00365

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

DIVISIÓN DE ESTUDIOS DE POSGRADO

"SOBRE LOS MODELOS DE NÈRON PARA CURVAS ELÍPTICAS"

T E S I S

QUE PARA OBTENER EL GRADO ACADÉMICO DE

MAESTRO EN CIENCIAS (MATEMÁTICAS)

P R E S E N T A :

JESÚS ROGELIO PÉREZ BUENDÍA

DIRECTOR DE TESIS: DR. ENRIQUE JAVIER ELIZONDO HUERTA.

2001

Agradecimientos

Me gustaría agradecer a todas las personas que me han apoyado, no sólo en este trabajo, sino durante toda la maestría: Mi familia, Judith, Eduardo, los cuates. Al instituto de Matemáticas por darme un espacio de estudio, al la DEGEP por su beca para estudios de Posgrado. Especialmente a Herbert y a Javier por haberme ayudado con sus becas de proyecto en los últimos meses y por estar siempre atentos a mis problemas. A todas las personas que estoy dejando de mencionar por la presión de tiempo en la que actualmente me encuentro, pero que saben que siempre los tendré en cuenta.

Introducción

Los Modelos de Nèron fueron propuestos por André Nèron a principios de la década de los 60's (1960), con la intensión de estudiar la estructura entera de las variedades abelianas sobre campos numéricos. Desde entonces, en Aritmética y Geometría Algebraica se ha aplicado la teoría de los modelos de Nèron con gran éxito. Recientemente, gracias al desarrollo de la Geometría Aritmética, se ha reactivado el interés por saber más sobre los modelos de Nèron y profundizar en las bases de su construcción.

En este trabajo explicaremos qué es un modelo de Néron para un caso especial de variedades abelianas: las curvas elípticas. Aunque suponemos que se cuenta con cierto conocimiento de la teoría de esquemas y, en general, de geometría algebraica; mencionaré las definiciones y resultados que serán utilizados.

De manera breve podemos decir, sea R es un anillo de valuación discreta con campo de fracciones K, y E/K es la curva elíptica dada por la ecuación de Weierstrass

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

donde cada $a_i \in R$. Sabemos que con esta ecuación podemos definir un esquema cerrado $W \subset \mathbb{P}^2_R$, donde además cada punto K-racional en $E(K)$ se puede extender a un punto en $W(K)$, es decir, a un sección Spec $(R) \longrightarrow W$. También sabemos que en los puntos K-racionales de E, tenemos una estructura de grupo, misma que, como veremos en este trabajo, se puede extender a un mapeo racional de $W \times_R W \longrightarrow W$ que, en general, no es un morfismo, por lo que W no es siempre un grupo-esquema. Sin embargo, si quitamos todos los puntos singulares en la fibra especial de W y llamamos al esquema resultante W^0, entonces la ley de grupo se extiende a un morfismo $W^0 \times_R W^0 \longrightarrow W^0$ que convierte a W^0 en un grupo-esquema sobre R, pero

cada punto en $E(K)$ no se extiende necesariamente a un punto en $\Pi^0(K)$.

Así, un modelo de Nèron para E/K es un esquema $\mathcal{E}/R$ que cumple con las propiedades de que cada punto en $E(K)$ se extiende a un punto en $\mathcal{E}(R)$ y la ley de grupo se extiende a un morfismo de $\mathcal{E} \times_R \mathcal{E} \longrightarrow \mathcal{E}$ que hace de $\mathcal{E}$ un grupo-esquema sobre R.

En el primer capítulo damos un repaso de conceptos algebraicos tales como anillos de Dedekind, anillos de valuación discreta, completaciones y extensiones ramificadas. Este material será utilizado durante todo el trabajo.

Debido a que estamos trabajando con modelos de Nèron para curvas elípticas, el segundo capítulo lo dedicamos a dar un repaso general de las mismas. Es importante mencionar que dentro del desarrollo de la tesis se trabaja con propiedades de algunos esquemas que son análogas a las que tienen las curvas elípticas; tales como la estructura de grupo en sus puntos racionales y las curvas obtenidas al reducir modulo π.

En el capítulo tres trabajamos con esquemas. Definimos sus propiedades generales y aquellas que serán utilizadas más adelante. También centramos nuestra atención en una construcción que será de gran utilidad: el producto fibrado. Este producto nos permitirá dar el análogo a la reducción modulo π para un esquema y extender la estructura de grupo a éstos.

Finalmente, en el capítulo cuatro iniciamos trabajando con grupos algebraicos como preámbulo a lo que definiremos como grupos esquemas. Después estudiaremos a las superficies aritméticas, mismas que podemos pensar como una superficie formada de curvas. De esta manera podremos relacionar directamente las propiedades que nos interesan de las curvas elípticas con las de los esquemas. Esto nos permitirá definir a los modelos de Nèron y dar algunas de sus características.

Índice General

Capítulo 1

Campos locales

Este capítulo tiene por objetivo presentar los conceptos básicos de la teoría algebraica de números que serán utilizados durante el trabajo. Particularmente se estudian aquellos resultados que están relacionados con los dominios de Dedekind.

1.1 Dominios de Dedekind

Definición 1.1.1. Un anillo R es de *valuación discreta*, si es un dominio de ideales principales que tiene un único ideal primo $\mathcal{M} \neq 0$ que es, por lo tanto, maximal.

Como R es principal, el ideal $\mathcal{M}$ está generado por un elemento π, es decir, $\mathcal{M} = \pi R$ que es único salvo multiplicación por unidades.

Definición 1.1.2. Al elemento $\pi \in R$ que genera al ideal maximal $\mathcal{M} \subset R$ lo llamamos *parámetro uniformizador* de R.

Notemos que el elemento π es irreducible.

Tenemos que todos los ideales diferentes de cero en R son de la forma $\pi^n R$ ([AM69]) donde π es un parámetro uniformizador, por lo que cada elemento $x \in R$ puede ser escrito como $x = \pi^m u$ con $m \in \mathbb{N}$ y u una unidad. Al entero m lo llamamos la *valuación* o el orden de x y lo denotamos por $v(x)$. Notemos que este número no depende de la elección de π.

Proposición 1.1.3. *Sea K el campo de fracciones del anillo de valuación discreta R y sea K^* las unidades en K. Se cumplen las siguientes propiedades*

- *El mapeo* $v : K^* \longrightarrow \mathbb{Z}$ *es suprayectivo,*
- $v(xy) = v(x) + v(y)$,
- $v(x+y) \geq min\{v(x), v(y)\}$

Demostración. Es inmediata de la definición. □

Extendamos la definición de v a todo K haciendo $v(0) = \infty$.

El conocimiento de la función v determina al anillo R, en efecto $R = \{x \in K : v(x) \geq 0\}$ y $\mathcal{M} = \{x \in K : v(x) > 0\}$. Con esto vemos que pudimos haber iniciado definiendo al mapeo v.

Ejemplo 1.1.4.

1. Sea $K = \mathbb{Q}$. Tomemos un número primo $p \in \mathbb{Z}$ fijo. Cada $x \in \mathbb{Q}$ se puede escribir de forma única como $p^a(r/s)$ donde $a, r, s \in \mathbb{Z}$ y r, s son primos con p. Definimos $v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z}$ como $v_p(x) = a$. v_p es una valuación discreta en $\mathbb{Q}$ con anillo de valuación el anillo local $\mathbb{Z}_{(p)}$.

2. Sea $K(x)$ el campo de fracciones del anillo $K[x]$. Para $f \in K[x]$ irreducible, definimos $v_f : K(x)^* \longrightarrow \mathbb{Z}$ de manera análoga al párrafo anterior. También v_f es una valuación discreta de $K(x)$ con anillo de valuación igual a $K[x]_{(f)}$: la localización de $K[x]$ respecto al ideal generado por f.

Proposición 1.1.5. *Sea R un dominio local noetheriano de dimensión uno, $\mathcal{M}$ su ideal máximo, $k = R/\mathcal{M}$ su campo residual. Las siguientes afirmaciones son equivalentes:*

1. *R es un anillo de valuación discreta.*
2. *R es enteramente cerrado*[1].
3. *$\mathcal{M}$ es un ideal principal.*
4. *$\dim_k(\mathcal{M}/\mathcal{M}^2) = 1$ como k-espacio vectorial.*

[1] Un dominio es enteramente cerrado, si los elementos en su campo de fracciones que son cero de un polinomio mónico con coeficientes en el anillo, son sólo los elementos del anillo (ver [AM69]).

5. *Existe un elemento* $\pi \in R$ *tal que cada ideal no nulo es de la forma* (π^n) $n \geq 0$.

Teorema 1.1.6. Sea R un anillo noetheriano de dimensión uno. Las siguientes afirmaciones son equivalentes:

1. R es enteramente cerrado.

2 Cada ideal primario en R es potencia de un primo.

3. Cada anillo local $R_{\mathfrak{P}}$ $(\mathfrak{P} \neq 0)$ es un anillo de valuación discreta.

Definición 1.1.7. Una anillo que satisface las condiciones del teorema anterior se denomina: *dominio de Dedekind.*

Corolario 1.1.8. *En un dominio de Dedekind, cada ideal no nulo tiene una factorización única como producto de ideales primos.*

Ejemplo 1.1.9. Sea R un anillo de ideales principales, entonces R es noetheriano y de dimensión uno Sea $\mathfrak{P} \neq 0$ un ideal primo en R, entonces también $R_{\mathfrak{P}}$ es noetheriano y de dimensión uno ya que R lo es Por la proposición 1.1 5 $R_{\mathfrak{P}}$ es de valuación discreta (ya que también es de ideales principales); usando ahora el Teorema 1.1 6. concluimos que R es dominio de Dedekind Así, todo dominio de ideales principales es de Dedekind.

Ejemplo 1.1.10. El anillo $\mathbb{Z}$ de los números enteros es un anillo de Dedekind.

Definición 1.1.11. Un *ideal fraccional* I de R es un subconjunto $I \subset K$ que es un R-módulo finitamente generado. Decimos que I es invertible si existe I' ideal fraccionario tal que $I.I' = A$.

Proposición 1.1.12. *En un dominio de Dedekind* R *cada ideal fraccionario diferente de cero es invertible.*

Demostración. En un dominio de valuación discreta, un ideal fraccional tiene la forma $\pi^n R$ donde $n \in Z$, por lo que es invertible Ahora tomemos en cuenta que localizando, se cumple que

$$(I\ J)_P = I_P\ J_P; \quad (I + J)_P = I_P + J_P; \quad (I\ .\ J)_P = (I_P \cdot J_P)$$

siempre que J sea finitamente generado. Ahora, como para cada ideal primo P el ideal I_P es fraccionario, concluimos que I es fraccionario ([AM69]) □

Corolario 1.1.13. *Los ideales fraccionarios diferentes de cero de un dominio de Dedekind forman un grupo bajo la multiplicación.*

Definición 1.1.14. Al grupo de ideales fraccionarios de un dominio de Dedekind lo llamamos *grupo ideal* del anillo.

1.2 Completaciones

Sea K un campo con una valuación discreta v y anillo de valuación R. Si a es un número real entre cero y uno, definimos

$$|x| := a^{v(x)} \text{ para } x \neq 0 \quad \text{y } |0| = 0.$$

Tenemos que se cumplen las siguientes fórmulas:

$$|x.y| = |x|.|y|$$
$$|x + y| \leq \sup(|x|, |y|)$$
$$|x| = 0 \text{ si y sólo si } x = 0$$

vemos que $|\ |$ nos define un *valor absoluto discreto* (ver[Ser79])

Definición 1.2.1. Una sucesión $\{a_n\}$ de elementos en K es una *sucesión de Cauchi*, si para cualquier real positivo ε existe un número natural N tal que

$$|a_m - a_n| < \varepsilon, \text{ para todos } m, n > N.$$

Sabemos que lo anterior es equivalente a decir que $\lim_{n\to\infty} |a_m - a_n| = 0$

Definición 1.2.2. Decimos que una sucesión converge hacia a si $\lim_{n\to\infty} |a - a_n| = 0$

Definición 1.2.3. Un campo K es *completo* respecto al valor absoluto, si toda sucesión de Cauchi converge en K. Un campo que es completo respecto a un valor absoluto discreto es un *campo local.*

Ahora mostraremos que todo campo con una valuación discreta puede ser encajado en un campo local.

Denotemos por C al conjunto de todas las sucesiones de Cauchi de elementos en K y por W al subconjunto de todas las sucesiones tales que

$\lim |x_n| = 0$. Definamos suma y multiplicación en C por las reglas tradicionales:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}; \quad \{a_n\}.\{b_n\} = \{a_n.b_n\}.$$

Es fácil ver que con estas operaciones C es un anillo conmutativo con unidad $1_C = \{1\}$.

Ahora veamos que W es un ideal de C. En efecto, notemos que $\{y_n\}$ es una sucesión de Cauchi en K, entonces $\{|y_n|\}$ es de Cauchi en los reales $\mathbb{R}$ y los términos $|y_n|$ están acotados, por lo que $\lim |x_n y_n| = \lim |x_n||y_n|$. Ahora sí. si $\{y_n\} \in W$ y $\{x_n\} \in C$ tenemos que $\{x_n y_n\} \in W$.

Definición 1.2.4. Definimos la completación del campo K como el anillo $\hat{K} := C/W$.

Teorema 1.2.5. El anillo $\hat{K}$ es un campo completo respecto a un valor absoluto discreto que además contiene encajado a K, y cuyo valor absoluto extiende al de K.

Demostración. Ver el libro [Jan96] □

El encaje $i : K \to \hat{K}$ está dado por $x \mapsto \{x\}+W$ es decir, a x lo mandamos a la clase de la sucesión constante, que es claramente de Cauchi. Para ver cómo está definido el valor absoluto en $\hat{K}$, definamos $|\{x_n\} + W|_0 := \lim |x_n|$ por lo que $|i(x)|_0 = \lim |x| = |x|$ y así vemos que este valor absoluto extiende, en efecto, al de K.

Ejemplo 1.2.6. Tomemos el campo de los números racionales $\mathbb{Q}$ Definamos el valor absoluto discreto dado por la valuación discreta del ejemplo ?? al que llamaremos *valor absoluto p-ádico* y al que denotaremos por $|\ |_p$. Más precisamente tomemos $c = 1/p$ para p un número primo fijo. Definimos

$$|x|_p := c^{v_p(x)}$$

donde $v_p(x) = n$ si $x = p^n(a/b)$ con a, b enteros primos con p.

Definición 1.2.7. Definimos al campo $\mathbb{Q}_p$ de los *racionales p-ádicos* como la completación de $\mathbb{Q}$ respecto al valor absoluto p-ádico $|\ |_p$

Una manera alternativa de construir a $\mathbb{Q}_p$ es la siguiente: Para cada $n \geq 1$ sea $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Un elemento en A_n define de manera natural un elemento en A_{n-1}. por lo que tenemos un homomorfismo

$$o_n : A_n \longrightarrow A_{n-1}$$

que es suprayectivo y cuyo kernel es $p^{n-1}A_n$.

La sucesión

$$\cdots \to A_n \to A_{n-1} \to \cdots \to A_1$$

forma un sistema proyectivo indexado por los enteros mayores que uno.

Definición 1.2.8. El anillo de los enteros p-ádicos $\mathbb{Z}_p$ es el límite proyectivo del sistema (A_n, ϕ_n) recién definido.

Proposición 1.2.9. *Sea $\varepsilon_n : \mathbb{Z}_p \longrightarrow A_n$ el mapeo que asocia a cada entero p-ádico, su n-ésima componente. La sucesión de grupos abelianos*

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$$

es exacta.

Demostración. Ver el libro [Ser73] □

Con esta proposición vemos que podemos identificar $\mathbb{Z}_p/p^n\mathbb{Z}_p$ con $\mathbb{Z}/p^n\mathbb{Z}$.

Definición 1.2.10. Alternativamente definimos el campo de los racionales p-ádicos $\mathbb{Q}_p$ como el campo de fracciones del anillo $\mathbb{Z}_p$.

Este campo será de gran utilidad en este trabajo y será citado frecuentemente.

Ejemplo 1.2.11. El campo $\mathbb{Q}_p$ es un ejemplo de un campo local cuyo anillo de valuación es $\mathbb{Z}_p$. La valuación está dada por la propiedad de que $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$ y de aquí que cada elemento $x \in \mathbb{Q}_p$ puede ser escrito de forma única (salvo unidades) como $x = p^n u$ donde u es una unidad en $\mathbb{Z}_p$ y entonces $v_p(x) = n$.

1.3 Extensiones Ramificadas

En esta sección simplemente daremos algunas definiciones y mencionaremos algunos resultados que serán de utilidad para la parte final del trabajo.

Sea K un campo y L una extensión finita de K. Denotemos por $[L : K]$ al grado de la extensión. Sea a un dominio noetheriano enteramente cerrado tal que K es su campo de fracciones. Denotemos por B a la cerradura[2] entera de A en L. Por las propiedades de la cerradura entera, tenemos que L es el campo de fracciones de B ([Lor96]).

Supongamos que además B es un A-módulo finitamente generado.

Proposición 1.3.1. *Si A es un dominio de Dedekind, también lo es B.*

Demostración. Ver el libro de Atiyah [AM69]. □

En adelante supondremos que A es un dominio de Dedekind.

Definición 1.3.2. Si $\mathcal{B}$ es un ideal primo de B y si $P = \mathcal{B} \cap A$, decimos que $\mathcal{B}$ *divide* a P y escribimos $\mathcal{B}|P$.

Notemos que esta definición es equivalente a decir que $\mathcal{B}$ contiene al ideal PB generado por P.

Definición 1.3.3. Sea $e_{\mathcal{B}}$ el exponente de $\mathcal{B}$ en la descomposición de pB en ideales primos, es decir

$$e_{\mathcal{B}} = v_{\mathcal{B}}(PB), \qquad PB = \prod_{\mathcal{B}|P} \mathcal{B}^{e_{\mathcal{B}}}$$

Al entero $e_{\mathcal{B}}$ lo llamamos *índice de ramificación* de $\mathcal{B}$ en la extensión L/K.

Si $\mathcal{B}$ divide a P, el campo $B/\mathcal{B}$ es una extensión del campo A/P. Como B es finitamente generado sobre A, $B/\mathcal{B}$ es una extensión finita de A/P.

Definición 1.3.4. Al grado de extensión

$$f_{\mathcal{B}} := [B/\mathcal{B} : A/P]$$

lo llamamos *grado de residuo* de $\mathcal{B}$ en la extensión L/K.

[2] La cerradura entera de A en L es el conjunto de todos los elementos en L que son enteros sobre A. Este conjunto resulta ser también un anillo (ver [AM69])

Definición 1.3.5. • Si Sólo hay un ideal primo $\mathcal{B}$ que divide a P y si $f_{\mathcal{B}} = 1$, decimos que L/K es *totalmente ramificada* en P.

- Si $e_{\mathcal{B}} = 1$ y $B/\mathcal{B}$ es una extensión separable[3] de A/P, decimos que L/K es *no ramificada* en $\mathcal{B}$.
- Si L/K es no ramificada para todos los primos $\mathcal{B}$ que dividen a P, decimos que L/K es *no ramificada* sobre P.

Para un estudio completo sobre el tema, se puede revisar el libro [Ser79].

[3]Una extensión algebraica L/K de campos es separable, si el polinomio mínimo sobre K de cada elemento en L no tiene factores irreducibles repetidos en el anillo de polinomios sobre $\overline{K}$ (ver [Mor96]).

Capítulo 2

Curvas elípticas

Nuestro interés principal en este trabajo es estudiar a los modelos de Nèron para curvas elípticas 4, por lo que en este capítulo daremos un repaso general de la teoría de las mismas. En particular se mencionaran las propiedades que generalizaremos a esquemas y aquellas que nos gustaría que cumplieran los modelos de Nèron. Así, estudiaremos la estructura de grupo en los puntos racionales y a las curvas que se obtienen al reducir módulo π.

2.1 Curvas

Sea k un campo. El plano afín definido sobre k es el conjunto $\mathbb{A}^2_k = k^2$. Si tomamos un polinomio no constante $f \in k[x,y]$ tal que no tenga factores repetidos en $\overline{k}[x,y]$ y tomamos un campo $K \supset k$ (por lo que $\mathbb{A}^2_k \subset \mathbb{A}^2_K$) donde K puede ser tan grande como se guste, podemos definir una curva afín C_f (= C si queda claro) sobre k, como el conjunto de ceros en $\mathbb{A}^2_K$ del polinomio f y para cada campo E tal que $k \subset E \subset K$ definimos los puntos E-racionales de C_f como:

$$C_f(E) := \{(a,b) \in \mathbb{A}^2_E \,.\, f(a,b) = 0\}.$$

La curva C es irreducible si f es irreducible, y es geométricamente (totalmente) irreducible, si f resulta irreducible en $\overline{k}$. Además, como los polinomios sobre un campo forman un anillo de factorización única, podemos descomponer a f como el producto $f = f_1 f_2 \cdots f_r$ de distintos polinomios irreducibles y entonces

$$C_f = C_{f_1} \cup C_{f_2} \cup \cdots \cup C_{f_r}$$

con cada C_{f_i} irreducible. Llamamos a las C_{f_i} las componentes irreducibles de C.

Definiendo de manera natural las derivadas parciales de un polinomio, podemos dar el concepto de singularidad y de recta tangente: un punto $p = (a, b) \in C$ es no singular si no es cero simultáneamente de las derivadas parciales $\partial f/\partial x$ y $\partial f/\partial y$. La línea tangente a C en p está dada por:

$$\left(\frac{\partial f}{\partial x}\right)_p (x - a) + \left(\frac{\partial f}{\partial y}\right)_p (y - b) = 0.$$

La curva C es no singular si todos sus puntos en $C(\overline{k})$ son no singulares. Un punto o una curva que no es no singular es, por lo tanto, singular.

Sea $p = (a, b) \in C(K)$. Podemos escribir a f como una suma de polinomios en $x - a$ y $x - b$ con coeficientes en K de la siguiente manera (la expansión de Taylor de f):

$$f(x, y) = f_1(x - a, y - b) + f_2(x - a, y - b) + \cdots + f_r(x - a, y - b)$$

donde cada f_i es un polinomio homogéneo en $x - a$ y $x - b$ de grado i . El punto p es *no singular* si, y sólo si, $f_1 \neq 0$, en cuyo caso la ecuación de la recta tangente por p es $f_1 = 0$.

Si C es singular en p, decimos que p tiene *multiplicidad* m, si $f = f_m(x - a, y - b) +$ {términos de orden mayor}, donde $f_m \neq 0$ y $m > 1$. Si $m = 2$ decimos que p es un *punto doble*.

Si escribimos

$$f_m(x - a, y - b) = \prod L_i^{r_i}$$

donde cada L_i es un polinomio lineal en $x - a$ y $x - b$ con coeficientes en $\overline{k}$, decimos que las líneas $L_i = 0$ son las *líneas tangentes* a C en p, y r_i la multiplicidad de L_i. El punto p es una *singularidad ordinaria* si las líneas tangentes son todas distintas, i.e., $r_i = 1$; y decimos que un punto ordinario doble es un *nodo*. Un punto doble es una *cúspide*, si sólo hay una línea tangente por este punto, i.e., si $r_2 = 2$.

Ahora estudiemos el caso proyectivo. Definimos el plano proyectivo sobre k como

$$\mathbb{P}_k^2 = \{(x, y, z) \in k^3 : (x, y, z) \neq 0\}/\sim$$

donde $(x, y, z) \sim (x', y', z')$ si y sólo si existe un $c \in k^* = k - \{0\}$ tal que $(x', y', z') = (cx, cy, cz)$. Escribimos $[x, y, c]$ para la clase de equivalencia de (x, y, z). Así $\mathbb{P}^2_k = \{[x, y, z] | (x, y, z) \in k^3\}$.

Un polinomio homogéneo no constante $F \in k[x, y, z]$ que no tenga factores repetidos en $\overline{k}[x, y, z]$ define una curva proyectiva plana C_F sobre k cuyos puntos en cualquier campo $K \supset k$ están dados por el subconjunto de $\mathbb{P}^2_K$):

$$C_F(K) = \{[x, y, z] | F(x, y, z) = 0\}.$$

Debido a que el polinomio es homogéneo, podemos notar que este conjunto está bien definido. Llamaremos *grado de la curva*, al grado del polinomio F (o el grado de f para el caso afín). De manera análoga al caso afín, la curva es unión de curvas planas irreducibles.

Sean $U_0 = \{[x, y, z] \in \mathbb{P}^2_k | x \neq 0\}$, $U_1 = \{[x, y, z] \in \mathbb{P}^2_k | y \neq 0\}$ y $U_2 = \{[x, y, z] \in \mathbb{P}^2_k | z \neq 0\}$; entonces tenemos que

$$\mathbb{P}^2_k = U_0 \cup U_1 \cup U_2$$

y para una curva $C = C_F$

$$C = C_0 \cup C_1 \cup C_2 \text{ donde } C_i = C \cap U_i,$$

además podemos identificar a U_0 (de hecho a cada U_i) con el plano afín vía el mapeo $[1, y, z] \longrightarrow (x, y)$ (o el equivalente), por lo que decimos que el plano proyectivo está cubierto por planos afines. Más aún, podemos identificar a C_0, C_1, C_2 con las curvas afines dadas por los polinomios

$$F(1, y, z), F(x, 1, z), F(x, y, 1)$$

respectivamente. Con esto podemos decir que la curva plana proyectiva C_F está cubierta por las tres curvas afines C_0, C_1, C_2 aunque en algunos casos sólo está cubierta por dos de éstas (ver [Mil96]).

Consideremos que k es un campo perfecto, por ejemplo $R = \mathbb{Z}$ y $k = \mathbb{Q}$, y tomemos una curva afín C_f definida sobre k (lo que denotaremos por C/k) y además tomemosla geométricamente irreducible. Si K es una extensión de Galois de k, y $f = \sum a_{ij} x^i y^j \in k[x, y]$, tenemos que si un punto $(a, b) \in C_f$, entonces también $\sigma(a, b) \in C_f$, donde $\sigma \in \mathrm{Gal}(K/k)$. En efecto:

$$0 = \sigma f(a, b) = \sigma\left(\sum a_{ij} x^i y^j\right) = \sum a_{ij} (\sigma a)^i (\sigma b)^j \quad f(\sigma a, \sigma b)$$

Por lo que $\mathrm{Gal}(K/k)$ actúa en $C(K)$. Más generalmente, si $C_1, C_2, \ldots$ son curvas sobre k, entonces $\mathrm{Gal}(K/k)$ estabiliza al conjunto $\cap_i C_i$, por lo que si tomamos a f junto con sus derivadas parciales, $\mathrm{Gal}(K/k)$ estabiliza al conjunto de puntos singulares de C_f. Análogamente podemos trabajar con curvas proyectivas planas y obtendremos el mismo resultado.

Tenemos especial interés en estudiar a las curvas cúbicas no singulares, ya que en ellas podemos definir una estructura de grupo sobre sus puntos. Consideremos los siguientes lemas:

Lema 2.1.1. *Si C/k tiene un punto singular, entonces tiene uno en $C(k)$, y si C es una cúbica, éste es el único punto singular.*

Demostración. Supongamos que $p \in C(E)$ donde E es una extensión de k. Notemos que basta suponer que la curva es afín, ya que la curva proyectiva está cubierta por curvas afines. Consideremos el ideal $I =< f, \partial f/\partial x, \partial f/\partial y >$. Como ideal de $E[x,y]$, $I = I_E \neq < 1 >$ ya que sus generadores tienen a p como raíz, esto implica que el ideal $I = I_{\overline{k}}$ visto como ideal de $\overline{k}[x,y]$ también es diferente de $< 1 >$ ya que si

$$I_{\overline{k}} = < 1 > \implies I_k = < 1 > \implies I_E = < 1 > .$$

Por lo tanto, usando el Nullstellensatz, tenemos que I también tiene un cero en $\overline{k}$; es decir, hay un punto singular q en $C(\overline{k})$ y, por lo tanto, en una extensión finita de k que además la podemos suponer normal (se puede tomar la cerradura normal) y, por consecuencia, es de Galois. Para ver que el punto q es el único punto singular, supongamos que existe otro r, entonces la recta que une a estos dos puntos se intersecta con la curva en al menos 4 puntos contando las multiplicidades, lo que contradice el teorema de Bezout[1] Así, como el grupo de Galois $\mathrm{Gal}(E/k)$ estabiliza a los puntos singulares, fija a q, pero éste sólo fija a los puntos de k, concluimos que $q \in C_k$. □

[1]El teorema de Bezout dice que si C_f y D_g son curvas proyectivas de grados m y n y además asumimos que no tienen una componente en común, entonces ellas se intersectan, sobre $\overline{k}$, en exactamente mn puntos contando multiplicidades; o bien

$$mn = \sum_p I(p, C_f \cap D_g)$$

donde la suma es sobre todos los puntos en $\mathbb{P}^2_{\overline{k}}$, y donde definimos $I(p, C_f \cap D_g) = 0$ si $p \notin C_f \cap D_g$; y si $p \in C_f \cap D_g$ entonces $I(p, C_f \cap D_g)$ es la multiplicidad de p en la intersección, definida como el número $\dim_{\overline{k}} \overline{k}[x,y]/(f,g)$.

Con este lema y el teorema de Bezout, vemos que si C tiene un punto singular, podemos parametrizar a los puntos de de la curva con las rectas por el punto singular (posiblemente salvo un número finito).

2.2 La ley de grupo

Ahora veamos que si C es cúbica no singular, podemos definir una suma sobre los puntos $C(K)$. Nuestro objetivo es ilustrar esta suma y su manera de operar, así como saber que $C(K)$ resulta un grupo. Sin embargo, para un tratamiento más delicado de este hecho, así como para una demostración, se pueden revisar los libros [Sil85], [Ful69] entre otros.

Tomemos dos puntos $p, q \in C(K)$. Por el teorema de Bezout, la línea que une a p y q intersecta en exactamente un punto más a C que denotaremos por pq y que también tiene coordenadas en K. Fijemos un punto 0 en $C(K)$ quien servirá como origen. Definimos

$$p + q := 0(pq),$$

es decir, el punto resultante de la suma entre p y q es el otro punto de intersección de la recta por 0 y por pq con C. Es necesario precisar algunos casos particulares tales como: Si $p = q$ entonces pp es el punto de intersección de la tangente por p con la cúbica; si la línea por p y q es tangente a la curva en q, entonces $pq = q$; y si p es un punto de inflexión, entonces $pp = p$.

Teorema 2.2.1. *Tenemos que $C(K)$, junto con la suma anterior, forma un grupo abeliano.*

Aquí daremos una demostración para el caso $k = \overline{k}$. Una demostración general se puede encontrar en [Ful69]

Sea C_F una curva proyectiva no singular sobre el campo k.

Definición 2.2.2. El Grupo de *divisores* $\mathrm{Div}(C)$ en C es el grupo abeliano libre generado por los elementos de $C(\overline{k})$. Entonces un elemento de $\mathrm{Div}(C)$ es una suma finita

$$D = \sum n_p[p], \qquad n_p \in \mathbb{Z} \qquad p \in C(\overline{k}).$$

El *grado* de D es $\sum n_p$

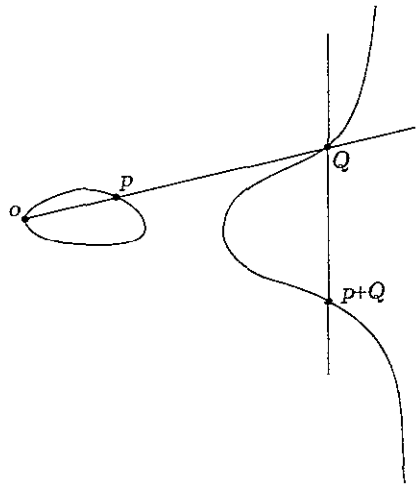


Figura 2.1: En esta figura se muestra cómo se suman dos puntos en una cúbica.

Tenemos un orden parcial en $\mathrm{Div}(C)$ de la siguiente manera:

$$\sum n_p[p] \leq \sum m_p[p] \iff \sum n_p \leq \sum m_p \text{ para todo } p.$$

Sea ϕ un mapeo racional en C. Por definición ϕ es un cociente $\frac{G(x,y,z)}{H(x,y,z)}$ de dos polinomios homogéneos del mismo grado, digamos de grado m, y además F no divide a H. Si $\phi \neq 0$, podemos suponer que F tampoco divide a G.

Por el teorema de Bezout, tenemos que:

$$(\deg F)m = \sum_p I(p, C_F \cap C_G) = \sum_p I(p, C_F \cap C_H).$$

Definimos el divisor asociado a ϕ como:

$$\mathrm{div}\phi = \sum_p I(p, C_F \cap C_G)[p] - \sum_p I(p, C_F \cap C_H)[p].$$

Los p que aparecen en $\mathrm{div}\phi$ con coeficientes positivos son llamados *ceros* y los que aparecen con coeficientes negativos *polos*. Notemos que $\mathrm{div}\phi$ tiene grado cero, por lo que tiene el mismo número de ceros que de polos contando multiplicidades. También notemos que las únicas funciones que no tienen ni ceros ni polos son las constantes.

Dado un divisor D, definimos

$$L(D) = \{\phi | \text{div}\phi + D \geq 0\} \cup \{0\}.$$

De tal manera que si $D = [p] + 2[q]$, entonces $L(D)$ está formado por todos los mapeos racionales que no tienen polos diferentes de p, q y que tienen a lo más un polo simple en p y un polo doble en q. Cada $L(D)$ es un k-espacio vectorial de dimensión finita (ver siguiente teorema) misma que denotaremos por $l(D)$.

Teorema 2.2.3 (Riemann-Roch). *Existe un entero g tal que para todos los divisores D*

$$l(D) \geq \deg D + 1 - g,$$

con igualdad para $\deg D > 2g - 2$.

Una demostración de este famoso teorema se puede encontrar el el libro de Fulton [Ful69].

Definición 2.2.4. Definimos el *género* de la curva C como el entero g del teorema anterior.

Definición 2.2.5. Al divisor de un mapeo racional lo llamaremos *principal* y al conjunto de divisores principales de C lo denotamos $P(C)$ Decimos que dos divisores D, D' son linealmente equivalentes $D \sim D'$ si difieren por un divisor principal.

Si denotamos por $\text{Div}^0(C)$ a los divisores de grado cero en C, tenemos

$$\text{Div}(C) \supset \text{Div}^0(C) \supset P(C).$$

Definición 2.2.6. Definimos los grupos de Picard

$$\text{Pic}(C) = \text{Div}(C)/P(C) \qquad \text{Pic}^0(C) = \text{Div}^0(C)/P(C).$$

Consideremos una curva proyectiva de género 1. De acuerdo al teorema de Riemann-Roch

$$l(D) = \deg D \quad \text{si, y sólo si,} \quad \deg D \geq 1$$

Proposición 2.2.7. *Sea C una curva proyectiva no singular de género 1, y sea $O \in C(k)$ donde $k = \overline{k}$. El mapeo*

$$C(k) \longrightarrow \mathrm{Pic}^0(C), \quad p \longmapsto [p] - [O]$$

es biyectivo.

Demostración. Definamos un inverso. Sea D un divisor de grado cero. Entonces $D + [0]$ tiene grado 1 y, por lo tanto, existe un mapeo racional ϕ, único salvo multiplicación por constantes. tal que $\mathrm{div}\phi + D + [0] \geq 0$. Los únicos divisores mayores o iguales al divisor cero de grado uno, son los puntos. Es decir, los de la forma $[p]$. Por lo que existe un punto bien definido $p \in C(k)$ tal que $D + [0] \sim [p]$, o bien, $D \sim [p] - [0]$. □

Esta biyección canónica nos dota a $C(k)$ de una estructura de grupo abeliano (con la suma $\oplus$) que, como veremos en seguida, es la misma definida anteriormente. En efecto, notemos que esta nueva estructura está determinada por la condición:

$$p \oplus q = s \text{ si, y sólo si, } [p] + [q] = [s] + [0].$$

Supongamos que $p + q = s$ (con la suma anterior). Sea l_1 la línea por p y q, y l_2 la línea por 0 y s. Por la definición de s sabemos que l_1 y l_2 tienen un punto en común r con C. Si vemos a estas líneas como funciones lineales en las variables x, y, z, y hacemos $\phi = l_1/l_2$, entonces ϕ tiene ceros en p, q, r y polos en $0, s, r$ y por lo tanto

$$\mathrm{div}\phi = [p] + [q] + [r] - [0] - [s] - [r] = [p] + [q] - [s] - [0]$$

con lo que $[p] + [q] \sim [0] + [s]$, y $p \oplus q = s$ según la nueva estructura.

Con esto nos queda ya una buena idea de cuál es la manera de demostrar que, en general, $C(K)$ es un grupo con la estructura inicial. Si se quiere revisar la demostración completa, es recomendable revisar el libro de [Sil85].

2.3 Curvas elípticas

Definición 2.3.1. Definimos el *género geométrico* de una curva plana proyectiva C como el número:

$$P_g(C) = \frac{(d-1)(d-2)}{2} - \sum \delta_p;$$

donde d es el grado de C. la suma es sobre todos los puntos singulares $p \in C(\bar{k})$. y $\delta_p = m_p(m_p-1)/2$ si p es una singularidad ordinaria de multiplicidad m_p.

Definición 2.3.2. Sea K un campo. Una *curva elíptica* sobre K es cualquiera de las siguientes:

1. Una curva E sobre K completa y no singular de género 1 junto con un punto $0 \in C(K)$.
2. Una curva proyectiva plana E de grado 3 junto con un punto $0 \in E(K)$.
3. Una curva proyectiva no singular de la forma

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Estas definiciones están relacionadas. En efecto, Sea E como en 3, entonces $E(K)$ contiene un punto canónico $0 = [0, 1, 0]$, y el par $(E, 0)$ satisface las otras dos definiciones: la 2 es inmediata y la 1 se sigue de la fórmula para el género geométrico. Si tomamos $(E, 0)$ como en 1, se puede ver que existe un isomorfismo de E sobre una curva como en 3 mandando 0 en $[0, 1, 0]$ Si $(E, 0)$ es como en 2, también es posible demostrar que hay un cambio de variables que transforma E en una curva como en C y a 0 en $[0, 1, 0]$ (ver [Sil85]).

Definición 2.3.3. A la ecuación

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{2.1}$$

que determina a la curva elíptica E, la llamamos la *ecuación de Weierstrass* de la curva.

Se demuestra que si una curva elíptica está dada por dos ecuaciones del tipo 2.1, entonces existe un cambio de coordenadas del tipo

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

con $u, r, s, t \in K$ y $u \neq 0$ y si suponemos que la característica del campo K es diferente de 2 o 3, podemos hacer el cambio de variables

$$x' = x, \quad y' = y + \frac{a_1}{2}x, \quad z' = z.$$

para eliminar al término xyz, y un con un cambio más por

$$x' = x, \quad y' = y + \frac{a_3}{2}, \quad z' = z$$

eliminaremos los términos x^2 y y. Así, finalmente llegaremos a una ecuación de la forma

$$E(a,b) := y^2z = x^3 + axz^2 + bz^3. \tag{2.2}$$

El siguiente teorema muestra la importancia de las ecuaciones del tipo 2.2. Una demostración de estos hechos se puede encontrar en [Sil85].

Teorema 2.3.4. *Asumamos que el campo K tiene característica diferente de 2 o 3.*

- *La curva $E(a,b) := y^2z = x^3 + axz^2 + bz^3 \quad a, b \in K$ es no singular y, por lo tanto, junto con el punto $0 = [0,1,0]$ define una curva elíptica.*
- *Cada curva elíptica sobre K es isomorfa a una de la forma $E(a,b)$.*
- *Dos curvas elípticas $E(a,b)$ y $E(a',b')$ son isomorfas si, y sólo si, existe un $c \in K^*$ tal que $a' = c^4a$, $b' = c^6b$ y entonces el isomorfismo está dado por*

$$[x,y,z] \longrightarrow [c^2x, c^3y, z].$$

Respecto a la ley de grupo de una curva elíptica dada por $E(a,b)$, podemos decir que el punto al infinito es el elemento cero y que la ley de grupo está determinada por:

$$p + q + r = 0 \iff p, q, r \text{ están en la misma línea recta}$$

y que

$$\text{si } \; p = [x,y,z] \text{ entonces } \quad -p = [x,-y,z],$$

de donde vemos que un punto de orden dos ($-p = p$) es de la forma $[x,0,1]$ donde x es raíz del polinomio $x^3 + ax + b$.

Ahora estudiemos los morfismos entre curvas elípticas.

Definición 2.3.5. Sean E_1 y E_2 dos curvas elípticas. Una *isogenea* entre E_1 y E_2 es un morfismo (mapeo polinomial de curvas)

$$\psi : E_1 \longrightarrow E_2$$

que satisface la condición $\psi(0) = (0)$. Las curvas E_1 y E_2 son *isogeneas* si existe una isogenea no cero ($\psi(E_1) \neq \{0\}$) entre ellas.

El siguiente teorema muestra la importancia de las isogeneas ya que muestra que éstas conservan la estructura de grupo.

Teorema 2.3.6. Sea

$$\psi : E_1 \longrightarrow E_2$$

una isogenea. Entonces

$$\psi(p+q) = \psi(p) + \psi(q) \quad \text{para todo } p, q \in E_1.$$

Demostración. Ver [Sil85]. □

Fijemos la siguiente notación que usaremos durante el resto del capítulo, salvo especificación.

Por K denotaremos un campo local respecto a la valuación v con anillo de enteros $R = \{x \in K : v(x) \geq 0\}$. Por $\mathcal{M}$ al ideal máximo de R dado por $\{x \in K : v(x) > 0\}$. Por π al parámetro uniformizador de R, i.e., $\mathcal{M} = \pi R$. Finalmente denotaremos por k al campo de residuos de R, es decir, $k = R/\mathcal{M}$.

Además supondremos que la valuación cumple con que $v(\pi) = 1$.

Definición 2.3.7. Sea E/K una curva elíptica con ecuación de Weierstrass

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Definimos el discriminante Δ de la curva elíptica como el número

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

donde

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

Cuando la curva elíptica está dada por una ecuación de la forma

$$E : y^2z = x^3 + axz^2 + bz^3,$$

entonces $\Delta = -16(4a^3 + 27b^2)$ ([Sil85]).

Dada una curva, aunque no sea elíptica, podemos asociarle su discriminante ([Sil85]). Sin embargo una curva es una curva elíptica si'y sólo si $\Delta \neq 0$.

Sea E/K una curva elíptica con ecuación de Weierstrass

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Si hacemos la substitución $[x, y, z] \longrightarrow [u^{-2}x, u^{-3}y, z]$ cada a_i se transforma en u^ia_i, por lo que, si escogemos a u como una potencia suficientemente grande de π tenemos que podemos encontrar una ecuación de Weierstrass con todos los coeficientes en R y, por lo tanto, $v(\Delta) \geq 0$ y entonces podemos escoger una ecuación tal que $v(\Delta)$ sea lo más pequeño posible.

Definición 2.3.8. Sea E/K una curva elíptica. Una ecuación de Weierstrass con las condiciones del párrafo anterior es llamada *ecuación minimal* de Weierstrass de la curva elíptica.

Teorema 2.3.9. Se cumple que:

- Cada curva elíptica tiene una ecuación minimal de Weierstrass.
- Una ecuación minimal de Weierstrass es única salvo por cambio de coordenadas

$$x = u^2x' + r \qquad y = u^3y' + su^2x' + t \qquad z = z'$$

con $r, s, t \in R$ y $u \in R^*$.

Ahora definamos una operación de "reducción módulo π" a la que denotaremos por una tilde. Así por ejemplo, el mapeo natural de reducción $R \longrightarrow R/\pi R = k$ es denotado por $t \longmapsto \bar{t}$.

Teniendo una ecuación minimal de Weierstrass para la curva elíptica E/K, podemos reducir sus coeficientes módulo π para obtener una curva

sobre k (que podría ser singular). A esta curva la denotaremos por $\tilde{E}/k$ y la llamaremos la *reducción de E módulo π*.

$$\tilde{E} : y^2z + \tilde{a}_1xyz + \tilde{a}_3yz^2 = x^3 + \tilde{a}_2x^2z + \tilde{a}_4xz^2 + \tilde{a}_6z^3$$

Debido a que iniciamos con una ecuación minimal, la ecuación de $\tilde{E}$ es única salvo el cambio de coordenadas del teorema 2.3.9.

Si $p \in E(K)$, podemos encontrar coordenadas homogéneas de $p = [x_0, y_0, z_0]$ donde cada $x_0, y_0, z_0 \in R$ y donde al menos una es diferente de cero. Definimos el punto reducido $\tilde{p} = [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0]$ que está en $\tilde{E}(k)$. Esto nos da un mapeo de reducción

$$\begin{aligned} E(K) &\longrightarrow \tilde{E}(k) \\ p &\longmapsto \tilde{p}. \end{aligned}$$

Definición 2.3.10. Sea E/K una curva elíptica y sea $\tilde{E}$ su reducción para una ecuación minimal. Decimos que:

- E tiene *buena reducción (estable)* sobre K, si $\tilde{E}$ es no singular.
- E tiene *reducción multiplicativa (semi estable)* si $\tilde{E}$ tiene un nodo.
- E tiene *reducción aditiva (inestable)* si $\tilde{E}$ tiene una cúspide.

En los casos 2 y 3 también decimos que E tiene *mala reducción*.

Proposición 2.3.11. *Sea E/K una curva elíptica con ecuación minimal de Weierstrass*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

E tiene buena reducción si y sólo si $v(\Delta) = 0$. En este caso $\tilde{E}$ es una curva elíptica

Ejemplo 2.3.12. Sea $q \geq 5$ un número primo. La curva elíptica (en su parte afín)

$$E_1 : y^2 = x^3 + qx^2 + 1$$

tiene buena reducción sobre $\mathbb{Q}_q$ mientras que

$$E_2 : y^2 = x^3 + x^2 + q$$

tiene reducción multiplicativa sobre $\mathbb{Q}_q$,

$$E_3 : y^2 = x^3 + q$$

tiene reducción aditiva sobre $\mathbb{Q}_q$.

Capítulo 3

Esquemas

Con el objetivo de fijar notación, iniciamos este capítulo con las primeras definiciones en la teoría de esquemas. Después introduciremos una familia de esquemas en la que estamos particularmente interesados: Los S-esquemas o bien, los esquemas con base S. Estudiaremos al producto fibrado, construcción que nos permitirá dar las generalizaciones o las extensiones de las propiedades de las curvas elípticas a algunos esquemas. Se analizaran conceptos tales como propiedad, suavidad y regularidad que son características necesarias para la teoría de los modelos de Nèron

3.1 Espacios anillados y localmente anillados

Un *espacio anillado* es un espacio topológico X junto con una gavilla de anillos $\mathcal{O}_X$.

Decimos que $(X, \mathcal{O}_X)$ es *localmente anillado* si para todo $x \in X$ la fibra $\mathcal{O}_x$ en x de la gavilla $\mathcal{O}_X$ es un anillo local. Denotaremos por M_x su ideal máximo y por $k(x)$ al campo residual $\mathcal{O}_x/M_x$.

Si U es un abierto de X denotaremos por $\Gamma(U, \mathcal{O}_X)$ al anillo de secciones de $\mathcal{O}_X$ sobre U y para todo $x \in U$, $f_x \in \mathcal{O}_x$ es el *germen* de f en x. Denotemos por $f(x)$ a la imagen de f_x en el campo residual $k(x)$.

Un homomorfismo de espacios anillados $(X, \mathcal{O}_X)$ y $(Y, \mathcal{O}_Y)$ es una pareja $(f, f^{\#})$ donde f es una aplicación continua de X en Y y donde $f^{\#}$ es un morfismo de gavillas de $\mathcal{O}_Y$ en $f_*(\mathcal{O}_X)$, donde $f_*(\mathcal{O}_X)$ denota la gavilla *imagen*

directa bajo f de $\mathcal{O}_X$ definida por

$$\Gamma(V, f_*(\mathcal{O}_X)) := \Gamma(f^{-1}(V), \mathcal{O}_X).$$

Si además $(X, \mathcal{O}_X)$ y $(Y, \mathcal{O}_Y)$ son localmente anillados, pedimos que el homomorfismo inducido por $f^\#$ sobre las fibras, $f_x^\# : \mathcal{O}_{f(x)} \to \mathcal{O}_x$ sea local, es decir que $M_{f(x)} = (f^\#)_x^{-1}(M_x)$.

Para simplificar la notación, desde ahora denotaremos simplemente por f, al morfismo de espacios anillados $(f, f^\#)$.

3.2 Esquemas

Sea R un anillo. Construyamos un espacio anillado $(\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$ de la siguiente manera:

- El conjunto asociado a $\operatorname{Spec} R$ es el conjunto de los ideales primos de R.

- La topología de $\operatorname{Spec} R$, llamada *topología de Zariski*, es definida por sus cerrados: si $p \in \operatorname{Spec} R$ y si $f \in R$, denotamos por $f(p)$ a la imagen de f en el campo de residuos de R_p. Así, decir que $f(p) = 0$ es equivalente a que $f \in p$. Decimos que $F \subset \operatorname{Spec} R$ es cerrado, si existe un subconjunto M de R tal que F sea el conjunto de ceros de M, es decir, $F = V(M) := \{p : f(p) = 0 \ \forall\ f \in M\} = \{p : M \subset p\}$. De esto tenemos que la familia de conjuntos de la forma

$$D(f) := \{p \in \operatorname{Spec} R | f(p) \neq 0\} = \{p \in \operatorname{Spec} R | f \neq p\}$$

es una base para los abiertos de $\operatorname{Spec} R$.

Proposición 3.2.1. *Se cumple lo siguiente:*

1. $D(f) = \emptyset \Leftrightarrow f$ *es nilpotente.*
2. *Una familia de abiertos* $\{D(f_i)\}_{i \in I}$ *es una cubierta de* $\operatorname{Spec} R$ *si y solamente si el ideal generado por las* f_i *es el total* R. *En particular* $D(f) = \operatorname{Spec} R$ *si y sólo si* f *es una unidad.*
3. $D(f) \cap D(g) = D(fg)$. *En particular* $D(f^n) = D(f)$.

4. $D(g) \subset D(f)$ *si y sólo si* $g \in \sqrt{(f)}$ ($\sqrt{(f)}$ *es el ideal radical del ideal* (f), *es decir, la intersección de todos los ideales primos que contienen a* f).

La demostración de estos hechos es consecuencia directa de la definición.

Observación 3.2.2. Observemos que si $D(f) \subset D(g)$, entonces podemos escoger g de manera que éste sea un múltiplo de f. En efecto, por la parte 4 de la proposición, tenemos que existe un entero n tal que $g^n = ff'$ pero sabemos que $D(g^n) = D(g)$. Por otro lado, el abierto $D(f)$ se identifica, junto con su topología, con el espacio Spec R_f ([Har77]).

- Ahora construyamos la gavilla estructural de Spec R. Para eso, asociemos a cada abierto básico no vacío $D(f)$ el anillo R_f. De la propiedad 4 y la observación deducimos que si $D(g) \subset D(f)$ tenemos un morfismo canónico $R_f \to R_g = R_{ff'} = (R_f)_{f'}$ y si $D(f) = D(f')$, entonces R_f se identifica canónicamente con $R_{f'}$. Esta construcción la podemos extender a una pregavilla en Spec R haciendo para cada abierto $U \in \text{Spec } R$

$$\Gamma(U, \mathcal{O}_{\text{Spec } R}) = \varprojlim_{D(f) \subset U} R_f$$

(ver [Har77] para los detalles). Sabemos que esta pregavilla es una gavilla si y solamente si para todo recubrimiento de todo abierto $D(f)$ por los $D(ff')$ se tiene que la sucesión siguiente es exacta

$$0 \longrightarrow R_f \xrightarrow{\psi} \prod_i R_{ff_i} \xrightarrow{\phi} \prod_{i,j} R_{ff_if_j}$$

donde $\psi(a)_i$ es la imagen canónica de a en $R_{ff_i} = (R_f)_{f_i}$, y $\phi(a_i)_{ij}$ es la diferencia de las imágenes canónicas de a_i y a_j en $R_{ff_if_j}$.

Notemos que para todo punto $p \in R$, la fibra es el anillo local R_p ya que

$$\mathcal{O}_{\text{Spec } R,p} = \varinjlim_{f \notin p} R_f = R_p.$$

Notemos que con lo anterior

$$\Gamma(\text{Spec } R, \mathcal{O}_{\text{Spec } R}) \quad A$$

Definición 3.2.3. Un *esquema afín* es un espacio anillado isomorfo al espectro de un anillo.

Sea $(X, \mathcal{O}_X)$ un espacio localmente anillado. Decimos que éste es un *esquema* si es localmente isomorfo a un esquema afín.

Proposición 3.2.4. *Si $(X, \mathcal{O}_X)$ es un esquema y U es un abierto de X, $(U, \mathcal{O}_X|U)$ es un esquema.*

Demostración. ver [Har77] □

Definición 3.2.5. Un *subesquema abierto* de un esquema X es un esquema U, cuyo espacio topológico es un abierto del espacio X, y cuya gavilla $\mathcal{O}_U$ es isomorfa a la gavilla restricción $\mathcal{O}_X|_U$ de la gavilla estructural de X. Una *inmersión abierta* es un morfismo $f : X \longrightarrow Y$ que induce un isomorfismo de X con un subesquema abierto de Y.

Definición 3.2.6. Una *inmersión cerrada* es un morfismo $f : X \longrightarrow Y$ de esquemas tal que f induce un homeomorfismo del espacio topológico X en un conjunto cerrado del espacio topológico Y y que además el morfismo inducido $f^\sharp : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ de gavillas en Y sea suprayectivo. Un *subesquema cerrado* de X es una clase de equivalencia de inmersiones cerradas, donde decimos que $f : X \to Y$ y $f' : X' \to Y$ son equivalentes si existe un isomorfismo $i : X' \to X$ tal que $f' = f \circ i$.

Ejemplo 3.2.7. Si X es el esquema afín Spec A y Y es Spec A/I donde I es un ideal de A, tenemos que el morfismo canónico $A \longrightarrow A/I$ induce un morfismo de esquemas $f : Y \longrightarrow X$ que es una inmersión cerrada. En efecto, el mapeo f es un homeomorfismo entre Y y el cerrado $V(I) \subset X$. El mapeo de las gavillas es suprayectivo ya que el mapeo en los tallos, que son las localizaciones de A y A/I respectivamente, es suprayectivo ([Har77]). Así, para cada ideal $I \subset A$ tenemos una estructura de esquema cerrado sobre $V(I)$. Notemos que cada cerrado Y de X puede tener muchas estructuras de esquema, al menos una para cada ideal $I \subset A$ tal que $V(I) = Y$ y de hecho, cada estructura de subesquema cerrado proviene de un ideal (ver [Har77]).

Ejemplo 3.2.8. Sea V una variedad afín sobre el campo K, y sea W una subvariedad cerrada. Tenemos que W está en correspondencia con con un

ideal primo P del anillo de coordenadas A de V. Sea $X = \operatorname{Spec} A$ el esquema asociado a V y $Y = \operatorname{Spec} A/P$ el esquema asociado a W, entonces Y es un subesquema cerrado de X.

Ahora definamos a los esquemas espacio afín y proyectivo sobre un anillo.

Definición 3.2.9. Sea R un anillo. Definimos el n-espacio afín sobre R $\mathbb{A}^n_R$ como

$$\mathbb{A}^n_R := \operatorname{Spec} R[x_1, x_2, \ldots, x_n].$$

Si $R = k$ donde k es un campo algebraicamente cerrado, vemos que los puntos cerrados de $\mathbb{A}^n_k$ están en correspondencia biyectiva con las n-adas de elementos en k.

Para construir el espacio proyectivo necesitamos introducir una manera de crear nuevos esquemas: el pegado de esquemas.

Sea X_i una familia de esquemas tales que para cada $i \neq j$ tenemos un abierto $U_{ij} \subset X_i$ que es un esquema con la gavilla restricción. También supongamos que tenemos un isomorfismo de esquemas $\phi_{ij} : U_{ij} \to U_{ji}$ para $i \neq j$ tal que

$$\phi_{ji} = \phi_{ij}^{-1} \text{ y que para cada } i, j, k \quad \phi_{ij}(U_{ij} \cap U_{ik}) = U_{ji} \cap U_{jk},$$

y que

$$\phi_{ik} = \phi_{jk} \circ \phi_{ij} \quad \text{en} \quad U_{ij} \cap U_{ik}.$$

Construyamos el esquema X resultante de pegar a los esquemas X_i de la siguiente manera. Tomemos a X como la unión ajena de los X_i módulo una relación de equivalencia

$$X = \bigcup_i X_i / \sim$$

donde $x_i \in U_{ij} \subset X_i$ está relacionado con $\phi_{ij}(x_i)$ para todo j (si $x_i \neq U_{ij}$ entonces lo relacionamos consigo mismo). Sean $\psi_i : X_i \to X$ los morfismos canónicos. Tenemos que X es un espacio topológico con la topología cociente, es decir, $V \subset X$ es abierto si, y sólo si, $\psi_i^{-1}(V) \subset X_i$ es abierto para todo i. Definimos la gavilla en X como

$$\Gamma(V, \mathcal{O}_X) := \left\{ \prod_i s_i \quad s_j \in \Gamma(\psi_j^{-1}(V), \mathcal{O}_{X_j}), \psi_{ij}(s_i|_{\psi_i^{-1}(V) \cap U_{ij}}) \quad s_j|_{\psi_j^{-1}(V) \cap U_{ji}} \right\}.$$

Tenemos que $\mathcal{O}_X$ es una gavilla y que $(X, \mathcal{O}_X)$ es un espacio localmente anillado. Más aún, como cada X_i es un esquema, cada punto de X tiene una vecindad que es afín, por lo que X también es un esquema ([Har77] o [EH99]).

Ahora sí podemos definir al espacio proyectivo.

Sea $S = R[x_0, x_1, \dots x_n]$ el anillo de polinomios en $n+1$ variables con coeficientes en el anillo R. Sea $A_i := [S_{(x_i)}]_0$ la componente homogénea de grado cero del anillo local $S_{(X_i)}$, es decir,

$$A_i = \left\{ \frac{F(x_0, x_1, \dots x_n)}{x_i^{\deg F}} \mid F \text{ es homogéneo} \right\} \cong R[y_0, y_1, \dots, \hat{y_i}, \dots y_n]$$

donde el $\hat{y_i}$ indica que se está suprimiendo la variable y_i. Sea $X_i = \operatorname{Spec} A_i$, tenemos que el anillo

$$A_{ij} := (A_i)_{x_i/x_j}$$

se identifica canónicamente con A_{ji}. Así, tenemos que $U_{ij} = \operatorname{Spec} A_{ij}$ se identifica canónicamente con $U_{ji} = \operatorname{Spec} A_{ji}$ además, módulo una identificación (inmersión abierta), podemos considerar a U_{ij} abierto de X_i.

Definición 3.2.10. Definimos el n-espacio proyectivo sobre R, $\mathbb{P}^n_R$ como el esquema resultante de pegar por los U_{ij} a los esquemas X_i definidos anteriormente.

Alternativamente, podemos hacer la siguiente definición.

Definición 3.2.11. Sea R un anillo. Definimos el n-espacio proyectivo sobre R, $\mathbb{P}^n_R$ como

$$\operatorname{Proj} R[x_0, x_2, \dots, x_n]$$

donde $\operatorname{Proj} R[x_0, x_2, \dots, x_n]$ denota al conjunto de todos los ideales primos homogéneos de grado positivo del anillo $R[x_0, x_2, \dots, x_n]$.

Para ver la equivalencia y los detalles, revisar el libro de Hartshorne [Har77] o el de Eisenbud-Harris [EH99]

3.3 Propiedades básicas

Sea $X = \operatorname{Spec} R$ un esquema afín. Sea B un subconjunto de X. Definimos la cerradura $\overline{B}$ de B, de manera tradicional, es decir,

$$\overline{B} = \bigcap \{F \subset X : B \subset F \text{ y } F \text{ es cerrado}\} = V(B).$$

Así, si $x, y \in X$ tenemos que:

$$y \in \overline{\{x\}} \text{ en } \operatorname{Spec} R \iff x \subset y \text{ en } R$$

.

Proposición 3.3.1. *Un esquema es un espacio T-cero, es decir, dados dos puntos distintos en un esquema X existe un abierto que sólo contiene a uno de estos puntos.*

Demostración. Si $X = \operatorname{Spec} R$ tenemos que si $y \notin \overline{\{x\}}$, entonces el abierto $X - \overline{\{x\}}$ resuelve el problema. si $y \in \overline{\{x\}}$ y $x \in \overline{\{y\}}$ entonces $x \subset y$ y $y \subset x$ por lo que $x = y$.

Si X no es afín, entonces existe un abierto afín U que contiene a x. Si $y \notin U$, el problema está resuelto, pero si $y \in U$, entonces pasamos al caso anterior. □

Proposición 3.3.2. *Un esquema afín $X = \operatorname{Spec} A$ es compacto.*

Demostración. Sea $(U_i)_{i \in I}$ una cubierta abierta de X como cada U_i es complemento de un cerrado, éstos están definidos por conjuntos $M_i \subset A$ de la siguiente manera:

$$U_i = \{p \in X : \exists\ f \in M_i,\ f(p) \neq 0\}.$$

Decir que los U_i cubren X es equivalente a decir que los conjuntos M_i generan al anillo A, por lo que existe un número finito de $m_j \in M_j$ tales que $1 = \sum m_j a_j$ y, por lo tanto, los U_j asociados a estos $m_j \subset M_j$ también cubren X. □

Definición 3.3.3. Decimos que un espacio topológico es irreducible, si no puede ser escrito como unión de dos cerrados propios, es decir,

X $\quad Z_1 \cup Z_2$ con Z_1 y Z_2 cerrados propios, entonces Z_1 o Z_2 $\quad X$

Ejemplo 3.3.4. La cerradura de un punto en un espacio topológico siempre es un subespacio irreducible.

Sabemos que el conjunto de subconjuntos irreducibles de un espacio topológico ordenado por inclusión tiene máximos.

Definición 3.3.5. Los subconjuntos irreducibles máximoes son llamados *componentes irreducibles.* Estas son cerradas ya que la cerradura de un irreducible es nuevamente irreducible.

Proposición 3.3.6. *Un abierto no vacío de un espacio irreducible es irreducible.*

Demostración. Sea X irreducible, U un abierto en X, y Z_1, Z_2 cerrados de X. Tenemos que

$$U = (Z_1 \cap U) \cup (Z_2 \cap U).$$

de esto deducimos que

$$X = (X - U) \cup Z_1 \cup Z_2.$$

Como $X - U \neq X$, $X = Z_1 \cup Z_2$, de donde tenemos, sin pérdida de generalidad, que $X = Z_1$ y $U = F \cap U$. □

Proposición 3.3.7. *Sea $X = \operatorname{Spec} R$ y sea A_{red} el cociente de A módulo su nilradical. Para que X sea irreducible es necesario y suficiente que A_{red} sea dominio entero.*

Demostración. Como también $X = \operatorname{Spec} A_{\text{red}}$, tenemos que si A_{red} es dominio entero, (0) es un ideal primo contenido en todos los otros ideales y, por lo tanto, $X = \overline{\{0\}}$ y X es irreducible.

Recíprocamente, si A_{red} no es dominio, entonces existen a, b diferentes de cero tales que $ab = 0$. Sean $V(a)$ y $V(b)$ los cerrados definidos por los ideales (a) y (b). Tememos que $V(a)$ y $V(b)$ son distintos de X ya que de lo contrario $V(a) = X$ implica que a es un elemento nilpotente y, por lo tanto, igual a 0, pero

$$V(a) \cup V(b) = V((a) \cap (b)) = v((a)(b)) = V(0) = X$$

y X no es irreducible. □

De la demostración anterior, tenemos el siguiente corolario.

Corolario 3.3.8. *Sea X un esquema. Todo subconjunto cerrado irreducible de X es la cerradura de un punto único llamado* punto genérico *de este subconjunto.*

Demostración. la unicidad se sigue del hecho que X es T0. Para demostrar la existencia consideremos primero el caso afín. Sea $X = \operatorname{Spec} R$ y sea Z un cerrado irreducible de X. Sea $Z_{red} = \operatorname{Spec} R/I$ el esquema reducido definido por Z, como Z es irreducible tenemos que R/I es un dominio entero y, por lo tanto, I es un ideal primo. Claramente tenemos que $\overline{\{I\}} = Z$.

Para el caso general tomemos a Z un cerrado irreducible de X, y sea $x \in Z$. Por ser esquema existe un abierto afín U que contiene a x. Tenemos que $Z \cap U$ es un abierto no vacío de un irreducible y, por lo tanto, es irreducible. Por lo que $Z \cap U = \overline{\{y\}}$ para algún y. Entonces $Z = \overline{\{y\}} \cup (Z - U)$ y, dado que Z es irreducible, $Z = \overline{\{y\}}$. □

Ahora trabajaremos con una clase especial de esquemas a los que llamaremos noetherianos. La demostración de las proposiciones referentes a éstos se pueden encontrar en [Har77] o [EH99].

Definición 3.3.9. Decimos que un esquema es *noetheriano* si, y solamente si, éste es la unión finita de abiertos afines $U_i = \operatorname{Spec} A_i$ donde cada A_i es noetheriano.

Proposición 3.3.10. *Si X es un esquema noetheriano, entonces el espacio topológico asociado a X es un espacio noetheriano, es decir, toda cadena descendente de cerrados de X es estacionaria.*

Corolario 3.3.11. *Toda familia no vacía de cerrados de X tiene un elemento minimal.*

Proposición 3.3.12. *Si X es un esquema que puede ser cubierto por un número finito de abiertos afines, entonces X es compacto. Particularmente los esquemas noetherianos son compactos.*

Proposición 3.3.13. *En un esquema noetheriano todo cerrado tiene solamente un número finito de componentes irreducibles.*

Teorema 3.3.14. Un esquema X es noetheriano si, y sólo si, toda cadena creciente de ideales de $\mathcal{O}_X$ es estacionaria.

Definición 3.3.15. Un esquema X es *reducido* si para cada conjunto abierto U, el anillo $\Gamma(U, \mathcal{O}_X)$ no tiene nilpotentes.

Proposición 3.3.16. *Un esquema X es reducido si, y sólo si, para todo $P \in X$ el anillo local $\mathcal{O}_{X,P}$ no tiene nilpotentes.*

Notemos que dado un esquema $(X, \mathcal{O}_X)$ siempre podemos asociarlo a un esquema reducido tomando $(X, (\mathcal{O}_X)_{\text{red}})$ tal como hicimos en la proposición 3.3.7.

Definición 3.3.17. Un esquema es *entero* si para cada abierto $U \subset X$, el anillo $\Gamma(U, \mathcal{O}_X)$ es un dominio entero.

Proposición 3.3.18. *Un esquema es entero si, y sólo si, es reducido e irreducible.*

Definición 3.3.19. Un morfismo $f : X \to Y$ de esquemas es *localmente de tipo finito* si existe una cubierta para Y de abiertos afines $V_i = \operatorname{Spec} B_i$ tal que para cada i, $f^{-1}(V_i)$ puede ser cubierto por abiertos afines $U_{ij} = \operatorname{Spec} A_{ij}$ donde cada A_{ij} es una B_i-álgebra finitamente generada. El morfismo f es *de tipo finito* si además cada $f^{-1}(V_i)$ puede ser cubierto por un número finito de los U_{ij}.

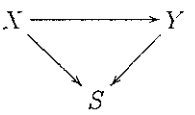
Definición 3.3.20. Un morfismo $f : X \to Y$ es *finito* si existe una cubierta para Y de abiertos afines $V_i = \operatorname{Spec} B_i$ tal que para cada i, $f^{-1}(V_i)$ es afín igual a $\operatorname{Spec} A_i$, donde A_i es una B_i-álgebra que es finitamente generada como B_i-módulo.

Ejemplo 3.3.21. Si V es una variedad sobre un campo algebraicamente cerrado k, entonces su esquema asociado W es un esquema noetheriano, entero y de tipo finito sobre k.

3.4 S-Esquemas

Definición 3.4.1. Fijemos a un esquema S. Un *S-esquema* es un esquema X equipado de un morfismo $X \to S$. Un *morfismo* de S-esquemas, al que

llamaremos S-morfismo, es un morfismo $X \to Y$ tal que el diagrama



es conmutativo. Si $S = \operatorname{Spec} R$, nos referiremos como R-esquema y R-morfismo, en vez de $\operatorname{Spec}(R)$-esquema y $\operatorname{Spec}(R)$-morfismo.

Definición 3.4.2. Sean X y T S-esquemas. El conjunto de puntos T-valuados de X es el conjunto

$$X(T) := \operatorname{Hom}_S(T, X) = \{S - \text{morfismos } T \to X\}.$$

Si $S = T$ diremos también que $X(S)$ es el conjunto de *secciones* del S-esquema X. Si $S = \operatorname{Spec}(R)$ diremos que son los puntos R-valuados y los denotaremos por $X(R)$.

Para ver cúal es la analogía con los puntos K-racionales de una variedad, veamos lo siguiente:

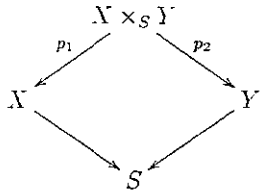
Ejemplo 3.4.3. Sea K un campo y $S = \operatorname{Spec}(K)$. Sea X/K un esquema afín dado por las ecuaciones $f_1 = f_2 = \cdots = f_n = 0$ con cada $f_i \in K[x_1, x_2, \ldots, x_m]$. Entonces

$$\begin{aligned} X(S) &= \{K - \text{morfismos } \operatorname{Spec}(K) \to X\} \\ &\cong \left\{K - \text{homomorfismos de álgebras } \frac{K[x_1, x_2, \ldots, x_m]}{(f_1, f_2 \ldots, f_n)} \longrightarrow K\right\} \\ &= \{P \in \mathbb{A}^m_K : f_1(P) = f_2(P) = \cdots = f_n(P) = 0\} \end{aligned}$$

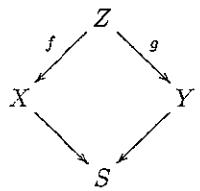
así vemos que $X(K)$ es compatible con lo que son los puntos racionales de la variedad definida por estos polinomios. Cabe mencionar que análogamente se puede ver que $X(R)$ se puede identificar con las m-tuplas en R^m que satisfacen los polinomios $f_1, f_2 \ldots, f_n \in R[x_1, x_2, \ldots, x_m]$.

Definición 3.4.4. Sea S un esquema, y sean X, Y dos S-esquemas. Definimos el *producto fibrado* de X y Y sobre S, denotado por $X \times_S Y$ como un esquema junto con morfismos $p_1 : X \times_S Y \to X$ y $p_2 : X \times_S Y \to Y$ que

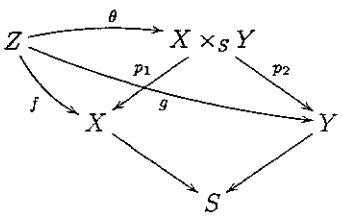
hacen conmutar el diagrama



y que además cumple con la siguiente propiedad universal: para todo S-esquema Z junto con morfismos $f : Z \longrightarrow X$ y $g : Z \longrightarrow Y$ tal que hace conmutativo al diagrama



existe un único morfismo $\theta : Z \longrightarrow X \times_S Y$ tal que $f = p_1 \circ \theta$ y $g = p_2 \circ \theta$, es decir, el diagrama



es conmutativo. Los morfismos p_1 y p_2 son llamados las *proyecciones* del producto fibrado en sus factores.

Teorema 3.4.5. Para cualesquiera dos S-esquemas, el producto fibrado $X \times_S Y$ existe y es único salvo isomorfismo.

Demostración. Para el caso afín, veamos que si $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, $S = \operatorname{Spec} R$, entonces A y B son R-álgebras. Aseguramos que $\operatorname{Spec}(A \otimes_R B)$ es el producto fibrado de X y Y. En efecto, para un esquema Z, dar un morfismo de Z a $\operatorname{Spec}(A \otimes_R B)$ es lo mismo que dar un morfismo de anillos de $A \otimes_R B$ a $\Gamma(Z, \mathcal{O}_Z)$, pero dar un homomorfismo de $A \otimes_R B$ en cualquier anillo es equivalente a dar morfismos de A y B a ese anillo induciendo el mismo

homomorfismo en R. Con lo que dar un morfismo de Z a $\mathrm{Spec}(A \otimes_R B)$ es equivalente a dar morfismos de Z a X y a Y, que resultan los morfismos de Z en S. Así, $\mathrm{Spec}(A \otimes_R B)$ es el producto fibrado. El caso general se hace pegando en las cartas afines (ver [Har77] para la demostración completa). □

Podemos pensar que el producto fibrado $X \times_S Y$ es, en cierto sentido, como el conjunto de pares (x, y) con la propiedad de que x y y tienen la misma imagen en S, hecho que es verdad para la categoría de conjuntos.

Definición 3.4.6. Sea $f : X \longrightarrow Y$ (X es un Y-esquema) un morfismo de esquemas, y sea $y \in Y$ un punto. Sea $k(y) = \mathcal{O}_{Y,y}/M_y$ su campo de residuos y sea $k(y) \longrightarrow Y$ el morfismo natural. Definimos la *fibra* del morfismo f sobre el punto y, como el esquema

$$X_y := X \times_Y \mathrm{Spec}\, k(y) = X \times_Y \{y\}.$$

Notemos que X_y es un esquema sobre $k(y)$ cuyo espacio topológico es homeomorfo a $f^{-1}(y)$ ([Har77]), por lo que la definición de la fibra concuerda con nuestra intuición.

Definición 3.4.7. Sea R un anillo y P un ideal máximo de R. Sea X un R-esquema. Definimos la *reducción módulo* P del esquema X como:

$$X_P := X \times_R \{P\} = X \times_R P.$$

Éste es un esquema sobre R/P.

De acuerdo con la definición anterior, vemos que si X es un esquema afín definido por polinomios con coeficientes en R, entonces X_P es el esquema sobre R/P definido por los mismos polinomios reducidos módulo P.

Definición 3.4.8. Sea R un domino entero, y sea $\eta = (0) \in \mathrm{Spec}\, R$ el punto genérico de $\mathrm{Spec}\, R$. Si X es un R-esquema, definimos a la *fibra genérica* de X como

$$X_\eta = X \times_R \eta$$

Éste es un esquema sobre el campo de fracciones K de R.

Notemos que si R es un anillo de valuación discreta con ideal máximo P, entonces el R-esquema X tiene dos fibras, la fibra genérica X_η/K y su *fibra especial* (o cerrada) X_P/k, donde $k = R/P$

Ejemplo 3.4.9. Sea $X \subset \mathbb{P}^2_R$ un esquema dado por una sola ecuación polinomial

$$F(x, y, z) = 0$$

con coeficientes en R. La fibra genérica $X_\eta \subset \mathbb{P}^2_K$ es la variedad definida por la misma ecuación $F(x, y, z) = 0$, y la fibra especial $X_P \subset \mathbb{P}^2_k$ es la variedad definida por la ecuación $\tilde{F}(x, y, z)$, donde $\tilde{F}$ se obtiene reduciendo módulo P a los coeficientes del polinomio F.

Definición 3.4.10. Sea $X \to S$ un S-esquema. Si en la definición de producto fibrado tomamos $Z = X$ y f, g los morfismos identidad $X \to X$ entonces obtenemos el *morfismo diagonal*

$$\delta_X : X \longrightarrow X \times_S X;$$

esto es. δ_X es el único morfismo hacia el producto fibrado con la propiedad de que $p_1 \circ \delta_X$ y $p_2 \circ \delta_X$ son la identidad.

Definición 3.4.11. Sea $\psi : X \to Y$ un S-morfismo. Entonces la *gráfica* de ψ es el único morfismo

$$\delta_\psi : X \longrightarrow X \times_S Y$$

tal que $p_1 \circ \delta_\psi$ es la identidad en X y $p_2 \circ \delta_\psi = \psi$.

Notemos que el morfismo diagonal es la gráfica del mapeo identidad $X \to X$.

Definición 3.4.12. Tomando en cuenta que cada esquema S admite un único morfismo $S \to \operatorname{Spec} \mathbb{Z}$, definimos el *espacio afín y proyectivo sobre* S como:

$$\mathbb{A}^n_S := \mathbb{A}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S \quad \text{y} \quad \mathbb{P}^n_S := \mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S.$$

La proyección en el segundo factor hace que estos espacios sean S-esquemas.

Notemos que si $S = \operatorname{Spec} R$, entonces tenemos que $\mathbb{A}^n(S) \cong \mathbb{A}^n_R$ y que $\mathbb{P}^n(S) \cong \mathbb{P}^n_R$ por lo que estas definiciones son compatibles con las definiciones de espacio afín y proyectivo sobre un anillo.

Definición 3.4.13. Sea X un S-esquema. Supongamos que tenemos un morfismo $S' \to S$. Entonces el esquema $X' := X \times_S S'$ es un esquema sobre S'. Decimos que obtuvimos a X' de X haciendo una *extensión de base* $S' \to S$.

3.5 Morfismos propios y separados

Para comenzar recordemos algunas definiciones de Álgebra Conmutativa.

Definición 3.5.1.

- La *dimensión de Krull* de un anillo A es el entero más grande d tal que existe una cadena de ideales primos distintos en A, con la propiedad de que

$$P_0 \subset P_1 \subset \cdots \subset P_d.$$

- Un anillo local A con ideal máximo $\mathcal{M}$ es *regular* si la dimensión de $\mathcal{M}/\mathcal{M}^2$ es igual a la dimensión de Krull de A.

Intuitivamente $\mathcal{M}/\mathcal{M}^2$ es el espacio cotangente de Spec A en el punto $\mathcal{M}$, por lo que la regularidad de A nos dice que el punto $\mathcal{M}$ es no singular en Spec A.

Definición 3.5.2. La *dimensión* de un punto P de un esquema X es la dimensión de Krull del anillo local $\mathcal{O}_{X,P}$. Si cada punto cerrado $P \in X$ tiene la misma dimensión, decimos que ésta es la *dimensión de* X.

Definición 3.5.3. Un punto P en un esquema X es *regular* (o no singular) si el anillo local $\mathcal{O}_{X,P}$ es un anillo local regular. Un esquema X es regular (o no singular) si cada punto de X es regular.

Proposición 3.5.4. *Sea R un dominio de Dedekind. El esquema afín* Spec R *es regular de dimensión uno*

Demostración. Por definición sabemos que en un dominio de Dedekind R tiene dimensión uno (ver 1 1 6) y que cada localización R_P es de valoración discreta, por lo que su ideal máximo $\mathcal{M}_P$ es principal y, por lo tanto, el $R_P/\mathcal{M}_P$-espacio vectorial $\mathcal{M}/\mathcal{M}^2$ es de dimensión uno, por lo que R_P es regular □

Ejemplo 3.5.5. Si Spec R es regular, entonces los espacios $\mathbb{A}^n_R$ y $\mathbb{P}^n_R$ son esquemas regulares.

Ahora pasemos a revisar la propiedad y suavidad de esquemas y sus morfismos

Definición 3.5.6. Sea $f : X \to Y$ un morfismo de esquemas. Decimos que f es *separado* si el morfismo diagonal $\delta_X : X \to X \times_Y X$ es una inmersión cerrada. En este caso también decimos que X es *separado* sobre Y. Un esquema X es *separado* si es separado sobre $\operatorname{Spec} \mathbb{Z}$.

Proposición 3.5.7.

- *Sea V una variedad algebraica sobre un campo algebraicamente cerrado k. Si W es su esquema asociado entonces es separado sobre k.*
- *Si $f : X \to Y$ es un morfismo de esquemas afines, entonces f es separado.*
- *Un morfismo $f : X \to Y$ es separado si, y sólo si, la imagen del mapeo diagonal es un cerrado de $X \times_Y X$.*

Demostración. Ver Hartshorne [Har77], página 96. □

Ahora enunciemos el *criterio valuativo de separabilidad.* La idea de éste es que para que un esquema sea separado, éste no debe contener subesquemas tales como curvas con puntos dobles, es decir, si C es una curva y $P \in C$, entonces un morfismo de $C - P$ a X debe admitir a lo más un morfismo de todo C a X que lo extienda.

Teorema 3.5.8 (Criterio valuativo de saparabilidad). Sea $f : X \to Y$ un morfismo de esquemas, y supongamos que X es noetheriano. Entonces f es separado si, y sólo si, las siguientes condiciones se cumplen:

Para cada campo K con anillo de valuación R sean $T = \operatorname{Spec} R$, $U = \operatorname{Spec} K$ y $i : U \to T$ el morfismo inducido por la inclusión $R \subset K$. Dado un morfismo T a Y y uno de U a X tales que hagan conmutativo al cuadro

$$\begin{array}{ccc} U & \longrightarrow & X \\ \downarrow{\scriptstyle i} & \nearrow & \downarrow{\scriptstyle f} \\ T & \longrightarrow & Y \end{array}$$

existe a lo más un morfismo de T a X que hace a todo el diagrama conmutativo.

Demostración. [Har77][página 97]. □

Definición 3.5.9. Un morfismo $f : X \to Y$ es *cerrado*, si la imagen de un subconjunto cerrado es cerrado. f es *universalmente cerrado*, si es cerrado y para cada morfismo $Y' \to Y$ el morfismo $f' : X' \to Y'$, obtenido por extensión de base, es también cerrado.

Definición 3.5.10. Un morfismo $f : X \to Y$ es *propio* si es separado, de tipo finito y universalmente cerrado.

Ejemplo 3.5.11. Sea k un campo y sea $X = \operatorname{Spec} k[x]$ la línea afín sobre k, entonces X es separado y de tipo finito sobre k, pero no es propio sobre k. En efecto, si tomamos la extensión de base $X \to \operatorname{Spec} k$, entonces el mapeo $X \times_k X \to X$ es la proyección del plano afín sobre la línea afín, que en general no es cerrado. Por ejemplo, la hipérbola dada por la ecuación $xy = 1$ es un cerrado del plano, pero su proyección a la línea afín consiste en toda la línea menos el origen, que no es un cerrado.

Intuitivamente un morfismo de esquemas $X \to S$ es propio si todas sus fibras son completas y separadas. Es el análogo algebraico de la propiedad de Hausdorff. Esencialmente esto significa que a las fibras de $X \to S$ no les falta ningún punto y que no tienen muchos puntos.

Teorema 3.5.12 (Criterio valuativo para propiedad). Sea $\phi : X \to S$ un morfismo de tipo finito de esquemas noetherianos. El mapeo ϕ es propio si, y sólo si, para cada anillo de valuación discreta R con campo de fracciones K y para cada cuadrado conmutativo de morfismos

$$\begin{array}{ccc} \operatorname{Spec} k & \longrightarrow & X \\ \downarrow & \nearrow & \downarrow \phi \\ \operatorname{Spec} R & \longrightarrow & S, \end{array}$$

existe un morfismo único $\operatorname{Spec} R \to X$ que hace a todo el diagrama conmutativo.

Demostración. [Har77][página 101] □

Notemos que si R es un anillo de valuación discreta con campo de fracciones K, entonces $\operatorname{Spec} R$ es un anillo regular de dimensión uno (caso particular de 3.5.4), y $\operatorname{Spec} K$ es $\operatorname{Spec} R$ con un punto cerrado removido. Entonces podemos interpretar a $\operatorname{Spec} K$ como una curva con un punto removido.

Ejemplo 3.5.13. Supongamos que tenemos una curva C y un punto $\gamma \in C$. También supongamos que tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} C - \gamma & \xrightarrow{F} & X \\ \downarrow & & \downarrow \\ C & \xrightarrow{f} & S \end{array}.$$

Si $X \to S$ es un morfismo propio, entonces la fibra de X sobre $f(\gamma)$ es separada y completa (universalmente cerrada), por lo que debería haber una única manera de extender F a todo C por el criterio anterior.

Una colección importante de S-esquemas propios son los esquemas proyectivos sobre S, como lo muestra el siguiente teorema.

Teorema 3.5.14. Sea S un esquema noetheriano, y sea $X \subset \mathbb{P}^n_S$ un subesquema cerrado del espacio proyectivo sobre S. Entonces X es propio sobre S, en particular $\mathbb{P}^n_S$ es propio sobre S.

Demostración. Ver [Har77]. □

Definición 3.5.15. Sea $\phi : X \to S$ un morfismo de tipo finito, sea $s \in X$, y $s = \phi(x) \in S$. El mapeo ϕ es *suave de dimensión relativa* r en el punto x, si existen abiertos afines

$$s \in \operatorname{Spec} R \subset S \quad \text{y} \quad x \in \operatorname{Spec} A \subset X$$

con

$$A = \frac{R[t_1, t_2, \ldots, t_{n+r}]}{(f_1, f_2, \ldots, f_n)} \quad \text{para algunos } f_1, f_2, \ldots, f_n \in R[t_1, t_2, \ldots, t_{n+r}]$$

tales que los menores de $n \times n$ de la matriz jacobiana $(\partial f_i / \partial t_j)$ generen a todo A como ideal. Decimos que ϕ es *suave* (o que X es suave sobre Y) si es suave en todos los puntos de X. Un morfismo que es suave de dimensión relativa igual a cero, lo llamamos *morfismo étale*.

Para nuestros propósitos, los ejemplos más importantes de morfismos suaves serán cuando X es un esquema suave sobre un anillo de valuación discreta o sobre un anillo de Dedekind R. En esta situación, la condición de que X sea suave sobre R es esencialmente equivalente a la afirmación de que sus fibras sean no singulares y que tengan la misma dimensión.

Teorema 3.5.16. Sea R un anillo de valuación discreta con campo de cocientes K, campo de residuos k e ideal máximo P. Sea X un R-esquema entero de tipo finito sobre R cuya fibra genérica X_η/K es no vacía. Entonces X es suave si, y sólo si, $X_\eta(\overline{K})$ y $X_P(\overline{k})$ no tienen puntos singulares.

Demostración. Ver [Sil94]. □

Hay muchas propiedades de los morfismos, tales como propiedad, separabilidad, suavidad, que se preservan bajo composiciones. Nosotros sólo usaremos el siguiente:

Proposición 3.5.17. *Si $\phi : X \to Y$ y $\psi : Y \to Z$ son morfismos suaves, entonces la composición $\psi \circ \phi : X \to Y$ es un morfismo suave.*

Demostración. Ver [Har77] □

Intuitivamente un morfismo de esquemas $X \to S$ es suave si todas sus fibras son no singulares, o, por decirlo de otra manera, X es una familia de esquemas regulares.

Para ilustrar todo lo anterior estudiemos el siguiente ejemplo.

Ejemplo 3.5.18. Sea R un anillo de valuación discreta, y sea π el parámetro uniformizador de R. Asumamos que $2, 3 \in R^*$. Sea $a \in R$. Definamos un esquema $X \subset \mathbb{P}^2_R$ por la ecuación

$$X : y^2z = x^3 + az^3.$$

Aseguramos que X es regular si, y sólo si, π^2 no divide a a. En efecto, para checar la regularidad de X, basta checar que X es regular en los puntos singulares de sus fibras X_η y X_P (recordar que suavidad implica regularidad). La fibra genérica X_η es la curva elíptica definida por la ecuación $y^2z = x^3+az^3$ que es una curva elíptica y, por lo tanto, no tiene puntos singulares. En la fibra especial X_P el único punto que puede ser singular es $[0, 0, 1]$ (es decir, en el primo $\gamma = (\pi, x, y, z - 1)$), pero éste sólo es singular si π divide a a, así que si π no divide a a, X es regular.

Supongamos pues que $a \in \mathcal{M} = \pi R$. Como el punto γ no está en el cerrado determinado por $z = 0$, y tomando en cuenta que la regularidad es una propiedad local, podemos deshomogenizar respecto a z, es decir, hacemos $z = 1$. Tenemos que el ideal máximo $\mathcal{M}$, del anillo local $\mathcal{O}$, está generado por

las imágenes correspondientes de x, y y π en $\mathcal{O}_\gamma$, es decir, $\mathcal{M}_\gamma$ está generado por x, y, π y éstas están relacionadas por

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

Si π^2 no divide a a, entonces $a = \pi u$ donde u es una unidad y, entonces, a es otro parámetro uniformizador de R, por lo que

$$\pi \in aR = (y^2 - x^3)R \subset M_\gamma^2,$$

de donde x, y generan a $\mathcal{M}_\gamma/\mathcal{M}_\gamma^2$, lo que implica que $\mathcal{O}_\gamma$ es regular.

Conversamente, si π^2 divide a a, entonces ninguno de x, y, π está en $\mathcal{M}_\gamma^2$ y, de hecho, $\mathcal{M}_\gamma/\mathcal{M}_\gamma^2$ no puede ser generado por menos de tres elementos, por lo que $\mathcal{O}_\gamma$ no es regular.

Siguiendo con el mismo ejemplo, notemos que X es propio sobre R, ya que es un subesquema cerrado de $\mathbb{P}_R^2$, ya vimos que si π divide a a, entonces la fibra especial X_P/k es singular, y entonces X no es suave y su punto singular es γ. Sea $X^0 := X - \gamma$ el esquema obtenido por remover γ de X. Esto hace a la fibra especial X_P^0 no singular, por lo que X^0 es un esquema suave sobre R, sin embargo, quitando al punto γ se destruye la completés de la fibra especial, y siguiendo la definición intuitiva de propiedad, vemos que X^0 no es propio sobre R. Sin embargo, más adelante probaremos que los puntos R-valuados son iguales, es decir $X^0(R) = X(R)$, lo que resultará de gran importancia en nuestro estudio.

Capítulo 4

Modelos de Nèron

Un modelo de Nèron para una curva elíptica es un esquema que, en cierto sentido, recupera la estructura de grupo de la curva. Además cada punto racional se extiende a un punto R-valuado del esquema. En este capítulo utilizamos todo el material antes estudiado para definir con precisión a los modelos de Nèron y estudiar algunas de sus características.

4.1 Grupos algebraicos

Esta sección es un preámbulo a lo que llamaremos grupos esquemas y mostraremos que las curvas elípticas son un caso particular de los mismos. Mostraremos también algunos hechos importantes, sin embargo, no profundizaremos demasiado ya que no es nuestro objetivo fundamental en el trabajo.

Definición 4.1.1. Un *grupo algebraico* es una variedad algebraica G y dos morfismos

$$\mu : G \times G \longrightarrow G \quad \text{y} \quad i : G \longrightarrow G$$

tales que satisfacen las siguientes propiedades.

1. Hay un punto $0 \in G$ tal que $\mu(P, 0) = \mu(0, P) = P$ para todo $P \in G$.
2. $\mu(P, i(P)) = \mu(i(P), P) = 0$ para todo $P \in G$
3. $\mu(P, \mu(Q, R)) = \mu(\mu(P, Q), R)$.

Decimos que G es conmutativo si además satisface

4. $\mu(P,Q) = \mu(Q,P)$.

Una grupo algebraico G está definido sobre K si la variedad G está definida sobre K, los morfismos μ e i están definidos sobre K y $0 \in G(K)$.

Ejemplo 4.1.2. Una curva elíptica es un grupo algebraico.

Definición 4.1.3. El *grupo aditivo* $\mathbb{G}_a$ y el *grupo multiplicativo* $\mathbb{G}_m$ son los grupos algebraicos conmutativos

$$\mathbb{G}_a \cong \mathbb{A}^1 \quad \text{y} \quad \mathbb{G}_m = \{x \in \mathbb{A}^1 : x \neq 0\}$$

las leyes de grupo están dadas por la suma y la multiplicación respectivas. Notemos que el grupo multiplicativo, aunque no es exactamente una variedad, si es regular o isomorfa a la variedad dada por $xy - 1 = 0$.

Definición 4.1.4. Un *homomorfismo* de grupos algebraicos $\psi : G \longrightarrow H$ es un morfismo de variedades tal que también es un homomorfismo de grupos.

Ejemplo 4.1.5. Una isogenea $\psi : E_1 \longrightarrow E_2$ entre dos curvas elípticas, es un morfismo de grupos algebraicos.

Proposición 4.1.6. *Sea G un grupo algebraico definido sobre el campo K. El conjunto de puntos K-racionales $G(K)$ es un subgrupo de G.*

Demostración. Se sigue de la definición. □

Definición 4.1.7. Sea G un grupo algebraico. A la componente conexa de G que contiene al elemento identidad 0, la llamamos *componente identidad* y la denotaremos por G^0. Al grupo cociente G/G^0

Proposición 4.1.8. *Sea G un grupo algebraico.*

1. *G es una variedad no singular*
2. *Cada componente conexa de G es irreducible*
3. *La componente conexa de G que contiene a la identidad, es un subgrupo normal de G de índice finito.*

Demostración 1. Hay un abierto de Zariski $U \subset G$ tal que es no singular. Para cada $P \in G$ sea $t_P \ . \ G \to G$ la translación por P, es decir, $t_P(Q) = \mu(P, Q)$. Notemos que t es un isomorfismo de G con él mismo. Tenemos que G lo podemos cubrir, entonces, por abiertos no singulares $t_p(U)$, $p \in G$, por lo que G es no singular.

2. Supongamos que $G = Z_1 \cup Z_2$ con Z_i cerrado. Como G es conexo tenemos que $Z_1 \cap Z_2 \neq \emptyset$, pero todo $p \in Z_1 \cap Z_2 \neq \emptyset$ es singular, lo que contradice la parte 1.

3. Sabemos que una variedad sólo tiene un número finito de componentes irreducibles por lo que también tiene sólo un número finito de componentes conexas: $G^0, G^1, \ldots, G^n$ donde G^0 es la componente conexa que contiene al 0. Sea $P \in G^0$; dado que t_p es un isomorfismo, t_p manda componentes conexas en componentes conexas, por lo que

$$t_P(G^0) = G^j \quad \text{para algún} \quad j,$$

pero $P = t_P(0) \in G^j$ por lo que $P \in G^0 \cap G^j$ y como G es no singular $G^0 = G^j$, esto significa que $\mu(P, Q) \in G^0$ para todo $P, Q \in G^0$, similarmente $i(G^0) = G^0$ por lo que G^0 es un subgrupo.

Ahora mostraremos que es normal. Fijemos un punto $Q \in G$ y consideremos el mapeo conjugación por Q, es decir,

$$\phi(P) = \mu(i(Q), \mu(P, Q))$$

Tenemos que ϕ es un automorfismo de G, por lo que también permuta las componentes de G. Más aún, $\phi(0) = 0$ por lo que $\phi(G^0) = G^0$ lo que demuestra que G^0 es un subgrupo normal. Para ver que tiene índice finito, escojamos un $P_j \in G^j$ para cada j y definamos los mapeos

$$\phi_j : G \longrightarrow G \quad \phi_j(P) = \mu(P, i(P_j)),$$

que, por un argumento análogo a los anteriores, también permuta componentes en G y satisface $\phi_j(P_j) = 0$, por lo que concluimos que $\phi_j(G_j) = G^0$. Entonces $P_0, P_1, \ldots P_n$ incluye un juego completo de representantes de las clases de G/G^0, por lo que G^0 tiene índice finito

Para terminar enunciemos un importante teorema que nos dice quienes son los grupos algebraicos de dimensión uno. Para ver la demostración ver el libro de Silverman [Sil94].

Teorema 4.1.9. Sea G un grupo algebraico conexo de dimensión uno definida sobre un campo algebraicamente cerrado. Entonces tenemos que $G \cong \mathbb{G}_a$ o $G \cong \mathbb{G}_m$ o bien, G es una curva elíptica.

4.2 Esquemas grupo

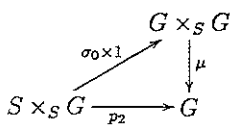
Un grupo esquema sobre S es un S-esquema G cuyas fibras forman una familia de grupos, lo que significa que somos capaces de multiplicar dos puntos que vivan en la misma fibra. Además esta multiplicación debe ser lo suficientemente apropiada para ser compatible con el producto fibrado $G \times_S G$.

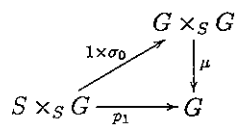
Definición 4.2.1. Sea S un esquema. Un *esquema grupo* sobre S es un S-esquema $G \longrightarrow S$ y S-morfismos

$$\sigma_0 : S \longrightarrow G, \quad i : G \longrightarrow G, \quad \mu : G \times_S G \longrightarrow G,$$

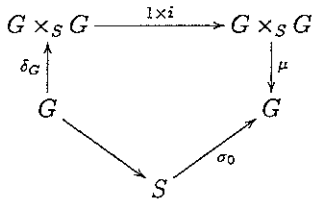
tales que los siguientes diagramas son conmutativos:

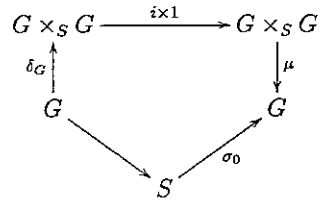
- **Identidad**



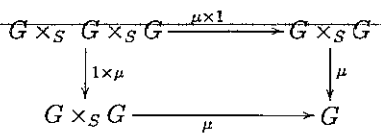


- **Inverso**





- **Asociatividad**



Sea R un anillo de valuación discreta con ideal maximal P y campo de fracciones K. Sea E/K una curva elíptica con buena reducción módulo P. Tomemos una ecuación minimal de Weierstrass para E.

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Entonces los coeficientes están en R, por lo que podemos usar esta ecuación para definir un esquema $\mathcal{E} \subset \mathbb{P}^2(R)$. El hecho de que E tenga buena reducción implica que el esquema $\mathcal{E}$ es suave sobre R, ya que buena reducción es equivalente al hecho de que la fibra especial $\mathcal{E}_P$ de un curva sea suave sobre el campo de residuos R/P.

La ley de suma en E está dada por funciones racionales con coeficientes en R, por lo que induce un mapeo racional

$$\mu : \mathcal{E} \times_R \mathcal{E} \longrightarrow \mathcal{E}.$$

Sabemos que la ley de suma en E (la fibra genérica) está dada por un morfismo. Más adelante probaremos que también μ resulta un morfismo de esquemas.

Ahora veamos que los puntos T-valuados de un esquema resultan ser un grupo.

Teorema 4.2.2. Sea G un grupo esquema sobre S. sea T un S-esquema cualquiera y sea $G(T)$ el conjunto de puntos T-valuados de G. Para cualesquiera dos elementos $\psi, \phi \in G(T)$, definimos un nuevo elemento $\psi * \phi \in G(T)$ por el siguiente diagrama conmutativo:

$$\begin{array}{ccc} T \times_S T & \xrightarrow{\psi \times \phi} & G \times_S G \\ \uparrow{\scriptstyle \delta_T} & & \downarrow{\scriptstyle \mu} \\ T & \xrightarrow[\psi * \phi]{} & G, \end{array}$$

en otras palabras:

$$\psi * \phi := \mu \circ (\psi \times \phi) \circ \delta_T \in G(T)$$

La operación da a $G(T)$ una estructura de grupo. El elemento identidad es la composición

$$T \longrightarrow S \xrightarrow{\sigma_0} G,$$

y el inverso está dado por $\iota \circ \psi$.

Demostración. Si X es un S-esquema, denotemos por $\pi_X : X \to S$ al morfismo que lo hace S-esquema.

Veamos que $\sigma_0 \circ \pi_T$ es, en efecto, el elemento identidad. para esto notemos que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} G \times_S T & \xrightarrow{1\times\pi_T} & G \times_S S \\ {\scriptstyle \psi\times 1}\uparrow & & \downarrow{\scriptstyle 1\times\sigma_0} \\ T \times_S T & \xrightarrow{\psi\times(\sigma_0\circ\pi_T)} & G \times_S G \\ {\scriptstyle \delta_T}\uparrow & & \downarrow{\scriptstyle \mu} \\ T & \xrightarrow{\psi*(\sigma_0\circ\pi_T)} & G \end{array}$$

Ahora, tomando en cuenta que $\mu \circ (1 \times \sigma_0) : G \times_S S \to G$ es la proyección en el primer factor (página 48), tenemos que

$$\psi * (\sigma_0 \circ \pi_T) = p_1 \circ (1 \times \pi_T) \circ (\psi \times 1) \circ \delta_T = p_1 \circ (\psi \times 1) \circ \delta_T = \psi.$$

Por lo que $\sigma_0 \circ \pi_t$ es el elemento identidad (Es análogo demostrar la composición en el otro sentido).

Para demostrar que el inverso de ψ es $i \circ \psi$ notemos que el siguiente diagrama conmuta:

$$\begin{array}{ccc} & & G \\ & {\scriptstyle \psi}\nearrow & \downarrow{\scriptstyle \delta_G} \\ T & \xrightarrow{\psi\times\psi} & G \times_S G \\ {\scriptstyle p_1}\uparrow & & \downarrow{\scriptstyle 1\times i} \\ T \times_S T & \xrightarrow{\psi\times(i\circ\psi)} & G \times_S G \\ {\scriptstyle \delta_T}\uparrow & & \downarrow{\scriptstyle \mu} \\ T & \xrightarrow{\psi*(i\circ\psi)} & G \end{array}$$

Como $\mu \circ (1 \times i) \circ \delta_G = \sigma_0 \circ \pi_G$ por la propiedad del inverso (página 48), y como $\pi_G \circ \psi = \pi_T$ ya que

$$\begin{array}{ccc} T & \xrightarrow{\psi} & T \\ & {\scriptstyle \pi_G}\searrow \quad \swarrow{\scriptstyle \pi_T} & \\ & S & \end{array}$$

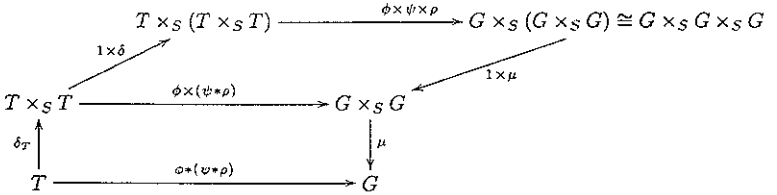
es conmutativo, tenemos que

$$\psi * (i \circ \psi) = \sigma_0 \circ \pi_G \circ \psi = \sigma_0 \circ \pi_T.$$

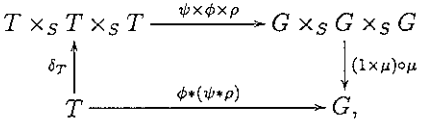
Es análogo la composición en el otro sentido.

Finalmente, para checar la asociatividad, notemos que por las propiedades del producto fibrado, existe un único morfismo $\delta_T : T \to T \times_S T \times_S T$ tal que al componerlo con las proyecciones, queda el mapeo identidad de T.

Tenemos que el siguiente diagrama es conmutativo:



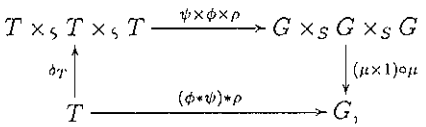
Además, la composición $\delta_T \circ (1 \times \delta_T)$ coincide con el mapeo $\delta_T : T \longrightarrow T \times_S T \times_S T$ por lo que se tiene:



es decir,

$$\phi * (\psi * \rho) = (1 \times \mu) \circ \mu \circ (\psi \times \phi \times \rho) \circ \delta_T.$$

Análogamente tenemos que



es decir,

$$(\phi * \psi) * \rho = (\mu \times 1) \circ \mu \circ (\psi \times \phi \times \rho) \circ \delta_T,$$

pero la propiedad de asociatividad (página 48) nos dice que $(\mu \times 1) \circ \mu = (1 \times \mu) \circ \mu$ por lo que

$$(\phi * \psi) * \rho = (\mu \times 1) \circ \mu \circ (\psi \times \phi \times \rho) \circ \delta_T = (1 \times \mu) \circ \mu \circ (\psi \times \phi \times \rho) \circ \delta_T = \phi * (\psi * \rho).$$

y se tiene la asociatividad en $G(T)$ y, por lo tanto, $G(T)$ es un grupo. □

4.3 Superficies aritméticas

Para los objetivos de esta tesis, la definición formal[1] de superficie aritmética es innecesaria, ya que se requieren definir conceptos técnicos de la geometría algebraica, mismos que no utilizaremos. Para nosotros bastará saber que una superficie aritmética cumple con lo siguiente:

Definición 4.3.1. Sea R un anillo de valuación discreta con campo de fracciones K. Una *superficie aritmética* $\mathcal{C}$ es un R-esquema adecuado cuya fibra genérica es una curva proyectiva conexa no singular C/K y sus fibras especiales son uniones de curvas sobre los campos de residuos apropiados. Así, una superficie aritmética es una familia de dimensión uno, de variedades de dimensión uno, por lo que $\mathcal{C}$ es un esquema de dimensión dos.

Nosotros estaremos interesados en superficies aritméticas que sean regulares, propias sobre R, o suaves sobre R. Recordemos que intuitivamente esto es: $\mathcal{C}$ es regular si es no singular como superficie, $\mathcal{C}$ es propia sobre R si sus fibras están completas, y $\mathcal{C}$ es suave sobre R si sus fibras son no singulares. Notemos que si $\mathcal{C}$ es suave sobre R, es automáticamente regular, pero lo converso no siempre es verdadero.

Nota 4.3.2. Es posible demostrar que si $\mathcal{C}$ es una superficie aritmética, entonces el conjunto de puntos singulares es un conjunto finito de puntos cerrados (ver [Sil94]).

Para que tengamos una noción más clara de lo que es una superficie aritmética, daremos los siguientes ejemplos.

Ejemplo 4.3.3. La línea proyectiva $\mathbb{P}^1_R$ sobre R es una superficie aritmética sobre R. En efecto, para cada ideal máximo $P \in R$, la fibra sobre P es $\mathbb{P}^1_k$, la línea proyectiva sobre el campo de residuos $k = R/P$. Notemos que $\mathbb{P}^1_R$ es propio y suave sobre R.

[1] La definición formal es la siguiente: Sea R un anillo de valuación discreta con campo de fracciones K. Una *superficie aritmética* es un R-esquema plano de tipo finito sobre R que es entero, normal y excelente. Además su fibra genérica es una curva proyectiva conexa no singular C/K y sus fibras especiales son uniones de curvas sobre los campos de residuos apropiados. Para ver las definiciones que se involucran en la anterior, se puede consultar [Har77] y [Mat80].

Ejemplo 4.3.4. Sea $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}}$ el subesquema cerrado de $\mathbb{P}^2_{\mathbb{Z}}$ dado por la ecuación

$$\mathcal{C} : y^2z = x^3 + 2x^2z + 6z^3$$

la fibra genérica de $\mathcal{C}$ es la curva elíptica $E/\mathbb{Q}$ con discriminante $\Delta = -2^6.3.97$, entonces para todos los primos $p \neq 2, 3, 97$, la fibra $\mathcal{C}_p$ es una curva elíptica sobre $\mathbb{F}_p$. Las otras fibras son:

$$\mathcal{C}_2 : y^2z = x^3, \quad \mathcal{C}_3 : y^2z = x^2(x + 2z), \quad \mathcal{C}_{97} : y^2z = (x + 66z)^2(x + 64z).$$

Como $\mathcal{C}/\mathbb{Z}$ es un subesquema cerrado de $\mathbb{P}^2_{\mathbb{Z}}$, tenemos que es propio sobre $\mathbb{Z}$. Como $\mathcal{C}$ tiene fibras singulares, no es suave sobre $\mathbb{Z}$. Aseguramos que

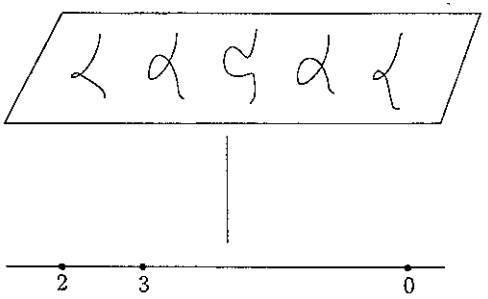


Figura 4.1: Aquí se ilustra la superficie aritmética $\mathcal{C} : y^2z = x^3 + 2x^2z + 6z^3$ sobre Spec $\mathbb{Z}$

$\mathcal{C}$ es regular. Para ver esto, es suficiente verificar que $\mathcal{C}$ es regular en los puntos singulares de las fibras. Para facilitar los cálculos, deshomogeneicemos haciendo $z = 1$ (la regularidad es una propiedad local, por lo que el deshomogeneizar no afecta a los cálculos).

Primero veamos que el punto $P \in \mathcal{C}$ correspondiente a la cúspide $x = y = 2 = 0$ (es decir, $P = (x, y, 2)$) en la fibra $\mathcal{C}_2 : y^2 = x^3$ es regular. El ideal máximo $\mathcal{M}_P$ del anillo local $\mathcal{O}_P$ en P está generado por x, y y 2, y el campo de residuos de P es $\mathcal{O}_P/\mathcal{M}_p \cong \mathbb{F}_2$. Por definición $\mathcal{C}$ es regular en P si

$$\dim_{\mathbb{F}_2} \mathcal{M}_P/\mathcal{M}_P^2 = 2.$$

Sabemos que esta dimensión no puede ser menor que dos ([AM69]), por lo que tenemos que mostrar que $\mathcal{M}_P/\mathcal{M}_P^2$ puede ser generado por dos elementos

(algunos entre x, y y 2). Usando la ecuación de $\mathcal{C}$ vemos que

$$2 = 3^{-1}(y^2 - x^3 - 2x^2) \in \mathcal{M}_P^2,$$

por lo que x y y generan y, por lo tanto, $\mathcal{C}$ es regular en P.

Ahora veamos que la fibra $\mathcal{C}_3 : y^2 = x^2(x+2)$, es regular en su punto singular correspondiente al ideal $P = (3, x, y)$. La demostración es análoga a la anterior, en efecto, el ideal máximo está generado por x, y y 3 y el campo de residuos $\mathcal{O}_P/\mathcal{M}_p \cong \mathbb{F}_3$. Tenemos que checar que

$$\dim_{\mathbb{F}_3} \mathcal{M}_P/\mathcal{M}_P^2 = 3.$$

Usando la ecuación de $\mathcal{C}$, tenemos

$$3 = 2^{-1}(y^2 - x^3 - 2x^2) \in \mathcal{M}_P^2,$$

y, por lo tanto, $\mathcal{C}$ es regular en P.

El caso del punto singular $P = (x + 66, y, 97)$ en la fibra $\mathcal{C}_{97}$ es un poco diferente. El ideal máximo $\mathcal{M}$ del anillo local $\mathcal{O}_P$ está generado por $x + 66, y, 97$, y tenemos que

$$6 = y^2 - x^3 - 2x^2 \in \mathcal{M}^2,$$

además $6 \cong (66)^2 64$, por lo que existe un k tal que $97k = (66)^2 64 - 6$ y entonces

$$97 = k^{-1}((66)^2 64 - 6) = k^{-1}(64x^2 - y^2 + x^3 + 2x^2) \in \mathcal{M}^2,$$

por lo que $\mathcal{M}/\mathcal{M}^2$ está generado por x y y y entonces

$$\dim_{\mathcal{O}_P/\mathcal{M}} \mathcal{M}/\mathcal{M}^2 = 2$$

y, por lo tanto $\mathcal{C}$ es regular.

Así tenemos que el esquema $\mathcal{C}$ es regular y propio sobre $\mathbb{Z}$. Si descartamos los tres puntos singulares en loas tres fibras singulares, obtenemos un subesquema abierto $\mathcal{C}^0 \subset \mathcal{C}$ con la propiedad de que $\mathcal{C}^0$ es suave[2] sobre $\mathbb{Z}$. Sin embargo, siguiendo la idea intuitiva de propiedad, $\mathcal{C}^0$ no es propio sobre $\mathbb{Z}$ ya que a sus fibras le faltan puntos.

[2]esto se debe a que $\mathcal{C}$ es excelente, que es una de las propiedades que se le piden formalmente a una superficie aritmética (ver [Mat80])

Ejemplo 4.3.5. Sea $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}}$ el subesquema cerrado de $\mathbb{P}^2_{\mathbb{Z}}$ dado por la ecuación

$$\mathcal{C} : y^2 = x^3 + 2x^2 + 4.$$

Las fibras singulares son $\mathcal{C}_2, \mathcal{C}_5$ y $\mathcal{C}_7$. En este caso el esquema $\mathcal{C}$ no es regular ya que el punto singular $P = (x, y, 2)$ de la fibra $\mathcal{C}_2$ no es regular. En efecto, el ideal máximo $\mathcal{M}_P$ está generado por $x, y, 2$ y ni x, ni y , ni 2 están en $\mathcal{M}^2$, por lo que

$$\dim_{\mathcal{O}_P/\mathcal{M}_P} \mathcal{M}_P/\mathcal{M}_P^2 = 3 \neq \dim \iota_P = \in,$$

y entonces P es un punto no regular y $\mathcal{C}$ es no regular.

Dentro de la definición formal de superficie aritmética[3] $\mathcal{C}$, se tiene que si $\mathcal{C}$ no es regular. su conjunto de puntos singulares es un conjunto finito formado por puntos cerrados, lo que quiere decir que una superficie aritmética es *regular en codimensión uno.* es decir, cada anillo local $\mathcal{O}_{x,\mathcal{C}}$ de codimensión uno es regular. Esto implica que para cada curva irreducible $F \subset \mathcal{C}$, o para cada punto $F \subset \mathcal{C}$ de codimensión uno, el anillo local $\mathcal{O}_F$ es un anillo de valuación discreta ([Har77]). Denotemos por

$$v_F : K(\mathcal{C})^* \longrightarrow \mathbb{Z}$$

a la valuación normalizada[4] correspondiente, donde $K(\mathcal{C})$ es es el campo de funciones[5] de $\mathcal{C}$.

Definición 4.3.6. Sea X un esquema noetheriano, entero y separado, que es regular en codimensión uno. Un *divisor primo* en X es un subesquema entero y cerrado Y de codimensión uno. Un *divisor de Weil* es un elemento del grupo abeliano libre Div$X$ generado por los divisores primos. Escribimos un divisor como

$$D = \sum n_i Y_i,$$

donde cada Y_i es un divisor primo, y los n_i son enteros y sólo un número finito de ellos son distintos de cero.

[3] La propiedad de excelencia

[4] Es decir, $v_F(\pi) = 1$, donde π es el parámetro uniformizador

[5] $K(\mathcal{C})$ es el anillo $\mathcal{O}_\gamma$ donde γ es el punto genérico de $\mathcal{C}$. Notemos que como γ es genérico, $\mathcal{O}_\gamma$ es un campo

Sea $\pi : \mathcal{C} \to \operatorname{Spec} R$ una superficie aritmética y sea P un punto con campo de residuos $k(P) = R/P$. La fibra

$$\mathcal{C}_P = \mathcal{C} \times_R P = \mathcal{C} \times_{\operatorname{Spec} R} \operatorname{Spec} k(P)$$

es una curva, pero puede ser reducible, singular o hasta no reducida. Esto nos permite escribir, a manera de divisor, a la fibra

$$\mathcal{C}_P = \sum_{i=1}^{r} n_i F_i$$

para ciertas curvas irreducibles $F_i, F_2, \ldots, F_r$ y multiplicidades $n_1, n_2, \ldots, n_r$ con $n_i \geq 1$ de la siguiente manera: fijemos un uniformizador $u \in R$ para P, es decir $\operatorname{ord}_P(u) = 1$. Entonces $\pi^*(u) = u \circ \pi$ es una función racional en $\mathcal{C}$, y la fibra de $\mathcal{C}$ sobre P está dada por

$$\mathcal{C}_P = \sum_{F \subset \pi^{-1}(P)} v_F(\pi^* u) F.$$

Para ilustrar esto, veamos el siguiente ejemplo.

Ejemplo 4.3.7. Consideremos la superficie aritmética afín $\mathcal{C} \subset \mathbb{A}^2_{\mathbb{Z}}$ definida por la ecuación

$$\begin{aligned} \mathcal{C} : 2y^5 - (x+1)y^4 - (2x^3 + x^2 + x)y^3 + (x^4 - x^3 - 3x^2)y^2 \\ + (x^4 + 3x^3)y - x^4 - x^3 + x^2 = \bar{5}. \end{aligned}$$

Pongamos atención a la fibra especial $\mathcal{C}_{\bar{5}}$ de $\mathcal{C}$ sobre el punto $(\bar{5}) \in \operatorname{Spec} \mathbb{Z}$. Esta fibra especial es una cura en $\mathbb{A}^2_{\mathbb{F}_5}$ definida por reducir la ecuación de $\mathcal{C}$ módulo 5. Tenemos que

$$\mathcal{C}_{\bar{5}} = (y^2 - x^3 - 3x^2)(y-2)^2(2y - x - 3) = 0.$$

Entonces $\mathcal{C}_{\bar{5}}$ está formada por tres componentes irreducibles

$$F_1 : y^2 - x^3 - 3x^2 = 0, \quad F_2 : y - 2 = 0, \quad F_3 : 2y - x - 3 = 0.$$

La componente F_2 de $\mathcal{C}_{\bar{5}}$ tiene multiplicidad 2 y las otras componentes tienen multiplicidad uno, por lo que, como esquema a manera de divisor, la fibra especial tiene la forma

$$\mathcal{C}_{\bar{5}} = F_1 + 2F_2 + F_3.$$

En particular, el esquema $\mathcal{C}_5$ no es irreducible ni singular. Cada punto en F_2 es un punto singular de $\mathcal{C}_5$ ya que aparece con multiplicidad mayor que 1. Los otros puntos singulares son el primo correspondiente al nodo $(0,0)$ en F_1 y los puntos de intersección de las F_i.

Ahora veamos una proposición que nos permite saber, en algunos casos, si un punto es no singular. Concretamente nos dice que si un punto $x \in \mathcal{C}_P$ es la imagen de un punto R-valuado, entonces es no singular.

Proposición 4.3.8. *Sea $\pi : \mathcal{C} \to \operatorname{Spec} R$ una superficie aritmética regular sobre un dominio de Dedekind R, y sea $P \in \operatorname{Spec} R$.*

1. *Sea $x \in \mathcal{C}_P \subset \mathcal{C}$ un punto cerrado en la fibra de $\mathcal{C}$ sobre P. Entonces $\mathcal{C}_P$ es no singular en x, si y sólo si $\pi^*(p) \nsubseteq \mathcal{M}^2_{\mathcal{C},x}$, donde π^* es el morfismo natural $\pi^* : R \to \mathcal{O}_{\mathcal{C},x}$ inducido por π.*

2. *Sea $\phi \in \mathcal{C}(R)$. Entonces $\mathcal{C}_P$ es no singular en $\phi(P)$.*

Demostración. Denotemos por β al ideal extendido de $\pi^*(P)$, es decir

$$\beta = \pi^*(P)\mathcal{O}_{\mathcal{C},x}.$$

Notemos que $\beta \subset \mathcal{M}^2_{\mathcal{C},x}$ ($\mathcal{M}^2_{\mathcal{C},x}$ es el ideal máximo de $\mathcal{O}_{\mathcal{C},x}$), ya que x vive en la fibra especial sobe P.

1 Primero asumamos que $\beta \nsubseteq \mathcal{M}^2_{\mathcal{C},x}$ y probaremos que x es un punto no singular de $\mathcal{C}_P$. Como $\mathcal{C}$ es regular, el anillo $\mathcal{O}_{\mathcal{C},x}$ es local regular de dimensión dos. Esto significa que podemos encontrar elementos $f_1, f_2 \in \mathcal{M}_{\mathcal{C},x}$ tales que

$$\mathcal{M}_{\mathcal{C},x} = f_1\mathcal{O}_{\mathcal{C},x} + f_2\mathcal{O}_{\mathcal{C},x} + \mathcal{M}^2_{\mathcal{C},x}.$$

Como R es dominio de Dedekind, todo ideal primo es principal, por lo que existe $t \in R$ tal que $P = tR$, y entonces $\pi^*(t) \in \beta \subset \mathcal{M}_{\mathcal{C},x}$, entonces

$$\pi^*(t) \equiv a_1 f_1 + a_2 f_2 (\operatorname{mod} \mathcal{M}^2_{\mathcal{C},x})$$

para algunos $a_1, a_2 \in \mathcal{O}_{\mathcal{C},x}$. Como supusimos que $\beta \nsubseteq \mathcal{M}^2_{\mathcal{C},x}$, entonces $\pi^* \notin \mathcal{M}^2_{\mathcal{C},x}$ por lo que al menos una de a_1 y a_2 no está en $\mathcal{M}_{\mathcal{C},x}$ y, por

lo tanto, alguna es unidad. Intercambiando f_1 y f_2 si fuera necesario, lo anterior nos dice que

$$\mathcal{M}_{\mathcal{C},x} = \pi^*(t)\mathcal{O}_{\mathcal{C},x} + f_2\mathcal{O}_{\mathcal{C},x} + \mathcal{M}^2_{\mathcal{C},x} = \beta + f_2\mathcal{O}_{\mathcal{C},x} + \mathcal{M}^2_{\mathcal{C},x}.$$

Como $\mathcal{C}_P = \mathcal{C} \times_R (R/P)$, su anillo local en x se obtiene del anillo local de $\mathcal{C}$ reduciendo módulo P. En otras palabras,

$$\mathcal{O}_{\mathcal{C}_P,x} = \mathcal{O}_{\mathcal{C},x}/\beta \quad \text{y } \mathcal{M}_{\mathcal{C}_P,x} = \mathcal{M}_{\mathcal{C},x}/\beta.$$

Por lo que

$$\mathcal{M}_{\mathcal{C}_P,x} = (\beta + f_2\mathcal{O}_{\mathcal{C},x} + \mathcal{M}^2_{\mathcal{C},x})/\beta = f_2\mathcal{O}_{\mathcal{C}_P,x} + \mathcal{M}^2_{\mathcal{C}_P,x},$$

lo que muestra que $\mathcal{M}_{\mathcal{C}_P,x}/\mathcal{M}^2_{\mathcal{C}_P,x}$ está generado solamente por f_2 y, por lo tanto, $\mathcal{O}_{\mathcal{C}_P,x}$ es un anillo local regular de dimensión uno y, entonces, x es un punto no singular de $\mathcal{C}_P$.

Conversamente, supongamos que $\mathcal{C}_P$ es no singular en x y que $\pi^*(P) \subset \mathcal{M}^2_{\mathcal{C},x}$. Por la regularidad de $\mathcal{C}$, tenemos que

$$\mathcal{M}_{\mathcal{C},x} = f_1\mathcal{O}_{\mathcal{C},x} + f_2\mathcal{O}_{\mathcal{C},x} + \mathcal{M}^2_{\mathcal{C},x}.$$

y, entonces, reduciendo modulo P tenemos

$$\begin{aligned}\mathcal{M}_{\mathcal{C}_P,x} =& (f_1\mathcal{O}_{\mathcal{C},x} + f_2\mathcal{O}_{\mathcal{C},x} + \mathcal{M}^2_{\mathcal{C},x})/\beta \\ & f_1\mathcal{O}_{\mathcal{C}_P,x} + f_2\mathcal{O}_{\mathcal{C}_P,x} + \mathcal{M}^2_{\mathcal{C}_P,x},\end{aligned}$$

Pero $\mathcal{O}_{\mathcal{C}_P,x}$ es no singular en x por lo que $\mathcal{M}_{\mathcal{C}_P,x}/\mathcal{M}^2_{\mathcal{C}_P,x}$ tiene dimensión uno y, entonces alguno de f_1 o f_2 está en β, pero como supusimos que $\pi^*(P) \subset \mathcal{M}^2_{\mathcal{C},x}$ entonces también $\beta \subset \mathcal{M}^2_{\mathcal{C},x}$, pero entonces $f_1($ o $f_2) \in \mathcal{M}^2_{\mathcal{C},x}$, lo que contradice el hecho de que f_1 y f_2 son generadores de $\mathcal{M}_{\mathcal{C},x}/\mathcal{M}^2_{\mathcal{C},x}$.

2. Supongamos que $\pi^*(P) \subset \mathcal{M}_{\mathcal{C},x}$, usando el hecho de que $\pi \circ \phi$ es el mapeo identidad en Spec R, calculamos que

$$P = (\pi \circ \phi)^*(P) = \phi^* \circ \pi^*(P) \subset \phi^*(\mathcal{M}^2_{\mathcal{C},x}) = (\phi^*\mathcal{M}_{\mathcal{C},x})^2 = P^2.$$

La última igualdad se sigue del hecho de que ϕ : Spec $R \to \mathcal{C}$ es un morfismo de esquemas, que son espacios localmente anillados, por lo

tanto el mapeo inducido $\phi^* : \mathcal{O}_{C,x} \to R_P$ es un homomorfismo local y $\phi^* \mathcal{M}_{C,x} = P$.

Sin embargo, como R es de Dedekind, P es máximo y la inclusión $P \subset P^2$ es imposible. Entonces $\pi^*(P) \nsubseteq \mathcal{M}^2_{C,x}$. Aplicando la primera parte de esta proposición, concluimos que x es no singular en la fibra C_P.

□

Corolario 4.3.9. *Sea R un dominio de Dedekind con campo de fracciones K. Sea C/R una superficie aritmética y sea C/K su fibra genérica .*

1 *Si C es propia sobre R, entonces*

$$C(K) = C(R).$$

2. *Supongamos que el esquema C es regular, y sea $C^0 \subset C$ el subesquema más grande tal que el mapeo $C^0 \to \operatorname{Spec} R$ es un morfismo suave. Entonces*

$$C(R) = C^0(R).$$

3. *En particular, si C es regular y propia sobre R, entonces*

$$C(K) = C(R) = C^0(R).$$

Demostración. 1. Notemos que cualquier punto en $C(R)$ se puede llevar a un punto en la fibra genérica $C(K)$ por especialización, por lo que existe un mapeo natural $C(R) \to C(R)$. Este mapeo es inyectivo ya que dos morfismos $\operatorname{Spec} R \to C$ que coinciden en un abierto denso, coinciden en todos lados. Ahora veamos que también es suprayectivo. Tomemos $\phi \in C(K)$. Como C es propio sobre R, el criterio valuativo nos dice que existe un morfismo $\sigma_{phi} : \operatorname{Spec} R \to C$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} C = C \times_R K & \longrightarrow & C \\ {\scriptstyle \phi}\uparrow & & \uparrow{\scriptstyle \sigma_\phi} \\ \operatorname{Spec} K & \longrightarrow & \operatorname{Spec} R \end{array} \quad .$$

Esto prueba que cada punto en $C'(K)$ viene de un punto en $C(R)$. Por lo que $C'(R) = C'(K)$.

2. La proposición anterior 4.3.8 nos dice que cada punto en $\mathcal{C}(R)$ intersecta a cada fibra en un punto no singular de la fibra, pero, por definición, $\mathcal{C}^0$ es el complemento en $\mathcal{C}$ de los puntos singulares en las fibras. Entonces la inclusión natural $\mathcal{C}^0(R) \to \mathcal{C}(R)$ es una biyección.

3. Se sigue de las dos partes anteriores.

□

Este corolario nos dice que si $\mathcal{C}$ es una superficie aritmética regular que es propia sobre R, entonces la parte suave $\mathcal{C}^0$ de $\mathcal{C}$ es lo suficientemente grande para que todos los puntos K-valuados de la fibra genérica se extiendan a puntos R-valuados de $\mathcal{C}^0$.

El siguiente teorema es muy importante para nuestro trabajo por que resuelve el problema: Dada una curva C/K, saber si existe una superficie aritmética $\mathcal{C}$ tal que su fibra genérica sea C/K y, en un sentido que veremos más adelante, nos permite saber si esta superficie es mínima. Sin embargo, la demostración de este teorema es muy técnica y las herramientas que se usan para la demostración, no son de utilidad para nuestros objetivos, es por eso que la omitiremos. Para las referencias de la prueba ver el libro [Sil94].

Teorema 4.3.10. Sea R un dominio de Dedekind con campo de fracciones K, y sea C/K una curva proyectiva no singular de género g.

1. **(Resolución de singularidades para superficies aritméticas).** Existe una superficie aritmética regular $\mathcal{C}/R$, propia sobre R, cuya fibra genérica es isomorfa a C/K. A $\mathcal{C}/R$ la llamamos *Modelo regular y propio* para la curva C/K.

2. **(Modelos minimales).** Asumamos que $g \geq 1$. Entonces existe un modelo regular y propio $\mathcal{C}^{\min}/R$ para C/K con la siguiente propiedad de minimalidad:

   Sea $\mathcal{C}/R$ otro modelo regular y propio para C/K. Fijemos un isomorfismo de la fibra genérica de $\mathcal{C}$, a la fibra genérica de $\mathcal{C}^{\min}$. Entonces el mapeo R-birracional

$$\mathcal{C} \longrightarrow \mathcal{C}^{\min}$$

es un R-isomorfismo. Llamamos a $\mathcal{C}^{\min}$ el *modelo minimal regular y propio* para C/K. Éste es único salvo R-isomorfismo único.

Proposición 4.3.11. *Sea R un dominio de Dedekind con campo de fracciones K. Sea C/K una curva proyectiva no singular de género $g \geq 1$. Sea $\mathcal{C}/R$ un modelo minimal regular y propio para C/K. Sea $\mathcal{C}^0$ el subesquema más grande de $\mathcal{C}$ que es suave sobre R. Entonces cada K-automorfismo $\tau : C/K \to C/K$ de la fibra genérica de $\mathcal{C}$, se extiende a un R-automorfismo*

$$\tau : \mathcal{C} \longrightarrow \mathcal{C} \qquad y \qquad \tau : \mathcal{C}^0 \longrightarrow \mathcal{C}^0.$$

Demostración. De la definición de modelo minimal, podemos inferir que τ se extiende a un R-automorfismo $\mathcal{C} \to \mathcal{C}$. Tomemos un punto $x \in \mathcal{C}^0$ y tomemos una vecindad abierta $U \subset \mathcal{C}^0$ de x. Entonces U es suave sobe R, más aún U es abierto de $\mathcal{C}$ ya que $\mathcal{C}^0$ es abierto de $\mathcal{C}$. Debido a que τ es un R-automorfismo, $\tau(U)$ es una vecindad abierta de $\tau(x)$ y es suave sobre R; esto implica que $\tau(x) \in \mathcal{C}^0$, lo que prueba que $\tau(\mathcal{C}^0) \subset \mathcal{C}^0$. Ahora apliquemos el mismo argumento para τ^{-1} con lo que concluimos que $\tau^{-1}(\mathcal{C}^0) \subset \mathcal{C}^0$ y, por lo tanto, τ da un R-automorfismo de $\mathcal{C}^0$. □

4.4 Modelos de Nèron

Definición 4.4.1. Sea R un dominio de Dedekind con campo de fracciones K, y sea E/K una curva elíptica. Un *modelo de Nèron* para E/K es un esquema grupo suave $\mathcal{E}/R$ cuya fibra genérica es E/K y que satisface la siguiente propiedad.

> [Propiedad del mapeo de Nèron] Sea $\mathcal{X}/R$ un R-esquema suave con fibra genérica X/K. Sea $\phi_K : X/K \to E/K$ un mapeo racional definido sobre K. Entonces existe un único R-morfismo $\phi_R : \mathcal{X}/R \to \mathcal{E}/R$ que extiende a ϕ_K.

Notemos que en la definición no se dice que $\mathcal{E}$ es propio sobre R

Proposición 4.4.2. *Sea R un dominio de Dedekind con campo de fracciones K, y sea E/K una curva elíptica*

1. *Supongamos que $\mathcal{E}_1$ y $\mathcal{E}_2$ son modelos de Nèron para E.Entonces existe un único R-isomorfismo psi : $\mathcal{E}_1 \to \mathcal{E}_2$ cuya restricción a la fibra genérica es el mapeo identidad en E/K. Es decir, el modelo de Nèron es único salvo único isomorfismo.*

2. *Sea K'/K una extensión finita no ramificada*[6]*, y sea R' la cerradura entera de R en K'. Sea $\mathcal{E}/R$ un modelo de Nèron para E/K. Entonces $\mathcal{E} \times_R R'$ es un modelo de Nèron para E/K'.*

Demostración. 1. El mapeo identidad $E/K \to E/K$ es un mapeo racional de la fibra genérica de $\mathcal{E}_1$ a la fibra genérica de $\mathcal{E}_2$, y, como $\mathcal{E}_1$ es suave sobre R la propiedad del mapeo de Nèron para $\mathcal{E}_2$ nos asegura que podemos extender el mapeo identidad de manera única a un R-morfismo $\psi : \mathcal{E}_1/R \to \mathcal{E}_2/R$. Análogamente tenemos un R-morfismo $\phi : \mathcal{E}_2 \to \mathcal{E}_1$ que es la identidad en la fibra genérica. Entonces tenemos dos morfismos $\psi \circ \phi : \mathcal{E}_1 \to \mathcal{E}_1$ y el identidad $\mathcal{E}_1 \to \mathcal{E}_1$ tal que son el mismo en la fibra genérica, pero la propiedad del mapeo de Nèron nos asegura que sólo hay un mapeo con esta propiedad, por lo que $\psi \circ \phi$ es la identidad. Análogamente vemos que $\phi \circ \psi$ es la identidad y, por lo tanto ϕ y ψ son isomorfismos.

2. Sea $\mathcal{X}'/R'$ un R'-esquema suave con fibra genérica X'/K'. Sea $\phi_{K'} : X'/K' \to E/K'$ un mapeo racional. La composición

$$\mathcal{X}' \longrightarrow \operatorname{Spec} R' \longrightarrow R$$

hace a $\mathcal{X}'$ un R-esquema. Más aún, como el morfismo $\operatorname{Spec} R' \to \operatorname{Spec} R$ es suave, la composición es también suave, por lo que $\mathcal{X}'$ es un R-esquema suave.

Ahora, la propiedad del del mapeo de Nèron para $\mathcal{E}/R$ nos dice que existe un R-morfismo $\phi_R \mathcal{X}' \to \mathcal{E}$ cuya restricción a la fibra genérica es la composición

$$X' \xrightarrow{\phi_{K'}} E \times_K K' \xrightarrow{p_1} E.$$

Los dos R-morfismos $\phi_R : \mathcal{X}' \to \mathcal{E}$ y $\pi_{\mathcal{X}'} \mathcal{X}' \to \operatorname{Spec} R'$, donde $\pi_{\mathcal{X}'}$ es el morfismo que lo hace R' esquema, determinan un R-morfismo

[6]Para la definición, ver la página 10. Esta definición implica, en particular que el morfismo $\operatorname{Spec} R' \to \operatorname{Spec} R$ sea suave (ver [Art84])

$o_{R'} = \phi_R \times \pi_{\mathcal{X}'}$ a el producto fibrado,

$$\phi_{R'} : \mathcal{X}' \longrightarrow \mathcal{E} \times_R R'.$$

Más aún, la restricción de $\phi_{R'}$ a la fibra genérica es $\phi_{K'}$, por lo que tenemos la existencia. Para demostrar la unicidad supongamos que dado un morfismo

$$\rho : X'/K \longrightarrow E/K' = E \times_K K'$$

se tienen dos morfismos

$$\phi_{R'}, \psi_{R'} : \mathcal{X}' \longrightarrow \mathcal{E} \times_R R'$$

tales que $\rho = \phi_{K'} = \psi_{K'}$, es decir, coinciden con ρ en su restricción a la fibra genérica. Haciendo la composición

$$\mathcal{X}' \longrightarrow \mathcal{E} \times_R R' \longrightarrow \mathcal{E}$$

y tomando en cuenta que

$$\mathcal{X}' \longrightarrow \operatorname{Spec} R' \longrightarrow \operatorname{Spec} R$$

hace a $\mathcal{X}'$ un R-esquema suave, tenemos que $\phi_R = p_1 \circ \phi_{R'}$ y $\psi_r = p_1 \circ \psi_{R'}$ son dos morfismos de $\mathcal{X}'$ a $\mathcal{E}$ tales que sus restricciones a la fibra genérica coinciden. Esto es

$$p_1 \circ \rho = \phi_K = \psi_K,$$

Pero, por la unicidad del mapeo de Nèron para $\mathcal{X}$ tenemos que $\phi_R = \psi_R$, pero entonces

$$\phi_{R'} = \phi_R \times_R R' = \psi_R \times_R R' = \psi_{R'},$$

lo que nos da la unicidad y la prueba está terminada.

□

Ahora usaremos el ecuación de Weierstrass de una curva elíptica para construir un grupo esquema cuya fibra genérica sea la curva elíptica.

Teorema 4.4.3. Sea R Un anillo de valuación discreta con campo de fracciones K, sea E/K una curva elíptica dada por la ecuación de Weierstrass con coeficientes en R

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Esta ecuación define un esquema $W \subset \mathbb{P}^2_R$. Sea $W^0 \subset W$ el subesquema más grande de W que es suave sobre R. Entonces

1. Tanto W/R como W^0/R tienen fibra genérica igual a E/K.

2. El mapeo natural $W(R) \to E(K)$ es una biyección. Si W es regular, entonces el mapeo natural $W^0(R) \to W(R)$ es una biyección, y en este caso hay una identificación $W^0(R) = E(K)$.

3. Los mapeos de adición y de inverso en E se extienden a R-morfismos

$$W^0 \times_R W^0 \longrightarrow W^0 \quad \text{y} \quad W^0 \longrightarrow W^0$$

que hacen a W^0 un grupo esquema sobre R. Más aún, el mapeo adición se extiende a un R-morfismo

$$W^0 \times_R W \longrightarrow W$$

que da una axión de W^0 en W.

Demostración. Primero observemos que si E/K tiene mala reducción, entonces E tiene sólo un punto singular en la reducción modulo P, $\tilde{E}$, donde P es el único primo de R. En otras palabras, la fibra especial de W contiene exactamente un punto singular. Si $\gamma \in W_P \subset W$ es este punto, entonces W^0 es obtenida por quitarle a W el punto γ, es decir

$$W^0 = W - \{\gamma\}.$$

1. W es es proyectivo sobre R ya que es el subesquema cerrado de $\mathbb{P}^2_R$ definido por la ecuación

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Su fibra genérica es la variedad en $\mathbb{P}^2_K$ definida por esta misma ecuación. Entonces la fibra genérica de W es precisamente E/K.

2. Como W es un subesquema cerrado de $\mathbb{P}^2_R$, es propio sobre R. Usando la parte 1, vemos que E/K es su fibra genérica, y entonces, usando la parte 1 del corolario 4.3.9 tenemos que

$$W(R) = E(K).$$

Además W es regular, por lo que gracias al corolario 4.3.9 parte 2 tenemos que $W(R) = W^0(R)$, y entonces concluimos que

$$E(K) = W^0(R).$$

3. Sean $\mu : W \times_R W \longrightarrow W$ y $\imath : W \longrightarrow W$ los mapeos racionales en W inducidos por el mapeo adición y el mapeo inverso en la fibra genérica E/K de W. El hecho de que la fibra genérica sea un grupo algebraico, significa que μ e $\imath$ satisfacen todos los axiomas de grupo en un un subesquema abierto no vació de W, por lo que deben satisfacer los axiomas de grupo en el abierto más grande en el que están definidos. Es decir, si si podemos mostrar que tanto μ como $\imath$ son son morfismos en $W^0 \times_R W$ y en W respectivamente, entonces los axiomas de grupo se cumplen automáticamente

Supongamos que $2, 3 \in R^*$, entonces podemos hacer cambios de variables para obtener la ecuación de Weierstrass en la forma $E(a, b)$ (ver página20) y definir a W como

$$W : y^2z = x^3 + axz^2 + bz^3.$$

Sea W_a el abierto afín de W determinado por

$$W_a = \{z \neq 0\} \subset W,$$

entonces las coordenadas afines se obtienen haciendo la substitución $z = 1$. Usando la fórmula explicita para μ en la parte afín (ver [Sil85]) tenemos que

$$\begin{aligned}\mu[(x_1, y_1), (x_2, y_2)] = &[(x_2 - x_1)((y_2 - y_1)^2 - (x_2 - x_1)^2(x_2 + x_1)),\\ &(y_2 - y_1)^3 + (x_2 - x_1)^2(x_1y_1 - x_2y_2 + 2x_2y_1\\ &- 2x_1y_2), (x_2 - x_1)^3]\end{aligned}$$

En realidad, esta fórmula nos da la restricción de μ a $W_a \times_R W_a$, y en este esquema afín, μ será un morfismo excepto posiblemente en el subesquema cerrado donde las tres coordenadas se anulen. Si ponemos atención a la tercera coordenada y luego a la segunda, encontramos que μ es un morfismo de $W_a \times_R W_a$ excepto posiblemente para el subesquema cerrado definido por las ecuaciones $x_2 - x_1 = y_2 - y_1 = 0$, con lo que vemos que μ es un morfismo salvo posiblemente en la diagonal.

Para trabajar con los puntos en la diagonal, veamos las siguientes relaciones que son verdaderas en $W_a \times_R W_a$

$$y_1^2 = x_1^3 + ax_1 + b \quad \text{y} \quad y_2^2 = x_2^3 + ax_2 + b.$$

Usando estas igualdades, podemos reescribir las coordenadas de μ de la siguiente manera:

$$\begin{aligned}\mu[(x_1,y_1);(x_2,y_2)] = \\ &[(y_1+y_2)((x_1+x_2)(y_1+y_2)^2 + (x_1^2+x_1x_2+x_2^2+a)^2); \\ &(x_1^2+x_1x_2+x_2^2+a)^3 - (y_1+y_2)^2((x_1+x_2)^3 + a(x_1+x_2) \\ &+b - y_1y_2); (y_1+y_2)^3].\end{aligned}$$

Así, vemos que μ es un morfismo en $W_a \times_R W_a$ salvo posiblemente en el subesquema cerrado definido por las ecuaciones $y_1+y_2 = x_1^2+x_1x_2+x_2^2+a = 0$.

Juntando las ecuaciones, vemos que μ es un morfismo de $W_a \times_R W_a$ excepto en el subesquema definido por las ecuaciones

$$x_2 - x_1 = y_2 - y_1 = y_1 + y_2 = x_1^2 + x_1x_2 + x_2^2 + a = 0,$$

que, haciendo los cálculos y tomando en cuenta que $2 \in R^*$ resultan equivalentes a $x_1 = x_2$, $y_1 = y_2 = 0$, $3x_1^2 + a = 0$. Además vemos que este subesquema está metido en la diagonal. Si identificamos W_a con la diagonal de $W_a \times_R W_a$, entonces μ es un morfismo excepto en el subesquema dado por $y = 3x^2 + a = 0$. Usando la relación $y_1^2 = x_1^3+ax_1+b$ y el hecho que $3 \in R^*$, vemos que el discriminante $4a^3+27b^2$ está contenido en el ideal generado por y y $3x^2 + a$, entonces, si W es suave sobre R, lo que implica que el discriminante es una unidad en R,

tenemos que μ es un morfismo en todo $W_a \times_R W_a$. Análogamente, si W no es suave sobe R entonces μ será un morfismo en $W_a \times_R W_a$ salvo por el esquema dado por

$$x_2 = x_1, \quad y_1 = y_2 = 0, \quad 3x_1^2 + a, \quad 4a^3 + 27b^2 = 0,$$

que es, precisamente, el punto singular en la fibra especial de la diagonal.

Sea W_a' el subesquema afín abierto de W dado por

$$W_a' = \{y \neq 0\} \subset W.$$

Notemos que W está cubierto por los cuatro subesquemas afines

$$W_a \times_R W_a, \quad W_a \times_R W_a', \quad W_a' \times_R W_a, \quad W_a' \times_R W_a',$$

ya que W no intersecta al esquema $y = z = 0$. Así como mostramos que μ es un morfismo en $W_a \times_R W_a'$, de una manera análoga se puede mostrar que μ morfismo en los otros tres esquemas abiertos afines con lo que prácticamente hemos terminado. Sólo tenemos que ver que el mapeo inverso

$$i : W \times_R W \longrightarrow W, \quad [x, y.z] \longmapsto [x, -y, z],$$

es un morfismo en W, pero esto es verdad ya que es la restricción de un morfismo en $\mathbb{P}^2_R \times_R \mathbb{P}^2_R$.

□

Corolario 4.4.4. *Si E/K tiene buena reducción, entonces W es suave sobre R. Por lo que W es un grupo esquema sobre R.*

Demostración. La demostración es inmediata después de notar que bajo las condiciones del corolario, $W = W^0$ Después aplicamos el teorema. □

Ahora ilustremos lo anterior con unos ejemplos

Ejemplo 4.4.5. Notemos que el esquema W/R del teorema anterior 4.4.3, es propio sobre R ya que es un subesquema cerrado de $\mathbb{P}^2_R$. Del criterio valuativo para la propiedad concluimos que $W(R) = E(K)$ Sin embargo,

en general el esquema W no es regular, ya que un punto singular en la fibra especial es casi siempre singular en W. Estudiemos un caso particular.

Supongamos que E está dada por la ecuación

$$E : y^2z + xyz = x^3 + az^3,$$

donde $a \in R^*$. Aseguramos que W, el esquema asociado a E, es suave sobre R. En efecto,

$$\partial E/\partial x = yz - 3x^2, \quad \partial E/\partial y = 2yz + xz, \quad \partial E/\partial z = y^2 + xy - 3az62,$$

que no tienen ningún cero común el el proyectivo. Entonces W es un modelo de Nèron para E.

Si $a \notin R^*$ y $v(a) \geq 1$, entonces su fibra especial (la reducción módulo el parámetro uniformizador π)

$$W_P : y^2z + xyz = x^3.$$

W_P tiene como punto singular a $\alpha = [0, 0, 1]$ (o bién α es el ideal primo maximal $(x, y, z = 1, \pi)$). Entonces

$$W^0 = W - \{\alpha\}.$$

Como α no está en el subesquema $z = 0$, podemos deshomogeneizar respecto a z y decir que l ideal maximal $\mathcal{M}_{W,\alpha}$ del anillo local $\mathcal{O}_{W,\alpha}$ en el punto α está generado por x, y, π. Si $v(a) - 1$, entonces a es también un uniformizador de R y entonces

$$\pi \in aR = (y^2 + xy - x^3)R \subset \mathcal{M}^2_{W,\alpha},$$

y entonces $\mathcal{M}_{W,\alpha}/\mathcal{M}^2_{W,\alpha}$ está generado por x y y, lo que implica que

$$\mathcal{M}_{W,\alpha}/\mathcal{M}^2_{W,\alpha}$$

tiene dimensión dos como $\mathcal{O}_{W,\alpha}/\mathcal{M}_{W,\alpha}$-espacio vectorial y, por lo tanto, es W es regular en α. Del corolario 4.3.9 en la página 59 parte 3, deducimos que $W^0(R) = W(R) = E(K)$.

Si $v(a) \geq 2$, Entonces W no es un esquema regular y W^0 no será un modelo de Nèron para E aunque W^0 si es un grupo esquema con fibra genérica E ya que si por ejemplo $a = b^2$ con $v(b) \geq 1$, entonces el punto $t = (0, b) \in E(K) = W(R)$ no está en $W^0(R)$ ya que $t \equiv (0, 0) (\mathrm{mod}\, P)$, por lo que no es un modelo de Nèron.

Ejemplo 4.4.6. Bajo las condiciones de la definición del modelo de Nèron, si $\mathcal{X} = \operatorname{Spec} R$ y $X = \operatorname{Spec} K$, entonces el conjunto de K-mapeos de $X/K \to E/K$ coincide con $E(E)$ (ver ejemplo 3.4.3 en la página 35), y el conjunto de de R-morfismos es el grupo de secciones $\mathcal{E}(R)$. Entonces la propiedad del mapeo de Nèron nos dice que cada punto en $E(K)$ proviene de uno en $\mathcal{E}(R)$, es decir que el mapeo de inclusión natural

$$\mathcal{E}(R) \hookrightarrow E(K)$$

es también suprayectivo, por lo que hay una identificación (biyección) entre $E(K)$ y $\mathcal{E}(R)$.

Bibliografía

[AM69] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[Art84] M. Artin. Nèron models. In Gary Cornell and Joseph H. Silverman, editors, *Arithmetic Geometry*, pages 213–230. Springer-Verlag, 1984.

[EH99] D. Eisenbud and J. Harris. *The Geometry of Schemes.* Springer-Verlag, 1999.

[Ful69] W. Fulton. *Algebraic curves.* Benjamin, 1969.

[Har77] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1977.

[Jan96] G. J. Janusz. *Algebraic Number Fields*, volume 7 of *Graduate Studies in Mathematics* American Mathematical Society, 1996.

[Lor96] Dino Lorenzini. *An invitation to Arithmetic Geometry*, volume 9. American Mathematical Society, 1996.

[Mat80] H. Matsumura *Commutative Algebra.* Benjamin, 2nd edition, 1980.

[Mil96] J. S. Milne. Elliptic curves. University of Michigan, August 1996. Notes for a course.

[Mor96] Patrik Morandi. *Field and Galois Theory*, volume 167 of *Graduate Text in Mathematics.* Springer-Verlag, New York, 1996

[Ser73] J. P. Serre. *Cours of Arithmetic*, volume 7 of *GTM.* Springer-Verlag, 1973

[Ser79] J.P Serre *Local Fields.* Number 67 in GTM Springer-Verlag 1979

[Sil85] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. volume 106. Springer-Verlag, 1985.

[Sil94] Joseph H Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151 in GTM. Springer-Verlag, 1994.