homogénea es:

$$\mathcal{E}'_0 \, : \, Y^2Z = Z^3.$$

Y tenemos:

$$Y^2Z = Z^3 \Leftrightarrow Y^2Z - Z^3 = 0 \Leftrightarrow Z(Y^2 - Z^2) = 0 \Leftrightarrow Z(Y - Z)(Y + Z) = 0.$$

De modo que $\mathcal{E}'_0$ consta de tres componentes irreducibles que son las rectas dadas por las ecuaciones: $Z = 0$; $Y = Z$ e $Y = -Z$. Precisamente son las rectas:

$$\begin{aligned} R_1 &= \{([X : Y : 0] \, ; [0 : 1])\} \\ R_2 &= \{([X : Z : Z] \, ; [0 : 1])\} \\ R_3 &= \{([X : -Z : Z] \, ; [0 : 1])\} \end{aligned}$$

Como $\mathcal{E}'_0$ es isomorfa a $\mathcal{E}_0^{min}$, ésta última tiene exactamente el mismo comportamiento.

Sólo nos falta ver qué pasa con los puntos tales que $U = 0$; o sea, la fibra $\mathcal{E}_\infty^{min}$. Aquí no podemos hacer lo mismo, pues como hicimos el Blow Up, no es cierto que $\mathcal{E}_\infty^{min}$ sea isomorfa a $\mathcal{E}'_\infty$. Justamente allí es donde hicimos el Blow Up. Tendremos que mirar entonces las ocho ecuaciones que definen a $\mathcal{E}^{min}$ y hacer $U = 0$. Evaluando $U = 0$ en las ecuaciones de $\mathcal{E}^{min}$ obtenemos que hay 5 componentes irreducibles. Son 5 rectas que son las siguientes:

$$\begin{aligned} L_1 &= \{([0 : 1 : 0] \, ; [1 : 0] \, ; [\alpha : 0 : \gamma])\} \\ L_2 &= \{([0 : 1 : 0] \, ; [1 : 0] \, ; [\alpha : \beta : 0])\} \\ L_3 &= \{([0 : Y : Z] \, ; [1 : 0] \, ; [0 : 1 : 0])\} \\ L_4 &= \{([X : Y : X] \, ; [1 : 0] \, ; [1 : 1 : 0])\} \\ L_5 &= \{([X : Y : -X] \, ; [1 : 0] \, ; [1 : -1 : 0])\} \end{aligned}$$

En resumen, $\mathcal{E}^{min} \subseteq \mathbb{P}^2 \times \mathbb{P}^1 \times \mathbb{P}^2$, es una superficie elíptica minimal dada por las ocho ecuaciones que listamos antes; con morfismo de proyección:

$$\pi^{min}([X : Y : Z] \, ; [T : U] \, ; [\alpha : \beta : \gamma]) = [T : U] \, ,$$

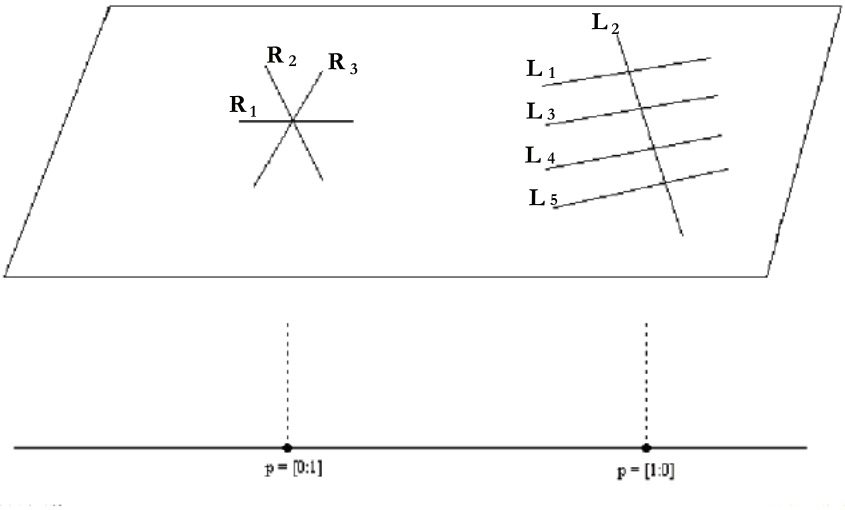


Figura 3.7: Fibras de $T = 0$ y $U = 0$

sobre $\mathbb{P}^1$. Las fibras $\mathcal{E}_q^{min}$ son curvas elípticas salvo para los puntos $[0:1]$, $[1:0]$; $\left[\frac{3}{2}\sqrt{3}:1\right]$ y $\left[-\frac{3}{2}\sqrt{3}:1\right]$ de $\mathbb{P}^1$. Las únicas fibras reducibles son las correspondientes a los puntos $[0:1]$ y $[1:0]$. Precisamente $\mathcal{E}_0^{min}$ consta de 3 rectas y $\mathcal{E}_\infty^{min}$ consta de 5 rectas. De acuerdo a cómo se intersecan las rectas de esas dos fibras podemos imaginar un diagrama como el de la Figura 3.7.

Por último, antes de volver con los resultados generales sobre superficies elípticas minimales, veamos cuáles son los puntos de E' (secciones de $\mathcal{E}'$) que obtenemos al trasladar los que teníamos en E. En primer lugar recordemos que, para pasar de E a E', vimos que la función que había que aplicar, trabajando en el afín $Z = U = 1$, era:

$$(x, y) \longmapsto \left(\frac{x}{t}, \frac{y}{t}\right).$$

Volviendo a coordenadas homogéneas, el isomorfismo entre E y E' es:

$$E \longrightarrow E'$$
$$[X:Y:Z] \mapsto [UX:UY:TZ]$$

De este modo, los 7 puntos de E que teníamos se corresponden con 7 puntos de E' según lo

siguiente:

$$\begin{aligned} E &\longrightarrow E' \\ [0:1:0] &\longrightarrow [0:1:0] \\ [T:T:U] &\longrightarrow [1:1:1] \\ [T:-T:U] &\longrightarrow [1:-1:1] \\ [0:T:U] &\longrightarrow [0:1:1] \\ [0:-T:U] &\longrightarrow [0:-1:1] \\ [1:1:1] &\longrightarrow [U:U:T] \\ [1:-1:1] &\longrightarrow [U:-U:T] \end{aligned}$$

3.4.2. Forma bilineal de Manin-Shioda

En esta sección veremos qué construcciones nuevas podemos hacer con una superficie elíptica minimal; y obtendremos resultados que nos darán interesante información acerca de la curva elíptica sobre $\overline{\mathbb{Q}(t)}$ asociada.

En esta parte volveremos a explotar la correspondencia que hay entre curvas elípticas sobre $\overline{\mathbb{Q}(t)}$ y superficies elípticas. A partir de las propiedades geométricas que ya vimos en superficies fibradas, y algunas otras que veremos a continuación específicas de superficies elípticas, vamos a poder construir una forma bilineal asociada a una curva elíptica sobre $\overline{\mathbb{Q}(t)}$ que, como veremos, tendrá una gran utilidad. De hecho es una de las construcciones esenciales de todo el trabajo que estamos haciendo.

Para esta parte vamos a trabajar con superficies elípticas minimales. Sólo mostraremos el caso particular en que la curva de base es $\mathbb{P}^1$; porque solamente nos interesan las curvas elípticas sobre $\overline{\mathbb{Q}(t)}$; pero todo puede generalizarse sin problemas.

Recordemos que dada una superficie elíptica $\mathcal{E}$, tenemos asociada a ella una curva elíptica E sobre $\overline{k} = \overline{\mathbb{Q}(t)}$. Vimos también que los puntos de E se corresponden con secciones de $\mathcal{E}$. Fijemos entonces un punto $P \in E(\overline{k})$. Este se corresponderá con una sección $\sigma_P : \mathbb{P}^1 \longrightarrow \mathcal{E}$. En cada fibra $\mathcal{E}_q$ que resulte ser una curva elíptica podemos usar su estructura algebraica y definir una función de *traslación* según el punto $\sigma_P(q) \in \mathcal{E}_q$. La suposición de que $\mathcal{E}$ es minimal nos asegura que podemos extender esa traslación a un morfismo definido en toda la superficie $\mathcal{E}$. El resultado es el siguiente:

Proposición 3.4.5. *Sea $\mathcal{E}$ una superficie elíptica minimal con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathbb{P}^1$ y sea E la curva elíptica sobre $\overline{k} = \overline{\mathbb{Q}(t)}$ asociada a $\mathcal{E}$ descripta en la Proposición 3.2.3. Dado $P \in E(\overline{k})$, sea σ_P la sección asociada a P. Entonces la función τ_P, definida en cada fibra $\mathcal{E}_q$ que sea una curva elíptica, como:*

$$\tau_P(q') = q' + \sigma_P(q),$$

se extiende a un morfismo:

$$\tau_P : \mathcal{E} \longrightarrow \mathcal{E}.$$

Y más aún, resulta ser un automorfismo de $\mathcal{E}$.

Demostración: Es claro que la función τ_P es una función birracional; pues es una función racional definida en casi todo punto $q' \in \mathcal{E}$ y tiene una vuelta racional que es τ_{-P}. Entonces, como τ_P y τ_{-P} son funciones birracionales y $\mathcal{E}$ es minimal, por la Proposición 3.4.4 resulta que ambas son morfismos. En particular, son automorfismos de $\mathcal{E}$. □

Necesitamos algunos resultados más antes de llegar al más importante. El próximo va a establecer una relación entre divisores de $\mathcal{E}$ y de E. Dado un punto $P \in E(\overline{k})$, tenemos la sección σ_P cuya imagen $\sigma_P(\mathbb{P}^1)$ es una curva irreducible de $\mathcal{E}$. Podemos considerar entonces el divisor $(\sigma_P(\mathbb{P}^1)) \in \mathcal{D}iv(\mathcal{E})$. Para que la notación no sea tan cargada vamos a escribir simplemente $(P) \in \mathcal{D}iv(\mathcal{E})$; teniendo en cuenta que no es lo mismo que $(P) \in \mathcal{D}iv(E)$.

Supongamos ahora que tenemos $P, Q \in E(\overline{k})$ y consideremos el punto $P + Q \in E(\overline{k})$. Una pregunta natural que surge es qué relación habrá entre los divisores $(P + Q)$ y $(P) + (Q)$ de $\mathcal{D}iv(\mathcal{E})$. En principio son cosas bien diferentes; pues el primero es el divisor dado por la curva irreducible de $\sigma_{P+Q}(\mathbb{P}^1)$, y el segundo es la suma en $\mathcal{D}iv(\mathcal{E})$ de los divisores (P) y (Q). Sin embargo hay un vínculo que se puede establecer y es el que surge de la siguiente proposición.

Proposición 3.4.6. *Sea $\mathcal{E}$ una superficie elíptica minimal con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathbb{P}^1$ y sea E la curva elíptica sobre $\overline{k} = \overline{\mathbb{Q}(t)}$ asociada a $\mathcal{E}$. Supongamos que tenemos $P_1, ..., P_r \in E(\overline{k})$ y enteros $n_1, ..., n_r$ tales que:*

$$[n_1]\, P_1 + \cdots + [n_r]\, P_r = \mathcal{O}.$$

Sea $n = n_1 + \cdots + n_r$. Entonces el divisor:

$$n_1(P_1) + \cdots + n_r(P_r) - n(\mathcal{O}) \in \mathcal{D}iv(\mathcal{E}),$$

es equivalente a un divisor fibral.

En particular, si $P, Q \in E(\overline{k})$, el divisor:

$$(P + Q) - (P) - (Q) + (\mathcal{O}),$$

es equivalente a un divisor fibral.

Demostración: Ver [10], Capítulo III, Proposición 9.2. □

Sólo nos falta presentar un resultado antes de mostrar la construcción de la forma bilineal. El resultado está propuesto como ejercicio en [10]. Precisamente: Capítulo III, Ejercicio 3.22. Dice lo siguiente:

Sea $\mathcal{E}$ una superficie elíptica minimal con morfismo de proyección $\pi : \mathcal{E} \longrightarrow \mathbb{P}^1$ y sea E la curva elíptica sobre $\overline{k} = \overline{\mathbb{Q}(t)}$ asociada a $\mathcal{E}$. Dado un punto $P \in E(\overline{k})$, consideremos $(P) \in \mathcal{D}iv(\mathcal{E})$. Entonces:

$$(P).\pi^*(q) = 1 \ \ \forall q \in \mathbb{P}^1.$$

En particular,

$$((P)-(\mathcal{O})).\pi^*(q)=0 \ \ \forall q\in\mathbb{P}^1.$$

Observemos que esto nos permite obtener un corolario inmediato. Recordando la Proposición 3.3.14, llamando $D=((P)-(\mathcal{O}))$, podemos asegurar que existe un divisor $\Phi_P\in\mathcal{D}iv(\mathcal{E})\otimes\mathbb{Q}$ tal que:

$$(D+\Phi_P).F=0 \ \ \forall F\in\mathcal{D}iv(\mathcal{E}) \ divisor\ fibral.$$

Vamos a definir:

$$D_P=(P)-(\mathcal{O})+\Phi_P.$$

Ahora sí podemos definir la forma bilineal.

Definición 3.4.7. Sea E una curva elíptica sobre $\overline{k}=\overline{\mathbb{Q}(t)}$. Definimos la aplicación:

$$\begin{array}{rccc}\langle\ ,\ \rangle : & E(\overline{k})\times E(\overline{k}) & \longrightarrow & \mathbb{R} \\ & \langle P,Q\rangle & = & -D_P.D_Q\end{array}$$

Antes de mostrar que efectivamente es una forma bilineal hagamos un comentario. Recordemos que en el Teorema 3.1.16 habíamos definido otra forma bilineal asociada a una curva elíptica sobre $\overline{\mathbb{Q}(t)}$. Uno puede preguntarse si hay relación entre una y otra. Hay un detalle que anticipa la respuesta y es que hemos usado la misma notación. Pues, en efecto, resulta que son **la misma** forma bilineal; y este es uno de los resultados más trascendentales de todo este texto y que vamos a demostrar a continuación; siguiendo la demostración hecha en [10], Capítulo III, Teorema 9.3.

Teorema 3.4.8. *Sea E una curva elíptica sobre $\overline{k}=\overline{\mathbb{Q}(t)}$ y sea $\mathcal{E}$ la superficie elíptica minimal asociada a E. Entonces la aplicación:*

$$\begin{array}{rccc}\langle\ ,\ \rangle : & E(\overline{k})\times E(\overline{k}) & \longrightarrow & \mathbb{R} \\ & \langle P,Q\rangle & = & -D_P.D_Q\end{array}$$

satisface las siguientes propiedades:

a) $\langle\ ,\ \rangle$ *es una forma bilineal.*

b) $\langle\ ,\ \rangle$ *coincide con la forma bilineal definida en el Teorema 3.1.16.*

Demostración: a) Veamos primero que $\langle\ ,\ \rangle$ está bien definida. O sea, que no depende de la elección de los divisores fibrales Φ. Sean $P,Q\in E(\overline{k})$ y sean Φ_P y Φ_Q divisores fibrales asociados a cada uno respectivamente. Entonces tenemos:

$$\langle P,Q\rangle=-D_P.D_Q=-D_P.((Q)-(\mathcal{O})+\Phi_Q)=-D_P.((Q)-(\mathcal{O}))-\underbrace{D_P.\Phi_Q}_{=0}=$$

$$((P)-(\mathcal{O})).((Q)-(\mathcal{O}))-\Phi_P.((Q)-(\mathcal{O})).$$

Ahora, si hacemos otra elección para los Φ, digamos Φ'_P y Φ'_Q, repitiendo la cuenta nos queda:

$$\langle P,Q\rangle = ((P)-(\mathcal{O})).((Q)-(\mathcal{O}))-\Phi'_P.((Q)-(\mathcal{O})).$$

Sólo basta ver entonces que:

$$\Phi'_P.((Q)-(\mathcal{O}))=\Phi_P.((Q)-(\mathcal{O})).$$

Por la unicidad en la Proposición 3.3.14 sabemos que $\Phi'_P=\Phi_P+F$, con $F\in\pi^*(\mathcal{D}iv(\mathcal{C})\otimes\mathbb{Q})$. Entonces:

$$\Phi'_P.((Q)-(\mathcal{O}))=(\Phi_P+F).((Q)-(\mathcal{O}))=\Phi_P.((Q)-(\mathcal{O}))+F.((Q)-(\mathcal{O}))=\Phi_P.((Q)-(\mathcal{O})).$$

En efecto, $F.((Q)-(\mathcal{O}))=0$ por el ejercicio que citamos antes.

Veamos ahora que es una forma bilineal. Dados $P,Q,R\in E(\overline{k})$, tenemos:

$$\langle P,Q+R\rangle-\langle P,Q\rangle-\langle P,R\rangle=-D_P.D_{Q+R}+D_P.D_Q+D_P.D_R=$$

$$-D_P.(D_{Q+R}-D_Q-D_R)=-D_P.(((Q+R)-(\mathcal{O})+\Phi_{Q+R})-((Q)-(\mathcal{O})+\Phi_Q)-((R)-(\mathcal{O})+\Phi_R))=$$

$$-D_P.((Q+R)-(Q)-(R)+(\mathcal{O})+\Phi_{Q+R}-\Phi_Q-\Phi_R).$$

Por la Proposición 3.4.6 $(Q+R)-(Q)-(R)+(\mathcal{O})$ es equivalente a un divisor fibral, digamos F. Entonces queda:

$$-D_P.(F+\Phi_{Q+R}-\Phi_Q-\Phi_R).$$

Y esto es cero, pues $F+\Phi_{Q+R}-\Phi_Q-\Phi_R$ es fibral. Luego,:

$$\langle P,Q+R\rangle-\langle P,Q\rangle-\langle P,R\rangle=0.$$

Por otro lado es claro que la aplicación es simétrica. Por lo tanto es efectivamente una forma bilineal.

b) Veamos ahora que coincide con la definida en el Teorema 3.1.16. Queremos ver que $\langle P,P\rangle=\hat{h}(P)$. Veamos:

$$\langle P,P\rangle=-D_P.D_P=-((P)-(\mathcal{O})+\Phi_P).D_P=-((P)-(\mathcal{O})).D_P=$$

$$2(P).(\mathcal{O})-(P)^2-(\mathcal{O})^2+((P)-(\mathcal{O})).\Phi_P. \qquad \textbf{(1)}$$

Afirmamos que $(P)^2$ no depende del punto P. Una forma de ver esto es la siguiente. No es difícil ver que el índice de intersección entre dos curvas irreducibles distintas se mantiene invariante bajo un automorfismo. Más precisamente, si τ es un automorfismo de $\mathcal{E}$ y $\Gamma_1,\Gamma_2\subseteq\mathcal{E}$ son dos curvas irreducibles; entonces:

$$(\Gamma_1).(\Gamma_2)=(\tau(\Gamma_1)).(\tau(\Gamma_2)).$$

En particular, considerando la sección asociada al punto P, tenemos que:

$$(P).(P)=(\tau_{-P}(P)).(\tau_{-P}(P))=(\mathcal{O}).(\mathcal{O}).$$

Recordando la Proposición 3.3.14 observamos que Φ_P es de la forma:

$$\Phi_P = \sum_{p \in \mathcal{C}} \sum_{i=0}^{r_p} a_{p_i}(\Gamma_{p_i});$$

donde los a_{p_i} dependen de los índices $((P) - (\mathcal{O})).(\Gamma_{p_j})$, para $1 \leq j \leq r_p$. Pero sabemos que $(P).(\Gamma_{p_j})$ y $(\mathcal{O}).(\Gamma_{p_j})$ sólo pueden valer 0 ó 1. De modo que $((P) - (\mathcal{O})).(\Gamma_{p_j})$ sólo toma finitos valores si vamos variando el punto P. Volviendo a la expresión que teníamos en **(1)**, concluimos que:

$$\langle P, P \rangle = 2(P).(\mathcal{O}) + O(1).$$

Esto es, existen constantes C_1 y C_2, que sólo dependen de la curva E, tales que, para todo $P \in E(\overline{k})$, se tiene:

$$C_1 \leq \langle P, P \rangle - 2(P).(\mathcal{O}) \leq C_2.$$

Calculemos $(P).(\mathcal{O})$. Vamos a suponer primero que $[2]\, P \neq \mathcal{O}$. Digamos que la curva elíptica E está dada afinmente por:

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

Recordemos que podemos suponer que el término cuadrático no aparece. Llamemos $P = (x_P, y_P)$. Podemos suponer también que $x_P, y_P \in \overline{k}$ no tienen polos comunes con A y B; cambiando de coordenadas si fuera necesario. Sea $p \in \mathbb{P}^1$ y calculemos $(P.\mathcal{O})_{\sigma_0(p)}$; donde σ_0 es la sección asociada a $\mathcal{O}$. Como σ_0 tiene un polo en p, si $x_P(p) \neq \infty$, entonces las secciones de P y de $\mathcal{O}$ no se intersecan en $\mathcal{E}_p$; por lo que $(P.\mathcal{O})_{\sigma_0(p)} = 0$. Si $x_P(p) = \infty$; es decir, $ord_p(x_P) < 0$; mirando la ecuación de E concluimos que:

$$3ord_p(x_P) = 2ord_P(y_P).$$

Para facilitar las cuentas hagamos el siguiente cambio de coordenadas:

$$w = \frac{x}{y} \qquad z = \frac{1}{y}.$$

Entonces la ecuación de la curva queda:

$$E \,:\, z = w^3 + Awz^2 + Bz^3;$$

y $P = (w_P, z_P) = \left(\frac{x_P}{y_P}, \frac{1}{y_P}\right)$.

Supongamos sin perder generalidad que p es de la forma $p = [t_0 : 1]$. Trabajando entonces en el afín $U = 1$, el anillo de valuación discreta de $\mathcal{E}$ en el punto $\sigma_0(p)$ es:

$$\frac{\overline{\mathbb{Q}}\,[w, z, t]_{(0,0,t_0)}}{(z - w^3 - Awz^2 - Bz^3)}.$$

Ahora, con el cambio de coordenadas que hicimos, es fácil encontrar funciones que determinen a las secciones de P y de $\mathcal{O}$. Tenemos que:

$$f_1(w, z, t) = w_P(t) - w \quad \textit{determina a } P$$

$$f_2(w,z,t) = w \quad determina\ a\ \mathcal{O}.$$

Luego:

$$(P.\mathcal{O})_{\sigma_0(p)} = \frac{\overline{\mathbb{Q}}\,[w,z,t]_{(0,0,t_0)}}{(z-w^3-Awz^2-Bz^3, w_P(t)-w, w)} \simeq \frac{\overline{\mathbb{Q}}\,[z,t]_{(0,t_0)}}{(z-Bz^3, w_P(t))}.$$

Pero $z - Bz^3 = z(1-Bz^3)$; y $1-Bz^3$ es una unidad en $\overline{\mathbb{Q}}\,[z,t]_{(0,t_0)}$. De modo que queda:

$$\frac{\overline{\mathbb{Q}}\,[z,t]_{(0,t_0)}}{(z-Bz^3, w_P(t))} \simeq \frac{\overline{\mathbb{Q}}\,[z,t]_{(0,t_0)}}{(z, w_P(t))} \simeq \frac{\overline{\mathbb{Q}}\,[t]_{t_0}}{(w_P(t))}.$$

Escribamos $w_P(t) = (t-t_0)^e v$; con v una unidad en $\overline{\mathbb{Q}}\,[t]_{t_0}$. Entonces:

$$\frac{\overline{\mathbb{Q}}\,[t]_{t_0}}{(w_P(t))} = \frac{\overline{\mathbb{Q}}\,[t]_{t_0}}{((t-t_0)^e)}.$$

Y:

$$dim_{\overline{\mathbb{Q}}}\left(\frac{\overline{\mathbb{Q}}\,[t]_{t_0}}{((t-t_0)^e)}\right) = e.$$

O sea, $(P.\mathcal{O})_{\sigma_0(p)} = e$. Pero por otro lado:

$$e = ord_{t_0}(w_P) = ord_{t_0}\left(\frac{x_P}{y_P}\right) = ord_{t_0}(x_P) - ord_{t_0}(y_P) = -\frac{1}{2}ord_{t_0}(x_P).$$

En conclusión nos queda:

$$(P.\mathcal{O})_{\sigma_0(p)} = \begin{cases} 0 & si\ ord_p(x_P) \geq 0 \\ -\frac{1}{2}ord_p(x_P) & si\, ord_p(x_P) < 0 \end{cases}$$

Por lo tanto:

$$(P).(\mathcal{O}) = \sum_{p\in\mathbb{P}^1}(P.\mathcal{O})_{\sigma_0(p)} = \sum_{p\in\mathbb{P}^1;\, ord_p(x_P)<0} -\frac{1}{2}ord_p(x_P) = \frac{1}{2}h_E(P).$$

Por lo que $2(P).(\mathcal{O}) = h_E(P)$. Luego, hemos visto que:

$$\langle P, P\rangle = h_E(P) + O(1),$$

siempre y cuando $[2]\,P \neq \mathcal{O}$. Pero sólo hay finitos P para los cuales $[2]\,P = \mathcal{O}$. De modo que, ajustando las constantes si fuera necesario, podemos suponer que la igualdad vale para todo P.

Definamos la función:

$$g(P) = \frac{1}{2}\langle P, P\rangle.$$

Entonces resulta que:

$$g(P) = \frac{1}{2}h_E(P) + O(1);$$

y, como ya vimos que $\langle\ ,\ \rangle$ es bilineal; se tiene:

$$g(2P) = 4g(P).$$

Por lo tanto, por el Teorema 3.1.16, tenemos que $g = \hat{h}_E$; como queríamos probar. □

Por lo que hicimos en la última demostración podemos asegurar que el siguiente concepto está bien definido.

Definición 3.4.9. Sea E una curva elíptica definida sobre $\overline{k} = \overline{\mathbb{Q}(t)}$ y $\mathcal{E}$ la superficie elíptica asociada a E. Se llama *género aritmético* de $\mathcal{E}$ al número:

$$\chi = -(P).(P),$$

donde P es cualquier punto de $E(\overline{k})$.

Una de las interesantes consecuencias que tiene este teorema es la siguiente. Por definición, es claro que los valores que toma la forma bilineal $\langle\ ,\ \rangle$ construida usando divisores e intersecciones, son *racionales*. Esto no es para nada evidente si miramos la construcción hecha con la altura canónica.

Cuando vimos el Teorema 3.1.16 y definimos aquella forma bilineal, observamos que era una manera de caracterizar a los puntos de torsión de una curva. Además mostramos una forma, que no parecía muy práctica, de acotar inferiormente el rango de la curva. Lo que logramos con este último teorema es tener otra manera de aplicar ese mismo razonamiento pero, en muchos casos, mucho más cómoda. Se trata de hacer exactamente lo mismo que aquella vez; pero ahora el cálculo de los valores que toma la forma bilineal puede ser más sencillo. En efecto, lo es en general; es más fácil calcular los índices de intersección de ciertas curvas que usar la definición de altura canónica que viene dada por un límite.

Ahora vamos a volver con nuestra curva elíptica sobre $\mathbb{Q}(t)$ que teníamos y veremos cómo se aplica esta última técnica para intentar acotar inferiormente su rango. Más aún, en el capítulo siguiente mostraremos ejemplos de construcciones en los que este recurso funciona de manera muy significativa, logrando encontrar ejemplos de curvas con rango considerablemente alto.

Volviendo a nuestro ejemplo, hagamos algunas cuentas. Consideremos nuestra curva elíptica E' sobre $\mathbb{Q}(t)$. Vamos a aplicar la forma bilineal de Manin-Shioda con los 7 puntos de E' que conocemos. Para ello necesitamos calcular el Φ_P de cada uno. Pero antes observemos que $[1:1:1]$ y $[1:-1:1]$ son inversos. Lo mismo ocurre con $[0:1:1]$ y $[0:-1:1]$; y con $[U:U:T]$ y $[U:-U:T]$. De manera que, si lo que queremos es encontrar puntos que sean linealmente independientes en $E'(\mathbb{Q}(t))$; podemos descartar a esos puntos que son inversos porque es evidente que no nos van a servir para nuestro objetivo. Quedémonos entonces con los puntos:

$$\begin{aligned} P_0 = \mathcal{O} &= [0:1:0] \\ P_1 &= [1:1:1] \\ P_2 &= [0:1:1] \\ P_3 &= [U:U:T] \end{aligned}$$

Calculemos entonces Φ_{P_1}, Φ_{P_2} y Φ_{P_3}. Recordando la definición, tenemos que considerar los divisores $D_{P_i} = (P_i) - (\mathcal{O})$ de $\mathcal{D}iv(\mathcal{E}^{min})$ y usar el procedimiento que vimos en la Proposición 3.3.14. Como vimos aquella vez, para esto sólo basta considerar las fibras de $\mathcal{E}^{min}$ que son

reducibles. En nuestro caso son $\mathcal{E}_0^{min}$ y $\mathcal{E}_\infty^{min}$. De manera que los Φ_{P_i} sólo tendrán componentes en esas fibras; y a esas componentes las notamos $\Phi_{P_i,0}$ y $\Phi_{P_i,\infty}$.

Empecemos por ver qué ocurre en $\mathcal{E}_0^{min}$. Aquí es más sencillo porque podemos mirar simplemente la fibra $\mathcal{E}'$; pues son isomorfas, ya que el Blow Up lo hicimos en $U = 0$. Teníamos en esta fibra las rectas R_1, R_2 y R_3. Para calcular los $\Phi_{P_i,0}$ vamos a necesitar calcular las intersecciones $(R_i).(R_j)$. Es claro que si $i \neq j$ entonces $(R_i).(R_j) = 1$; pues basta con que recordemos la Figura 3.7. Para calcular R_i^2 podemos usar la Proposición 3.3.11. A partir de la ecuación de $\mathcal{E}'$:

$$\mathcal{E}' \, : \, Y^2ZU = TX^3 - TXZ^2 + Z^3U,$$

vemos que:

$$T(X^3 - XZ^2) = UZ(Y - Z)(Y + Z).$$

De aquí podemos concluir fácilmente que, si llamamos u_0 a la función $\frac{T}{U}$, que es un uniformizador local en $[0 : 1]$; se tiene que $ord_{R_i}(u_0 \circ \pi') = 1$. La razón que nos permite concluir esto es que las ecuaciones que definen a las rectas aparecen con multiplicidad 1. En consecuencia:

$$\pi'^*([0 : 1]) = \sum_{i=1}^{3} ord_{R_i}(u_0 \circ \pi')(R_i) = (R_1) + (R_2) + (R_3).$$

Así, por ejemplo, por la Proposición 3.3.11:

$$0 = R_1.\pi'^*([0 : 1]) = R_1^2 + (R_1).(R_2) + (R_1).(R_3) = R_1^2 + 2.$$

Con lo cual $R_1^2 = -2$. Análogamente: $R_2^2 = R_3^2 = -2$.

Otra cosa que vamos a necesitar son las intersecciones $(P_i).(R_j)$. Donde, recordemos, la notación (P_i) se refiere al divisor $(\sigma_{P_i}(\mathbb{P}^1)) \in \mathcal{D}iv(\mathcal{E})$. Esto no es difícil. Simplemente mirando las ecuaciones concluimos que $\mathcal{O}$ y P_3 intersecan en un punto a R_1, y P_1 y P_2 intersecan en un punto a R_2. Además es fácil verificar, parametrizando, que las intersecciones son transversales. (Ver Figura 3.8).

Para $i = 1, 2, 3$; planteamos entonces $\Phi_{P_i,0} = a_{2,i}(R_2) + a_{3,i}(R_3)$ y consideramos el sistema:

$$\begin{cases} a_{2,i}R_2^2 + a_{3,i}(R_2).(R_3) = & ((\mathcal{O}) - (P_i)).(R_2) \\ a_{2,i}(R_3).(R_2) + a_{3,i}R_3^2 = & ((\mathcal{O}) - (P_i)).(R_3) \end{cases}$$

Con las cuentas que ya hicimos tenemos los siguientes cuadros:

.	R_2	R_3
R_2	-2	1
R_3	1	-2

.	R_2	R_3
$\mathcal{O}$	0	0
P_1	1	0
P_2	1	0
P_3	0	0

	$((\mathcal{O}) - (P_i)).(R_2)$	$((\mathcal{O}) - (P_i)).(R_3)$
P_1	-1	0
P_2	-1	0
P_3	0	0

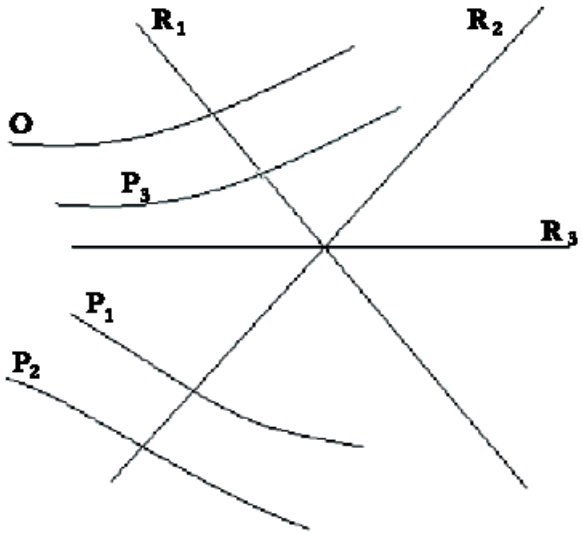


Figura 3.8: Fibra de $T = 0$.

Resolviendo los sistemas nos queda que $a_{2,1} = a_{2,2} = \frac{2}{3}$; $a_{3,1} = a_{3,2} = \frac{1}{3}$ y $a_{2,3} = a_{3,3} = 0$. De manera que:

$$\Phi_{P_1,0} = \Phi_{P_2,0} = \frac{2}{3}(R_2) + \frac{1}{3}(R_3)$$
$$\Phi_{P_3,0} = 0$$

No es sorprendente que $\Phi_{P_3,0} = 0$ ya que la sección asociada a P_3 pasa por la misma componente de $\mathcal{E}'_0$ que la sección asociada a $\mathcal{O}$.

Veamos ahora qué pasa en $\mathcal{E}^{min}_\infty$. Aquí no nos queda otra alternativa que usar las ocho ecuaciones que definen a $\mathcal{E}^{min}$. En esta fibra tenemos las rectas L_1, L_2, L_3, L_4 y L_5. En este caso también vamos a necesitar las intersecciones $(L_i).(L_j)$ y $(P_i).(L_j)$. Recordando el dibujo, es fácil decir cuánto da $(L_i).(L_j)$ si $i \neq j$. Simplemente se tiene que:

$$(L_i).(L_j) = 0 \ \ si \ i, j \neq 2, \ i \neq j;$$

y:

$$(L_i).(L_2) = 1, \ \ \forall i \neq 2.$$

Para calcular L_i^2 necesitamos conocer $(\pi^{min})^*([1:0])$. Este es un trabajo un poco más costoso que antes porque tenemos muchas más ecuaciones. Pero no es mucho más difícil. Vamos a mostrar cuánto dan $ord_{L_1}(u_\infty \circ \pi^{min})$ y $ord_{L_2}(u_\infty \circ \pi^{min})$, donde u_∞ es la función $\frac{U}{T}$, que es uniformizador local en $[1:0]$. La cuenta para las rectas L_3, L_4 y L_5 es análoga a la de L_1; así que vamos a dejarlas para que, quien lo desee, las verifique. Afirmamos que $ord_{L_1}(u_\infty \circ \pi^{min}) = 1$. Una manera muy elegante de probar esto es mostrando que existe una sección de $\mathcal{E}^{min}$ que pasa por L_1. Pues recordemos que si Γ es una sección de $\mathcal{E}^{min}$, entonces:

$$(\Gamma).(\pi^{min})^*(q) = 1, \ \ \forall q \in \mathbb{P}^1.$$

En particular:

$$(\Gamma).(\pi^{min})^*([1:0]) = 1.$$

Esto implicaría que el orden de la componente por la que pasa Γ debe ser 1. Veremos en efecto que podemos conseguirnos una tal sección, que no es otra de las que estamos considerando. Sin embargo mostremos también la cuenta explícita para ver que también se puede hacer *a mano*.

Consideramos el anillo local $\mathcal{O}_{L_1}$, que es la localización del anillo de coordenadas de $\mathcal{E}^{min}$ en el ideal que define a L_1. Busquemos un uniformizador local del ideal $I(L_1)$ visto dentro de $\mathcal{O}_{L_1}$. Mirando cuáles son los puntos que conforman la recta L_1 podemos encontrar fácilmente generadores de $I(L_1)$. En efecto:

$$I(L_1) = (X, Z, U, \beta).$$

De la segunda ecuación de $\mathcal{E}^{min}$ tenemos que:

$$\alpha Z - \beta X = 0 \; en \, \mathcal{O}_{L_1}.$$

Y como $\alpha \notin I(L_1)$,

$$Z = \left(\frac{X}{\alpha}\right) \beta \; en \; \mathcal{O}_{L_1}.$$

Por lo que $Z \in (\beta)\mathcal{O}_{L_1}$.

Mirando ahora la quinta ecuación de $\mathcal{E}^{min}$ tenemos:

$$Z^2\beta\gamma + XY\alpha^2 - XY\beta^2 - Y^2\beta\gamma = 0 \; en \, \mathcal{O}_{L_1}.$$

Entonces:

$$\beta(Z^2\gamma - XY - Y^2\gamma) = -XY\alpha^2.$$

Como $Z^2\gamma \in I(L_1)$, $XY \in I(L_1)$ e $Y^2\gamma \notin I(L_1)$; el factor que multiplica a β no pertenece a $I(L_1)$, de manera que:

$$\beta = -\left(\frac{Y\alpha^2}{Z^2\gamma - XY - Y^2\gamma}\right) X.$$

Luego, $\beta \in (X)\mathcal{O}_{L_1}$.

Por último, mirando la tercera ecuación de $\mathcal{E}^{min}$, tenemos:

$$\alpha UY - \gamma XT = 0 \; en \, \mathcal{O}_{L_1}.$$

Análogamente a lo que hicimos antes, como $\gamma \notin I(L_1)$ y $T \notin I(L_1)$, resulta que $X \in (U)\mathcal{O}_{L_1}$.

De todo esto se concluye que:

$$I(L_1) = (U)\mathcal{O}_{L_1},$$

por lo que $ord_{L_1}(u_\infty \circ \pi^{min}) = 1$.

Veamos ahora qué pasa con L_2. En este caso, veremos en seguida, no tenemos a mano una sección de $\mathcal{E}^{min}$ que pase por L_2. Así que no podríamos usar el argumento que dijimos antes. En efecto,

ocurre que **no existe** tal sección; pues se tiene que $ord_{L_2}(u_\infty \circ \pi^{min}) = 2$. Veamos por qué. Mirando los puntos de L_2 obtenemos los siguientes generadores del ideal $I(L_2)$:

$$I(L_2) = (X, Z, U, \gamma).$$

De la segunda ecuación de $\mathcal{E}^{min}$ tenemos:

$$\alpha Z - \beta X = 0 \; en \, \mathcal{O}_{L_2};$$

y como hicimos antes, dado que $\alpha \notin I(L_2)$, concluimos que $Z \in (X)\mathcal{O}_{L_1}$.

Mirando ahora la tercera ecuación:

$$\alpha UY - \gamma XT = 0 \; en \, \mathcal{O}_{L_2}.$$

Y como $\alpha \notin I(L_2)$ e $Y \notin I(L_2)$; obtenemos que $U \in (X)\mathcal{O}_{L_1}$.

Miremos ahora la quinta ecuación:

$$Z^2\beta\gamma + XY\alpha^2 - XY\beta^2 - Y^2\beta\gamma = 0 \; en \, \mathcal{O}_{L_2}.$$

Con sencillas cuentas algebraicas obtenemos:

$$\gamma\beta(Z - Y)(Z + Y) = -XY(\alpha - \beta)(\alpha + \beta). \quad \textbf{(1)}$$

Dado que ni β, ni $Z - Y$ ni $Z + Y$ pertenecen a $I(L_2)$; obtenemos que $\gamma \in (X)\mathcal{O}_{L_1}$.

Por todo esto concluimos que:

$$I(L_2) = (X)\mathcal{O}_{L_2}.$$

O sea, X es un uniformizador local. Pero nosotros queremos calcular $ord_{L_2}(u_\infty \circ \pi^{min})$; es decir, el orden de la función $\frac{U}{T}$ en ese anillo de valuación discreta. Para ello volvamos a mirar la tercera ecuación de $\mathcal{E}^{min}$ y escribámosla del siguiente modo:

$$\alpha Y \left(\frac{U}{T}\right) = \gamma X.$$

Tomando orden a ambos miembros de la igualdad tenemos:

$$ord_{L_2}(\alpha) + ord_{L_2}(Y) + ord_{L_2}\left(\frac{U}{T}\right) = ord_{L_2}(\gamma) + ord_{L_2}(X).$$

Como $ord_{L_2}(\alpha) = ord_{L_2}(Y) = 0$ y $ord_{L_2}(X) = 1$, nos queda que:

$$ord_{L_2}\left(\frac{U}{T}\right) = ord_{L_2}(\gamma) + 1.$$

Sólo nos falta calcular $ord_{L_2}(\gamma)$; pero para eso tomemos orden en la igualdad **(1)**. Tenemos que ni β, ni $Z - Y$, ni $Z + Y$, ni Y, ni $(\alpha - \beta)$, ni $(\alpha + \beta)$ pertenecen a $I(L_2)$; por lo que sus órdenes son 0. En consecuencia nos queda:

$$ord_{L_2}(\gamma) = ord_{L_2}(X) = 1.$$

Luego:

$$ord_{L_2}\left(\frac{U}{T}\right) = ord_{L_2}(\gamma) + 1 = 2.$$

O sea, como habíamos afirmado, $ord_{L_2}(u_\infty \circ \pi^{min}) = 2$.

Como dijimos, con cuentas similares a las que hicimos para L_1 podemos ver que:

$$ord_{L_i}(u_\infty \circ \pi^{min}) = 1 \quad \text{para } i = 3, 4, 5.$$

Con esto nos queda:

$$(\pi^{min})^*([1:0]) = \sum_{i=1}^{5} ord_{L_i}(u_\infty \circ \pi^{min})(L_i) = (L_1) + 2(L_2) + (L_3) + (L_4) + (L_5).$$

Ahora sí podemos calcular L_i^2. Como ya sabemos el valor de $(L_i).(L_j)$ para $i \neq j$, podemos usar el procedimiento de antes y nos queda:

$$L_i^2 = -2, \ \forall i.$$

Lo que nos falta hacer es calcular las intersecciones $(P_i).(L_j)$. Necesitamos ver por qué recta pasan las secciones asociadas a los puntos que tenemos. Esto no es tan inmediato como en la fibra $\mathcal{E}_0^{min}$. Lo que debemos hacer es levantar las secciones que tenemos en $\mathcal{E}'$, a través del Blow Up, a secciones de $\mathcal{E}'$. En las fibras distintas de $\mathcal{E}_\infty^{min}$ hay una relación de uno a uno; por lo que cada sección de $\mathcal{E}'$ se levanta a una sección de $\mathcal{E}^{min}$. Una vez que obtengamos las curvas de $\mathcal{E}^{min}$, que son las levantadas de nuestras secciones en $\mathcal{E}'$, nos tenemos que fijar a cuál de las componentes de $\mathcal{E}_\infty^{min}$ interseca.

Empecemos por la sección de $\mathcal{O}$. Si en las ecuaciones de $\mathcal{E}^{min}$ hacemos $X = Z = 0$, $Y = 1$; nos queda que $\alpha = \beta = 0$. Por lo tanto la sección de $\mathcal{O}$ se levanta a la sección dada por:

$$\{([0:1:0]\,;[T:U]\,;[0:0:1])\}\,.$$

Cuando $U = 0$ esta sección interseca a L_1.

Para levantar la sección de P_1 tenemos que hacer $X = Y = Z = 1$. Afinizando en $U = 1$ nos quedan las relaciones $\alpha = \beta = t\gamma$. Volviendo a coordenadas homogéneas nos queda la sección dada por:

$$\{([1:1:1]\,;[T:U]\,;[T\gamma:T\gamma:U\gamma])\} = \{([1:1:1]\,;[T:U]\,;[T:T:U])\}\,.$$

Cuando $U = 0$ esta sección interseca a L_4.

Para levantar la sección de P_2 hacemos $X = 0$, $Y = Z = 1$. Afinizando en $T = 1$ nos queda $\alpha = 0$ y $\gamma = u\beta$. Volviendo a coordenadas homogéneas nos queda:

$$\{([0:1:1]\,;[T:U]\,;[0:T\beta:U\beta])\} = \{([0:1:1]\,;[T:U]\,;[0:T:U])\}\,.$$

Cuando $U = 0$ esta sección interseca a L_3.

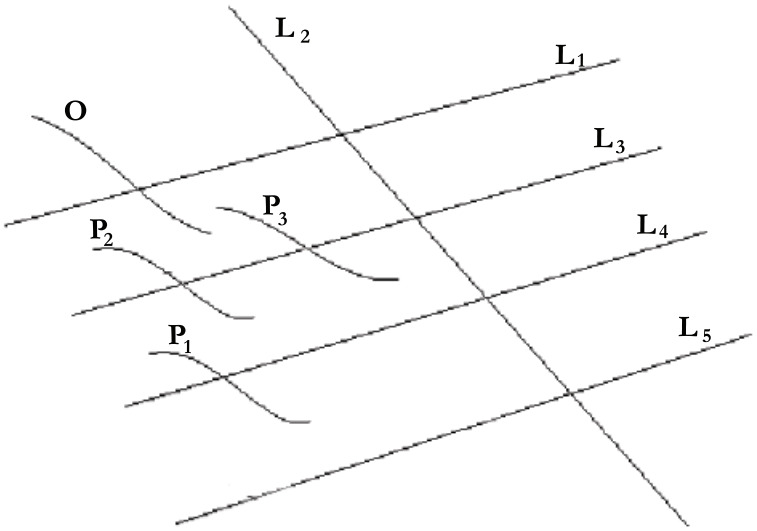


Figura 3.9: Fibra de $U = 0$.

Por último, para levantar la sección de P_3 hacemos $X = Y = U$, $Z = T$. Afinizando en $T = 1$ nos queda $\alpha = u\beta$ y $\gamma = u^2\beta$. Volviendo a coordenadas homogéneas nos queda:

$$\left\{\left([U : U : T]\,; [T : U]\,; \left[TU\beta : T^2\beta : U^2\beta\right]\right)\right\} = \left\{\left([U : U : T]\,; [T : U]\,; \left[TU : T^2 : U^2\right]\right)\right\}.$$

Cuando $U = 0$ esta sección interseca a L_3.

Podemos verificar fácilmente, parametrizando, que las intersecciones son transversales. Nos quedó una situación como la de la Figura 3.9.

Ya tenemos todo para ponernos a calcular los $\Phi_{P_i,\infty}$. Para $i = 1, 2, 3$; planteamos $\Phi_{P_i,\infty} = a_{1,i}(L_1) + a_{3,i}(L_3) + a_{4,i}(L_4) + a_{5,i}(L_5)$ y consideramos el sistema:

$$\begin{cases} a_{1,i}L_1^2 + a_{3,i}(L_1).(L_3) + a_{4,i}(L_1).(L_4) + a_{5,i}(L_1).(L_5) = ((\mathcal{O}) - (P_i)).(L_1) \\ a_{1,i}(L_3).(L_1) + a_{3,i}L_3^2 + a_{4,i}(L_3).(L_4) + a_{5,i}(L_3).(L_5) = ((\mathcal{O}) - (P_i)).(L_3) \\ a_{1,i}(L_4).(L_1) + a_{3,i}(L_4).(L_3) + a_{4,i}L_4^2 + a_{5,i}(L_4).(L_5) = ((\mathcal{O}) - (P_i)).(L_4) \\ a_{1,i}(L_5).(L_1) + a_{3,i}(L_5).(L_3) + a_{4,i}(L_5).(L_4) + a_{5,i}L_5^2 = ((\mathcal{O}) - (P_i)).(L_5) \end{cases}$$

Con las cuentas que hicimos tenemos ahora los siguientes cuadros:

.	L_1	L_3	L_4	L_5
L_1	-2	0	0	0
L_3	0	-2	0	0
L_4	0	0	-2	0
L_5	0	0	0	-2

.	L_1	L_3	L_4	L_5
$\mathcal{O}$	1	0	0	0
P_1	0	0	1	0
P_2	0	1	0	0
P_3	0	1	0	0

	$((\mathcal{O})-(P_i)).(L_1)$	$((\mathcal{O})-(P_i)).(L_3)$	$((\mathcal{O})-(P_i)).(L_4)$	$((\mathcal{O})-(P_i)).(L_5)$
P_1	1	0	-1	0
P_2	1	-1	0	0
P_3	1	-1	0	0

Resolviendo los sistemas nos queda:

$$a_{1,1} = -\frac{1}{2},\ \ a_{4,1} = \frac{1}{2},\ \ a_{3,1} = a_{5,1} = 0$$

$$a_{1,2} = a_{1,3} = -\frac{1}{2},\ \ a_{3,2} = a_{3,3} = \frac{1}{2},\ \ a_{4,2} = a_{4,3} = 0.$$

De manera que:

$$\Phi_{P_1,\infty} = -\frac{1}{2}(L_1) + \frac{1}{2}(L_4)$$

$$\Phi_{P_2,\infty} = \Phi_{P_3,\infty} = -\frac{1}{2}(L_1) + \frac{1}{2}(L_3).$$

En definitiva, recordando que $D_{P_i} = (P_i) - (\mathcal{O}) + \Phi_{P_i}$, nos queda:

$$D_{P_1} = (P_1) - (\mathcal{O}) + \frac{2}{3}(R_2) + \frac{1}{3}(R_3) - \frac{1}{2}(L_1) + \frac{1}{2}(L_4)$$

$$D_{P_2} = (P_2) - (\mathcal{O}) + \frac{2}{3}(R_2) + \frac{1}{3}(R_3) - \frac{1}{2}(L_1) + \frac{1}{2}(L_3)$$

$$D_{P_3} = (P_3) - (\mathcal{O}) - \frac{1}{2}(L_1) + \frac{1}{2}(L_3).$$

Queremos calcular los números $\langle P_i, P_j\rangle = -D_{P_i}.D_{P_j}$. Ya conocemos las intersecciones $(L_i).(L_j)$, $(R_i).(R_j)$, $(P_i).(L_j)$ y $(P_i).(L_j)$. Es claro que $(L_i).(R_j) = 0$; pues son curvas fibrales de distintas fibras, por lo que su intersección es vacía.

Sólo nos falta conocer las intersecciones $(P_i).(P_j)$. El caso $i \neq j$ es fácil. Basta con mirar las 4 secciones que estamos considerando y ver si se intersecan. Resulta que la única intersección se da entre las secciones de P_1 y P_3 en el punto $([1:1:1]\,;[1:1])$. Parametrizando es fácil ver que la intersección es transversal.

Por último, calculemos P_i^2; esto es, calculemos $-\chi$. Como no depende de la sección basta calcularlo para una, digamos P_1^2. Necesitamos una función tal que su divisor tenga a (P_1) como componente. Proponemos:

$$F([X:Y:Z]\,;[T:U]\,;[\alpha:\beta:\gamma]) = \frac{X-Z}{Y}.$$

No es difícil ver que las curvas irreducibles de $\mathcal{E}^{min}$ que se anulan con la función $X - Z$ son exactamente $(\mathcal{O})$, (P_1), $(-P_1)$, (L_1), (L_2) y (L_4). Haciendo $Y = 0$ en las ecuaciones de $\mathcal{E}^{min}$

observamos que hay una única curva irreducible que aparece. Es una curva horizontal que, si la vemos en $\mathcal{E}'$ y afinizando en $Z = U = 1$, está dada por:

$$\Gamma = \left\{([x : 0 : 1] ; [t : 1]) \ : \ tx^3 - tx + 1 = 0\right\}.$$

De modo que:

$$div(F) = n_0(\mathcal{O}) + n_1(P_1) + n_2(-P_1) + m_1(L_1) + m_2(L_2) + m_4(L_4) + s(\Gamma).$$

No vamos a decir cuál es el valor de cada uno de los enteros que aparecen ahí; sólo los que necesitemos. Tenemos:

$$-\chi = P_1^2 = (P_1).((P_1) - div(F)).$$

Como la sección de P_1 no corta ni a la sección de $\mathcal{O}$ ni a la de $-P_1$; ni a las rectas L_1, L_2 y Γ; su intersección con todas ellas será 0; por lo que no nos interesa el orden con el que aparecen en $div(F)$. Sólo nos importan entonces los números n_1 y m_4. Pero no es nada difícil comprobar que ambos dan 1. Son cuentas idénticas a las que hicimos antes. Luego, nos queda:

$$-\chi = P_1^2 = -(P_1).(L_4) = -1.$$

O sea, $\chi = 1$. Podemos entonces resumir las intersecciones $(P_i).(P_j)$ en el siguiente cuadro:

.	$\mathcal{O}$	P_1	P_2	P_3
$\mathcal{O}$	-1	0	0	0
P_1	0	-1	0	1
P_2	0	0	-1	0
P_3	0	1	0	-1

No nos queda más que hacer las cuentas. Ya sabemos cuánto dan todas las intersecciones. Sólo hay que hacer las distributivas correspondientes. La matriz que obtenemos es:

$$M = \langle P_i, P_j \rangle_{1 \leq i,j \leq 3} = \begin{pmatrix} \frac{1}{3} & -\frac{1}{6} & -\frac{1}{2} \\ -\frac{1}{6} & \frac{1}{3} & 0 \\ -\frac{1}{2} & 0 & 1 \end{pmatrix}.$$

Resulta:

$$det(M) = 0.$$

Esto dice que los 3 puntos son linealmente dependientes. Más aún, el núcleo de M es el subespacio:

$$\mathbb{S} = \langle (2, 1, 1) \rangle.$$

De lo que podemos inferir una relación lineal que satisfacen P_1, P_2 y P_3 en $E(\mathbb{Q}(t))$ que es:

$$2P_1 + P_2 + P_3 = \mathcal{O} \ \ o\, bien \ \ P_3 = -2P_1 - P_2.$$

Si nos limitamos a la submatriz:

$$M' = \langle P_i, P_j \rangle_{1 \leq i,j \leq 2} = \begin{pmatrix} \frac{1}{3} & -\frac{1}{6} \\ -\frac{1}{6} & \frac{1}{3} \end{pmatrix};$$

tenemos:

$$det(M') = \frac{1}{12} \neq 0.$$

La conclusión que sacamos es que los puntos P_1 y P_2 de la curva E' son linealmente independientes. En particular, el rango de E' es mayor o igual que 2. Además el punto P_3 es combinación lineal de P_1 y P_2.

Recordemos que la curva E' es isomorfa a la curva E, que es con la que habíamos empezado. Si volvemos a mirar los puntos P_1 y P_2 en E, tenemos los puntos $[T : T : U]$ y $[0 : T : U]$. Escribamos entonces en resumen la conclusión a la que pudimos arribar:

Resumen 3.4.10. Sea E la curva elíptica sobre $\mathbb{Q}(t)$ dada por la ecuación afín:

$$E \, : \, y^2 = x^3 - t^2 x + t^2.$$

Se tiene que el rango de E es mayor o igual que 2. Más aún, los puntos de coordenadas afines $(x, y) = (t, t)$ y $(x, y) = (0, t)$ son linealmente independientes.

Nos pareció interesante usar este ejemplo para desarrollar detalladamente esta técnica para que se vea que, si bien puede resultar trabajosa, no es muy difícil a los efectos prácticos.

En el capítulo siguiente mostraremos una construcción de una curva con muchos más puntos linealmente independientes.

Antes de pasar a esta última parte vamos a enunciar un teorema muy importante (cuya demostración es bastante difícil) que nos permite obtener un corolario muy interesante de todo lo que hicimos. Observemos que si tenemos una curva elíptica E sobre $\mathbb{Q}(t)$, especializando la t en distintos valores obtenemos curvas E_t sobre $\mathbb{Q}$. Y para casi todas esas especializaciones (para todas salvo finitas) E_t es una curva elíptica. Precisamente E_t no es más que la fibra $\mathcal{E}_t$ de la superficie elíptica $\mathcal{E}$ asociada a E. Hay un resultado muy intersante que vincula a la curva E con las curvas E_t que es el siguiente:

Teorema 3.4.11. (*Teorema de Especialización de Silverman*). *Sea E una curva elíptica sobre $\mathbb{Q}(t)$ que no se descompone. Sean $P_1, ..., P_r \in E(\mathbb{Q}(t))$ puntos linealmente independientes. Digamos, $P_i = [X_i(t) : Y_i(t) : Z_i(t)]$, con $X_i(t), Y_i(t), Z_i(t) \in \mathbb{Q}(t)$. Entonces, para casi todo t, los puntos $P_i \in E_t$, que resultan de especializar en t, son linealmente independientes en la curva elíptica E_t.*

Este teorema se puede encontrar en [10], Capítulo III, Sección 11; o también en el trabajo [11].

Corolario 3.4.12. *Sea E una curva elíptica sobre $\mathbb{Q}(t)$ que no se descompone. Si E tiene rango mayor o igual que r, entonces, para casi todo t, la curva elíptica E_t sobre $\mathbb{Q}$ tiene rango mayor o igual que r.*

Corolario 3.4.13. *Si E es una curva elíptica sobre $\mathbb{Q}(t)$ de rango mayor o igual que r; se tiene una familia infinita de curvas elípticas E_t sobre $\mathbb{Q}$, todas de rango mayor o igual que r.*

Este es un resultado muy interesante por varias razones. El hecho de poder conseguir, a partir de una curva elíptica de rango alto en $\mathbb{Q}(t)$, una familia infinita de curvas elípticas de rango alto en $\mathbb{Q}$ es algo para nada trivial. Ocurre que en general no es fácil conseguir curvas elípticas de rango elevado. Si uno elige una curva elíptica al azar, lo más probable es que tenga rango 0 o 1. En el ejemplo que hicimos, si bien no conseguimos una curva de rango muy alto; como consecuencia obtuvimos infinitas curvas de rango al menos 2; curvas que no se encuentran fácilmente. En el siguiente capítulo retomaremos estos comentarios.

Para terminar con este capítulo, y con el ejemplo que hemos trabajado; uno puede plantearse lo siguiente. Si bien conseguimos una familia infinita de curvas sobre $\mathbb{Q}$ de rango mayor o igual a 2; muchas de ellas, o quizás todas, podrían ser isomorfas, con lo cual, en realidad la familia de infinitas curvas no sería tan interesante. Pero tener una respuesta a este interrogante no es muy difícil. Recordemos que dos curvas son isomorfas si, y sólo si, su j-invariante es igual. Podemos entonces calcular el j-invariante de la curva E y obtener así el de todas las especializaciones. Si ese j-invariante no es constante; sino que depende de t, entonces sí, dentro de la familia de curvas, infinitas de ellas serán no isomorfas. El j-invariante de E es:

$$j = \frac{(48t^2)^3}{\Delta} = \frac{48^3 t^5}{16t^4(4t^2-27)} = \frac{48^3 t}{16(4t^2-27)}.$$

Claramente, para una especialización fija de t, sólo hay finitos t' para los que el j-invariante coincide. De hecho, a lo sumo hay un solo t' distinto de t. En consecuencia, efectivamente conseguimos una familia de infinitas curvas elípticas sobre $\mathbb{Q}$, no isomorfas dos a dos, con rango mayor o igual que 2. Son las que se obtienen con casi todas las especializaciones de E.

Capítulo 4

Construcción de Mestre

En este último capítulo vamos a mostrar brevemente y sin mucho detalle una construcción precisa de una curva elíptica sobre $\mathbb{Q}(t)$ de rango relativamente alto; lo cual se prueba usando la técnica que desarrollamos en el capítulo anterior. Nos vamos a basar en un trabajo de Jean François Mestre de los años '90 que fue muy importante ya que logró muchos avances. El mismo trabajo fue base para que se hicieran diversas construcciones posteriores.

4.1. Una familia de Curvas Elípticas sobre $\mathbb{Q}(t)$ de rango mayor o igual que 8

La construcción de esta familia es muy sencilla. Se trata de poder conseguir una curva elíptica sobre $\mathbb{Q}(t)$ de la cual conozcamos muchos puntos, y luego tratar de ajustar las cosas para que la mayor cantidad posible entre todos esos puntos que uno encuentra sean linealmente independientes.

Seamos precisos. Supongamos que tenemos un polinomio mónico $q \in \mathbb{Q}[t][x]$ de grado 8 con todas sus raíces en $\mathbb{Q}[t]$ y distintas:

$$q(x) = \prod_{i=1}^{8} (x - \alpha_i),$$

con $\alpha_i \in \mathbb{Q}[t]$ y $\alpha_i \neq \alpha_j$.

Es fácil ver, con simples cuentas algebraicas, que existe una escritura para q del siguiente modo:

$$q = g^2 - r.$$

Donde $g, r \in \mathbb{Q}[t][x]$; $deg(g) = 4$ y $deg(r) \leq 3$.

Esta escritura se obtiene simplemente considerando polinomios genéricos:

$$g = \sum_{i=0}^{4} a_i x^i \quad y \quad r = \sum_{i=0}^{3} b_i x^i,$$

y planteando el sistema de ecuaciones correspondiente que surge de igualar los coeficientes de q y de $g^2 - r$, obteniendo así los valores de a_i y b_i.

Si resulta que $deg(r) = 3$ uno puede considerar la curva de ecuación:

$$E : y^2 = r(x).$$

Si r no es mónico, eso no es mucho problema, ya que con un simple cambio de coordenadas en $\mathbb{Q}(t)$ podemos conseguir que lo sea. Si además resulta que su discriminante es no nulo, E es una curva elíptica.

Sorprendentemente, de una manera muy sencilla, nos conseguimos una curva elíptica que contiene 8 puntos conocidos; pues, por construcción tenemos que:

$$0 = q(\alpha_i) = g(\alpha_i)^2 - r(\alpha_i).$$

Por lo que:

$$g(\alpha_i)^2 = r(\alpha_i).$$

De este modo tenemos que los 8 puntos de coordenadas afines $P_i = (\alpha_i,\, g(\alpha_i))$ son puntos de E. Como además tenemos, como siempre, el punto $\mathcal{O} = [0 : 1 : 0]$, tenemos 9 puntos conocidos en E.

El siguiente paso es elegir los α_i. Los elegimos de la siguiente manera:

$$\alpha_i = k_i \pm t\,,\ i = 1, 2, 3, 4;$$

con $k_i \in \mathbb{Q}$. Si uno hace esa elección para los α_i, queda el polinomio:

$$q(x) = \prod_{i=1}^{4}(x - (k_i \pm t)).$$

Debido a la simetría que tiene q, cuando calculamos el polinomio r nos queda de la forma:

$$r(x) = At^2x^3 + Bt^2x^2 + t^2(Ct^2 + D)x + t^2(Et^2 + F).$$

Donde $A, B, C, D, E, F \in \mathbb{Q}$ dependen de k_1, k_2, k_3 y k_4. Nos queda entonces la curva:

$$y^2 = At^2x^3 + Bt^2x^2 + t^2(Ct^2 + D)x + t^2(Et^2 + F).$$

Dividiendo por t^2 y cambiando y por $y' = \frac{y}{t}$; es claro que esta curva es isomorfa a:

$$E : y^2 = Ax^3 + Bx^2 + (Ct^2 + D)x + (Et^2 + F).$$

Lo que hay que hacer en este paso es elegir los k_i de manera conveniente. En primer lugar tiene que satisfacerse que $A \neq 0$ y $\Delta \neq 0$; para que E sea efectivamente una curva elíptica. Con esto no perdemos demasiada libertad para los k_i. Una vez que nos aseguramos de que E es una curva elíptica nos ponemos a hacer el procedimiento que desarrollamos en el capítulo anterior. Hay que encontrar la superficie elíptica minimal asociada a E; considerar los 9 puntos que tenemos en

E, aplicar la forma bilineal y ver cuántos de ellos resultan ser linealmente independientes. Para todas estas cuentas nos ayudamos con programas de computadora; pero no porque sean difíciles, sino porque están involucradas muchas más variables que en el ejemplo que hicimos en el capítulo anterior. Luego de hacer este desarrollo vimos que existe un conjunto abierto-Zariski $\mathcal{U}$ en $\overline{\mathbb{Q}}^4$ tal que si $(k_1, k_2, k_3, k_4) \in \mathbb{Q}^4 \cap \mathcal{U}$, entonces la curva elíptica sobre $\mathbb{Q}(t)$ resultante tiene rango mayor o igual que 8. En efecto, construimos la forma bilineal y vimos que, en tales condiciones, la matriz de 8×8, $M = \langle P_i, P_j \rangle$, tiene determinante no nulo.

Observemos que tenemos una familia considerablemente grande de curvas sobre $\mathbb{Q}(t)$ de rango mayor o igual que 8. Decimos que es considerablemente grande porque los conjuntos abiertos Zariski en $\overline{\mathbb{Q}}^4$ son muy grandes, por lo que hay bastante libertad para elegir los valores de los k_i. Una de las posibles elecciones para los k_i es la siguiente:

$$k_1 = 1, k_2 = -2, k_3 = 8, k_4 = -4.$$

Con esos valores obtenemos la curva sobre $\mathbb{Q}(t)$ de ecuación afín:

$$E : y^2 = 12x^3 + 88x^2 + (-12t^2 + 96)x + 9t^2.$$

y los puntos P_i resultan ser:

$$\begin{aligned} P_1 &= (1 + t, -11t - 14) & P_2 &= (1 - t, -11t + 14) \\ P_3 &= (-2 + t, -7t + 8) & P_4 &= (-2 - t, -7t - 8) \\ P_5 &= (8 + t, 17t + 112) & P_6 &= (8 - t, 17t - 112) \\ P_7 &= (-4 + t, t - 16) & P_8 &= (-4 - t, t + 16). \end{aligned}$$

4.2. La construcción de Mestre

La construcción que hizo Jean François Mestre en su trabajo (ver [3]) sigue la misma técnica que mostramos recién, pero con algunas variantes. El toma como q un polinomio de grado 12; es decir, lo construye con valores racionales k_1, k_2, k_3, k_4, k_5 y k_6. El asunto es que el polinomio r le queda en principio de grado menor o igual que 5. Después, a la hora de elegir los k_i pide que el coeficiente de grado 5 de r sea cero. Se conforma con que r quede de grado 4 y sin raíces múltiples; en tal caso, lo que obtiene es una curva con un punto singular (el [0:1:0]), y la desingularización de esa curva resulta una curva elíptica. Esto último pude verse en [12]. La diferencia es que, luego de desingularizar, ya no es cierto necesariamente que el punto $[0 : 1 : 0]$ pertenezca a la curva; de modo que toma como origen a otro punto de manera arbitraria.

Por otro lado, las condiciones que le pide a los k_i son bastante más restrictivas que las que tuvimos que pedir nosotros en el ejemplo anterior. De este modo construye una curva elíptica (ya no una familia) sobre $\mathbb{Q}(t)$ pero de rango mayor o igual que 11. La curva es la siguiente:

$$y^2 = (429t^2 + 53260)x^4 - (5434t^2 + 1239000)x^3 + (-3432t^4 - 2451t^2 + 1222156)x^2 +$$

$$(21736t^4 - 3637984t^2 + 134780352)x + 6864t^6 - 1074992t^4 + 53200096t^2 - 758849264.$$

Esta curva contiene los siguientes 12 puntos $\mathbb{Q}(t)$-racionales:

$$P_1 = (-2t + 10, -138t^2 - 258t + 2184) \qquad P_2 = (-2t + 11, 346t^2 - 2998t - 1512)$$

$$P_3 = (-2t - 17, 1578t^2 + 22902t + 88536) \qquad P_4 = (-2t - 16, -1490t^2 - 22394t - 77220)$$

$$P_5 = (-2t + 14, 710t^2 - 6734t + 3720) \qquad P_6 = (-2t + 17, -1006t^2 + 9472t - 15708)$$

$$P_7 = (2t + 17, 1006t^2 + 9472t + 15708) \qquad P_8 = (2t + 14, -710t^2 - 6734t - 3720)$$

$$P_9 = (2t - 16, 1490t^2 - 22394t + 77220) \qquad P_{10} = (2t - 17, -1578t^2 + 22902t - 88536)$$

$$P_{11} = (2t + 11, -346t^2 - 2998t + 1512) \qquad P_{12} = (2t + 10, 138t^2 - 258t - 2184).$$

Eligiendo al punto P_{12} como origen resulta que los otros 11 puntos son linealmente independientes, por lo que la curva tiene rango mayor o igual que 11.

Posteriormente se pudo probar que esta misma curva tiene un punto más linealmente independiente con los que se tenían (ver [4] o [7]); y más aún, que el rango es exactamente igual a 12. Luego, con otro trabajo, a partir de la misma construcción, pero con otra elección de los parámetros, se encontró otra curva con rango igual a 13. (Ver [7]).

Estos avances fueron muy importantes ya que se conoce muy poco acerca del rango de las curvas elípticas en general. Para curvas elípticas sobre $\mathbb{Q}$ se conoce una con rango igual a 28. Para curvas sobre $\mathbb{Q}(t)$ se ha logrado, en los últimos años, encontrar una con rango igual a 15; y la construcción se basa también en el trabajo de Mestre. Esto tiene consecuencias sobre las curvas sobre $\mathbb{Q}(t)$; pues por el Teorema de las Especializaciones, tenemos la existencia de una familia infinita de curvas elípticas sobre $\mathbb{Q}$ de rango mayor o igual que 15. Esto no queda desestimado porque se sepa que hay una curva de rango 28; pues precisamente se conoce **una** de ellas; mientras que, pasando por la curva sobre $\mathbb{Q}(t)$ encontramos que las de rango mayor o igual que 15 son **infinitas**.

Bibliografía

[1] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag (1977).

[2] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag (1983).

[3] J-F. Mestre *Courbes elliptiques de rang* ≥ 11 *sur* $\mathbb{Q}(t)$, J C. R. Acad. Sci. Paris Sér. I Math. 313 (1991) p. 139-142.

[4] J-F. Mestre *Courbes elliptiques de rang* ≥ 12 *sur* $\mathbb{Q}(t)$, J C. R. Acad. Sci. Paris Sér. I Math. 313 (1991) p. 171-174.

[5] I. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag (1977).

[6] T. Shioda, *On the Mordell-Weil Lattices*, Comm. Math. Univ. Sancti Pauli., 39 (1990) p. 211-240.

[7] J. Scholten, *Elliptic Curves of high rank over function fields*, preprint.

[8] J. Silverman - J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag (1992).

[9] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag (1986).

[10] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag (1994).

[11] J. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. 342 (1983) p. 197-211.

[12] A. Weil, *Remarques sur un mémoire d'Hermite*, Arch. Math. 5 (1954) p. 197-202.