EL HOMOMORFISMO DE MANIN PARA LA CURVA ELÍPTICA

ELIANA MILENA ZOQUE LÓPEZ
ASESOR: LUIS JAIME CORREDOR

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ, D.C., ENERO DE 2003

Índice de contenido

1 Introducción

En 1966 Manin publicó su artículo "Rational points of algebraic varieties over function fields" ([Man]) donde demostraba la conjetura de Mordell para curvas algebraicas sobre campos de funciones. La idea fundamental de este artículo es un homomorfismo que desde entonces se conoce como el homomorfismo de Manin. El siguiente paso es estudiar el kernel de este homomorfismo, que se conoce como el kernel de Manin. El kernel de Manin juega un papel importante en la demostración de la conjetura de Mordell, incluso en las demostraciones posteriores por Buium y Hrushovski.

El artículo de Manin comienza ilustrando la idea fundamental mediante el ejemplo de la curva elíptica $E : y^2 = x(x-1)(x-t), t \neq 0, 1$ que es una variedad abeliana. Básicamente, el razonamiento que aparece es el siguiente:

Sea γ un ciclo de dimensión 1 en C y sea $\omega = \dfrac{dx}{y}$. El período $\eta(t) = \displaystyle\int_\gamma \omega$, considerado como función de t, es una función infinitamente valuada. Estas funciones son soluciones de la ecuación diferencial lineal de Gauss:

$$2t(1-t)\frac{d^2\eta}{dt^2} + 2(1-2t)\frac{d\eta}{dt} - \frac{1}{2}\eta = 0.$$

El espacio de soluciones de esta ecuación tiene dimensión 2 y tiene como base a dos períodos $\eta_1(t) = \displaystyle\int_{\gamma_1} \omega$ y $\eta_2(t) = \displaystyle\int_{\gamma_2} \omega$ donde γ_1 y γ_2 son ciclos linealmente independientes que generan la homología de C.

La integral $\displaystyle\int_\infty^P \omega$ está bien definida módulo combinaciones lineales del tipo $m_1\eta_1(t) + m_2\eta_2(t)$. Para eliminar la indeterminación se aplica el operador de Gauss a ambos lados, ya que este elimina a $\eta_1(t)$ y $\eta_2(t)$. Así se obtiene la función

$$\mu(P) = \left(2t(1-t)\frac{d^2}{dt^2} + 2(1-2t)\frac{d}{dt} - \frac{1}{2}\right)\int_\infty^P \omega.$$

Además se tiene que

$$\int_\infty^P \omega + \int_\infty^Q \omega = \int_\infty^{P \oplus Q} \omega$$

donde $\oplus$ es la operación de grupo en C, tomando a ∞ como la identidad. Por esto y la linealidad del operador de Gauss se obtiene que $\mu(P) + \mu(Q) = \mu(P \oplus Q)$ así que μ es un homomorfismo de grupos.

Para hallar $\mu(P)$ de forma explícita se observa que

$$\left(2t(1-t)\frac{\partial^2}{\partial t^2} + 2(1-2t)\frac{\partial}{\partial t} - \frac{1}{2}\right)\frac{dx}{y} = \frac{1}{4}d\frac{y}{(x-t)^2}$$

donde ∂t denota la derivada parcial con respecto a t manteniendo a x fijo y d es el diferencial manteniendo a t fijo.

$$\mu(P) = \left(2t(1-t)\frac{d^2}{dt^2} + 2(1-2t)\frac{d}{dt} - \frac{1}{2}\right)\int_{\infty}^{P}\frac{dx}{y}$$

pero hay que tener en cuenta que P depende de t.

Manin obtiene la siguiente fórmula, que es ligeramente incorrecta:

$$\mu(P) = \frac{1}{2}\frac{y(t)}{(x(t)-t)^2} - \frac{d}{dt}\left(2t(t-1)\frac{\frac{d}{dt}x(t)}{y(t)}\right) - 2t(t-1)\frac{d}{dt}x(t)\frac{d}{dt}\left(\frac{1}{y(t)}\right).$$

En [Po], Pong corrige la fórmula de Manin y da una demostración de la validez de dicha fórmula, utilizando herramientas analíticas similares a las que utiliza Manin en la introducción de su artículo. La fórmula a la que llega Pong es

$$M(P(t)) = -\frac{y}{(x-t)^2} + \left(2t(t-1)\frac{x'}{y}\right)' + \frac{t(t-1)x'}{(x-t)y}$$

donde $'$ denota la derivada con respecto a t.

El objetivo de este trabajo es dar de manera formal una prueba algebraica de la validez de la fórmula del homomorfismo de Manin. En el segundo capítulo se dan preliminares de geometría algebraica necesarios para plantear y resolver el problema. En el tercer capítulo se halla la fórmula explícita para el homomorfismo de Manin. Para lograr esto se utilizarán las herramientas que Manin desarrolla en su artículo sobre ecuaciones de Picard-Fuchs y sistemas de cuasiparámetros. En el capítulo cuatro se muestra el enfoque estándar del homomorfismo de Manin usando teoría de modelos. Finalmente, en el apéndice se muestra la relevancia del kernel de Manin en la demostracion de la conjetura de Mordell-Lang.

2 Preliminares

2.1 Algunos conceptos algebraicos

2.1.1 Anillos Noetherianos y de valuación discreta

Definición 2.1. *Un anillo R es Noetheriano si todo ideal es finitamente generado. Equivalentemente, R es Noetheriano si toda cadena ascendente de ideales de R es eventualmente estacionaria.*

Teorema 2.2 (Teorema de la base de Hilbert). *Si R es noetheriano, $R[x]$ también lo es.*

La demostración se encuentra en [K]. Por inducción se demuestra que si R es Noetheriano $R[x_1, \cdots, x_n]$ es Noetheriano.

Definición 2.3. *Un anillo R es de valuación discreta si existe un elemento irreducible $T \in R$ tal que cada $z \in R$ no nulo se puede escribir de manera única en la forma $z = uT^n$, donde u es unidad y n un entero no negativo. Un $T \in R$ que satisfaga estas condiciones es un parámetro local de R.*

Lema 2.4. *Sea R un dominio noetheriano con un único ideal maximal que es principal. Entonces R es de valuación discreta.*

Demostración. Sea T un generador del ideal maximal M de R. Se mostrará que T satiface las condiciones de la definición.

Para verificar la unicidad supóngase que $uT^n = vT^m$, con u, v unidades y $n \geq m$. Entonces $uT^{n-m} = v$. $n = m$ pues de lo contrario $v \in M$, contradiciendo que v es unitario. Así que $uT^n = vT^n$ y como R es un dominio, $u = v$.

Ahora se mostrará que todo $z \in R$ no nulo puede ser expresado como vT^n. Si z es unidad se toma $v = z, n = 0$. En caso contrario el ideal generado por z es propio y está contenido en el maximal, luego $z \in M$. Por esto z se puede expresar de la forma $z = z_1T$. Si z_1 es unidad, ya se tiene la expresión deseada. Si no, se toma $z_1 = z_2T$ y se prosigue de este modo, tomando en cada paso $z_i = z_{i+1}T$ si z_i no es unidad. Supongamos que este proceso no acaba eventualmente. Por otro lado la cadena de ideales $(z_1) \subset (z_2) \subset \cdots$ se estabiliza, porque R es noetheriano. Sea $(z_n) = (z_{n+1})$. Existe $v \in R$ tal que $z_{n+1} = z_nv = z$ y por esto $z_n = z_{n+1}T = z_nTv$, luego $Tv = 1$, pero T no es unitario. $\square$

2.1.2 Derivaciones

Definición 2.5. *Sean $R \subset S$ anillos. Una derivación sobre R es una función $\delta : R \to S$ que satisface las siguientes condiciones para todo $x, y \in R$:*

1. $\delta(x+y) = \delta(x) + \delta(y)$.
2. $\delta(xy) = x\delta(y) + y\delta(x)$.

Un anillo diferencial es un anillo dotado de una derivación. Un campo diferencial es un anillo diferencial que además es un campo.

Definición 2.6. *Dado un campo diferencial K, el campo de constantes de K es el campo $\{a \in K \mid \delta(a) = 0\}$.*

Es fácil verificar que el campo de constantes es en efecto un campo y que si K es algebraicamente cerrado de característica cero, su campo de constantes también es algebraicamente cerrado.

Se mostrará una herramienta que es muy útil para mostrar que una función es una derivación. Dado un anillo S, se define el anillo de números duales de S del siguiente modo:

$$S[\epsilon] = S[x]/(x^2) = \{a + b\epsilon \mid a, b \in S\}$$

donde $\epsilon = x \bmod x^2$. Sea $\pi : S[\epsilon] \to S$ definida por $\pi(a + b\epsilon) = b$.

Lema 2.7. *Toda derivación $\delta : R \to S$ define un homomorfismo*

$$t_\delta : R \to S[\epsilon], t_\delta(a) = a + (\delta a)\epsilon$$

el cual levanta a π, es decir $\pi \circ t_\delta = \delta$. Además, para toda función $\delta : R \to S$, t_δ es un homomorfismo si y sólo si δ es una derivación.

Demostración. $t_\delta(a+b) = t_\delta(a) + t_\delta(b)$ si y sólo si $\delta(a+b) = \delta(a) + \delta(b)$.

$t_\delta(ab) = ab + \delta(ab)\epsilon$. Por otro lado

$$\begin{aligned} t_\delta(a)t_\delta(b) &= (a + (\delta a)\epsilon)(b + (\delta b)\epsilon) \\ &= ab + ((\delta a)b + a(\delta b))\epsilon + (\delta a)(\delta b)\epsilon^2 \\ &= ab + ((\delta a)b + a(\delta b))\epsilon \end{aligned}$$

Luego t_δ es homomorfismo si y sólo si δ es una derivación. □

Lema 2.8. *Sea $\delta : R \to S$ una derivación y sean $s_1, \cdots, s_n \in S$. Entonces existe una única derivación $\delta' : R[x_1, \cdots, x_n] \to S$ que extiende a δ tal que $\delta'(x_i) = s_i$.*

Demostración. Se extiende $t_\delta : R \to S[\epsilon]$ a $t_{\delta'} : R[x_1, \cdots, x_n] \to S$ mediante

$$t_{\delta'}(x_i) = x_i + s_i\epsilon.$$

$t_{\delta'}$ es un homomorfismo, luego $\delta' = \pi \circ t_{\delta'}$ es una derivación. La unicidad es clara. $\square$

Lema 2.9. *Sean S un campo, R un subanillo de S y $\bar{R}$ el campo de cocientes de R. Sea $\delta : R \to S$ una derivación. Entonces existe una única extensión $\bar{\delta} : \bar{R} \to S$.*

Demostración. Se quiere extender t_δ a $\bar{R}$ con la regla usual de derivación. Pero todo $t_\delta(r)$ es unidad en $S[\epsilon]$, y si $\delta r = s$ se tiene que

$$\begin{aligned}(r + s\epsilon)^{-1} &= \frac{1}{r}\left(1 + \frac{s}{r}\epsilon\right)^{-1} \\ &= \frac{1}{r}\left(1 - \frac{s}{r}\epsilon\right) \\ &= \frac{1}{r} - \frac{s}{r^2}\epsilon.\end{aligned}$$

Luego t_δ se extiende de manera única a $\bar{R}$, por $\bar{\delta}\left(\frac{1}{r}\right) = -\frac{1}{r^2}\delta r$. $\square$

2.2 Variedades

2.2.1 Variedades afines

A continuación se darán algunos conceptos básicos de la geometría algebraica. Estos conceptos pueden encontrarse en [Hu],[K],[Sh2], [Sp]. Frecuentemente ésto se hace con campos algebraicamente cerrados, pero en este trabajo K sera un campo arbitrario y k un subcampo de K.

Definición 2.10. *Un subconjunto $V \subseteq K^n$ es una variedad afín definida sobre k si existen polinomios $f_1, \cdots, f_m \in k[x] = k[x_1, \cdots, x_n]$ tales que V es el conjunto solución en K^n del sistema de ecuaciones $f_i(x) = 0;\ i = 1, \cdots, m$. Un subconjunto de V que es una variedad se llama una subvariedad de V.*

Definición 2.11. *Dado un subconjunto $X \in K^n$ el conjunto de polinomios que se anulan en X forman un ideal de $K[x_1, \cdots, x_n]$ que se llama el ideal de X y se denota por $I(X)$.*

Lema 2.12. *Intersección arbitraria de variedades afines es igual a una subintersección finita.*

Esto se sigue facilmente del Teorema 2.2, ya que K al ser un campo es Noetheriano.

Definición 2.13. *Para una variedad afín V se define su topología de Zariski como aquella que tiene como cerrados a las subvariedades de V.*

Se verifica que en efecto es una topología utilizando el Lema anterior.

Definición 2.14. *Una variedad V es irreducible si no existen subvariedades propias y no vacías V_1, V_2 de V tales que $V = V_1 \cup V_2$. Equivalentemente, V es irreducible si no se puede expresar como la unión de dos cerrados de Zariski propios.*

La demostración del siguiente Lema se encuentra en [K].

Lema 2.15. *V es irreducible si y solo si $I(V)$ es primo.*

Definición 2.16. *Sea V una variedad afín. Se define el anillo coordenado $K[V]$ de V como $K[x_1 \cdots, x_n]/I(V)$. Si V es irreducible $K[V]$ es un dominio y se puede formar su campo de cocientes $K(V)$ que se llama el campo de funciones racionales de V.*

Definición 2.17. *La dimensión de una variedad irreducible V es el grado de trascendencia del campo de funciones $K(V)$ sobre K y se denota por $\dim V$.*

Definición 2.18. *Sean $V \subset K^n, W \subset K^m$ variedades afines. Un morfismo de V en W es una función $f = (f_1, \cdots, f_n) : V \to W$ tal que $f_i \in K[V]$ para todo i.*

Definición 2.19. *Una variedad cuasi-afín es un subconjunto abierto de una variedad afín. Toda variedad cuasi-afín está dotada de la topología de subespacio.*

Definición 2.20. *Sea $V \subset K^n$ una variedad afín.*

1. *Una función parcial f de V en K es regular en $a \in V$ si existen un abierto de U de V con $a \in U$ y polinomios $P, Q \in K[x_1 \cdots, x_n]$ tales que Q no se anula en ningún punto de U y además sobre U vale que $f = \dfrac{P}{Q}$. Dos funciones regulares se identifican si coinciden en su dominio común.*
2. *El anillo local en a es el anillo formado por las funciones regulares en a y se denota por $\mathcal{O}_a$. Este anillo tiene un único ideal maximal $\mathcal{M}_a = \{r \in \mathcal{O}_a | r(a) = 0\}$.*
3. *Sea U un subconjunto abierto de V. Una función $f : U \to K$ es regular si es regular en cada punto de U.*
4. *Sean U_1 y U_2 variedades cuasi-afines. $f : U_1 \to U_2$ es morfismo si sus funciones componentes son regulares en U_1. Un isomorfismo es un morfismo inyectivo cuyo inverso también es morfismo.*

Definición 2.21. *Una variedad (abstracta) es un conjunto V con un recubrimiento $V_1, \cdots, V_m$; y por cada i una biyección $f_i : V_i \to U_i$, donde U_i es una variedad afín, tal que para cualesquiera i, j, con $1 \leq i, j \leq m$ se tiene lo siguiente:*

1. *$U_{ij} = f_i(V_i \cap V_j)$ es abierto en U_i.*

2. $f_j \circ f_i^{-1}$ *es un isomorfismo entre las variedades cuasi-afines* U_{ij} *y* U_{ji}*.*

Una variedad tiene su propia topología de Zariski definida del siguiente modo: $U \subset V$ *es abierto si, para cada* i*,* $f_i(U \cap V_i)$ *es abierto en* U_i*. Una función racional de* V *en* K *es un morfismo de un subconjunto abierto de* V *en* K*. Se identifican dos funciones racionales si coinciden en su dominio común. El conjunto de funciones racionales de* V *forma un campo* $K(V)$*.*

2.2.2 Variedades proyectivas

Definición 2.22. *El espacio proyectivo* n*-dimensional* $\mathbb{P}^n(K)$ *sobre el campo* K *es el conjunto de rectas de* K^{n+1} *que pasan por el origen.*

Todo punto $(a_0, \cdots, a_n) \neq 0$ determina una sola de estas rectas, que es $\{(\lambda a_0, \cdots, \lambda a_n) \mid \lambda \in K\}$. Además todo elemento de $\mathbb{P}^n(K)$ puede ser representado de esta forma. Dos puntos $(a_0, \cdots, a_n)$ y $(b_0, \cdots, b_n)$ determinan la misma recta si y solo si existe $\lambda \in K$ no nulo tal que $a_i = \lambda b_i$ para todo $i = 0, \cdots, n$. Una $(n+1)$-tupla que representa un elemento $a \in \mathbb{P}^n$ se llama un sistema de coordenadas homogéneas para a y se escribe $a = (a_0 : \cdots : a_n)$.

Definición 2.23. *Un subconjunto* $V \subseteq \mathbb{P}^n$ *es una variedad proyectiva si existen polinomios homogéneos* $F_1, \cdots, F_m \in K[x_0 \cdots, x_n]$ *tales que* V *es el conjunto solución del sistema de ecuaciones* $F_i(x) = 0;\ i = 1, \cdots, m$*.*

Las definiciones de funciones regulares y anillos locales pueden extenderse al caso proyectivo, pero en este caso los polinomios con los cuales se hacen los cocientes deben ser homogéneos del mismo grado para garantizar la buena definición.

Sea $U_i = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(K) | a_i \neq 0\}$. Cada $a \in U_i$ posee un único sistema de coordenadas homogéneas de la forma $(a_0, \cdots, a_{i-1}, 1, a_{i+1}, \cdots, a_n)$. Las coordenadas $(a_0, \cdots, a_{i-1}, a_{i+1}, \cdots, a_n)$ son las coordenadas no homogéneas de a con respecto a U_i. Se define $f_i : K^n \to U_i$ del siguiente modo: $f_i(a_0, \cdots, a_{i-1}, a_{i+1}, \cdots, a_n) = (a_0, \cdots, a_{i-1}, 1, a_{i+1}, \cdots, a_n)$. Esto hace de $\mathbb{P}^n(K)$ una variedad según la Definición 2.21.

Para un polinomio homogéneo $G \in K[x_1, \cdots, x_{n+1}]$ se define $G_* = G(x_1, \cdots, x_n, 1)$. Reciprocamente, para todo $g \in K[x_1, \cdots, x_n]$ se define $g^* = x_{n+1}^{\deg(g)} g\left(\frac{x_1}{x_{n+1}}, \cdots, \frac{x_n}{x_{n+1}}\right)$. Estos procesos se llaman "homogenizar" y "deshomogenizar" polinomios con respecto a x_{n+1}, respectivamente.

Por lo general $\mathbb{P}^n(K) \setminus U_n = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(K) \mid a_n = 0\}$ se denomina el hiperplano del infinito. Mediante f_n es posible identificar a K^n como un subconjunto de $\mathbb{P}^n(K)$.

2.3 Formas diferenciales

Sea $f \in K[x] = K[x_1, \cdots, x_n]$. $D_{x_i} f$ representa su derivada parcial respecto a la variable x_i. $(D_x f)(a)$ es el vector en K^n cuya i-ésima componente es $(D_{x_i} f)(a)$.

Definición 2.24. *Sea $V \subseteq K^n$ una variedad afín definida por los polinomios $f_1, \cdots, f_m$. Se define el espacio tangente de una variedad afín como*

$$T(V) = \{(a, u) \mid a \in V, (D_x f_j)(a) \cdot u = 0 \text{ para } j = 1, \cdots, m\}.$$

El espacio tangente en $a \in V$ es $T_a(V) = \{u \mid (a, u) \in T(V)\}$. Claramente $T_a(V)$ es un K-espacio vectorial.

Definición 2.25. *V es una variedad suave en el punto a si $\dim T_a(V) = \dim V$.*

Definición 2.26. *Sean $V \subseteq K^n$ y $W \subseteq K^m$ variedades afines, y sea $\varphi : V \to W$ una función regular. $\varphi = (\varphi_1, \cdots, \varphi_m)$ donde $\varphi_i : K^n \to K$. Para cada $a \in V$ se define la aplicación lineal $d\varphi_a : T_a(V) \to T_{\varphi(a)}(W)$ del siguiente modo:*

$$d\varphi_a u = ((D_x \varphi_1)(a) \cdot u, \cdots, (D_x \varphi_m)(a) \cdot u).$$

La definición anterior se extiende a $K(V)$ del modo natural. Es fácil ver que esta definición es buena.

Definición 2.27. *Una m-forma diferencial ω sobre V es una función que asigna a cada $a \in V$ un funcional multilineal y alternado $\omega_a : T_a(V)^m \to K$. Una función $f : V \to K$ se considera una 0-forma.*

Por ejemplo, toda función regular $\varphi : V \to K$ induce una 1-forma diferencial $d\varphi$, donde $d\varphi_a$ es como se definió anteriormente, identificando $T_{\varphi(a)K}$ con K. Para el presente trabajo solo nos interesarán las 0-formas y las 1-formas. Dos operaciones importantes entre formas diferenciales son el producto exterior y la derivada exterior. Sus definiciones se encuentran en [Wa]. El producto exterior se denota por $\wedge$. Para el caso de 0-formas, la definición del producto exterior coincide con el producto usual. La demostración del siguiente Lema se encuentra en [Wa].

Lema 2.28. *El conjunto de formas diferenciales sobre V forma un álgebra, con la suma definida del modo natural y el producto exterior.*

A continuación se describen algunas propiedades de las formas diferenciales que se siguen facilmente de la definición.

Lema 2.29. *Sean $f, g : V \to K$ regulares y ω una m-forma.*

1. $d(f + g) = df + dg$.

2. *$d(fg) = f\ dg + g\ df$.*

3. *$d(f\omega) = f\ d\omega + df \wedge \omega$.*

4. *$d(af) = a\ df$ si $a \in K$.*

5. *$df = D_{x_1} f\ dx_1 + \cdots + D_{x_n} f\ dx_n$, es decir,*

$$df_a u = (D_{x_1} f)(a)\ dx_1(u) + \cdots + (D_{x_n} f)(a)\ dx_n(u)$$

   donde x_i es la i-ésima proyección.

6. *Toda 1-forma ω se puede expresar de la forma*

$$\omega = f_1\ dx_1 + \cdots + f_n\ dx_n$$

   donde $f_j : V \to K, j = 1, \cdots, n$.

7. *$d \circ d = 0$.*

Una forma diferencial es regular en P si las funciones $f_1, \cdots, f_n$ de la parte *6.* del Lema 2.29 son regulares en P.

Definición 2.30. *La derivada exterior de una 1-forma $\omega = f_1\ dx_1 + \cdots + f_n\ dx_n$ es $d\omega = df_1 \wedge dx_1 + \cdots + df_n \wedge dx_n$*

Definición 2.31. *Una forma ω es cerrada si $d\omega = 0$ y es exacta si $\omega = d\eta$ para alguna forma η.*

Definición 2.32. *Sean V y W variedades algebráicas, $f : V \to W$ regular y ω una forma diferencial regular sobre W. Se define la forma $f^*\omega$ sobre V, llamada el pull-back de ω, de la siguiente manera:*

$$f^*\omega_p(u) = \omega_{f(p)}(df_p u).$$

Lema 2.33.

1. *$f^*(dg) = d(f^*g) = d(g \circ f)$.*

2. *$f^*(\omega_1 + \omega_2) = f^*(\omega_1) + f^*(\omega_2)$.*

3. *$f^*(g\omega) = (g \circ f) \cdot f^*(\omega)$.*

Demostración. *1.* En primer lugar es claro que $f^*g = g \circ f$. Además

$$d(g \circ f)_p(u) = (D_x(g \circ f))(p) \cdot u,$$

$$f^*(dg)_p(u) = (dg)_{f(p)}(df_p u) = (D_x g)(f(p))\left((D_x f_1)(p) \cdot u, \cdots, (D_x f_1)(p) \cdot u\right)$$

y ambas expresiones coinciden por la regla de la cadena.

2. Es evidente.

3.

$$f^*(g\omega)_p(u) = (g\omega)_{f(p)}(df_p u) = g(f(p))\omega_{f(p)}(df_p u) = (g \circ f)(p) f^*(\omega).$$

□

2.4 La curva elíptica

2.4.1 Grupos algebraicos

Definición 2.34. *Un grupo algebraico es una variedad G dotada de morfismos $\mu : G \times G \to G$ y $\iota : G \to G$ tales que G es un grupo con multiplicación μ e inverso ι.*

Lema 2.35. *Sea G un grupo algebraico y sea H un subgrupo de G.*

1. *La clausura de Zariski de H es subgrupo de G.*

2. *Si H es construible(combinación booleana de cerrados) entonces es cerrado en G.*

La demostración se encuentra en [Pi2].

Teorema 2.36. *Un grupo algebráico es suave en todos sus puntos.*

La demostración se encuentra en [Pi2]. La idea es mostrar que existe por lo menos un punto donde la variedad es suave, y por medio de el morfismo de multiplicación es posible mostrar que cualquier otro punto también lo es.

Definición 2.37. *Sea G un grupo algebráico. Una forma diferencial sobre G es invariante si $(\lambda^g)^*\omega = \omega$ para todo $g \in G$, donde λ^g es la multiplicación a izquierda por g.*

Teorema 2.38. *Si G es un grupo algebráico d-dimensional, las 1-formas diferenciales invariantes sobre G forman un K-espacio vectorial d-dimensional.*

Demostración. Se mostrará que el espacio de las formas diferenciales invariantes sobre G es isomorfo al espacio dual de K^d. Sea h un elemento fijo de G y sea ω una forma invariante bajo traslaciones. $\omega_h : T_h(G) \to K$ puede ser identificado con un elemento del dual de K^d, ya que por el Teorema 2.25 $T_h(G)$ es un K-espacio vectorial de dimensión d. Ahora se mostrará que toda función lineal $\gamma : T_h(G) \to K$ determina de manera única una forma ω invariante bajo traslaciones tal que $\gamma = \omega_h$. Esto se sigue del hecho de que si ω es invariante bajo traslaciones entonces

$$\omega_g(u) = (\lambda^{hg^{-1}})^*\omega_g(u) = \omega_h(d\lambda_g^{hg^{-1}}(u))$$

□

El concepto de variedad abeliana es fundamental para todo lo que vamos a hacer. Para dar la definición se necesitan unos conceptos preliminares.

Definición 2.39. *Una variedad X es completa si para toda variedad Y la proyección $\pi : X \times Y \to Y$ es cerrada.*

En [Sh1, I.5.] se muestra que toda variedad proyectiva es completa.

Lema 2.40. *Sea X una variedad completa e irreducible. Entonces toda función regular $f : X \to K$ es constante.*

Demostración. Sea $Z = \{(x, y) \in X \times K \mid f(x)y = 1\} \subset X \times K$. Z es cerrado en $X \times K$, luego la proyección $\pi(Z)$ en K es cerrada, pero los únicos cerrados de Zariski K son K mismo y sus subconjuntos finitos. Como $0 \notin \pi(Z)$, entonces $\pi(Z)$ es igual a un conjunto finito de puntos. Pero $\pi(Z)$ es irreducible, luego es un singleton. Así que f es constante. $\square$

Como corolario del Lema anterior se tiene que todo morfismo de una variedad completa e irreducible en una variedad afín es constante.

Definición 2.41. *Un grupo algebraico es conexo si es irreducible; es decir, si su variedad subyacente es irreducible. Una variedad abeliana es un grupo algebráico conexo cuya variedad subyacente es completa.*

En [Pi2] se muestra que toda variedad abeliana es un grupo abeliano.

2.4.2 Divisores

Sea K algebraicamente cerrado. Un polinomio en $K[x]$ está determinado de manera única, excepto por un factor constante, por sus raíces con sus respectivas multiplicidades. Similarmente una función racional $\varphi(x) = f(x)/g(x)$, con $f, g \in K[x]$, está determinada, excepto por un factor constante, por las raíces de f y de g. Es decir, por los polos y los ceros de φ, con sus respectivas multiplicidades. Para distinguir las multiplicidades de las raíces de f y las de g, a estas últimas se las considerará con signo negativo.

Se desea hacer un análogo de esto para funciones racionales sobre curvas. Un tratamiento completo del tema, para variedades algebráicas arbitrarias, se encuentra en [Sh2].

Definición 2.42. *Una curva algebraica plana es el conjunto de puntos del plano afín K^2 cuyas coordenadas x, y satisfacen una ecuación polinomial no constante $f(x, y) = 0$.*

Teorema 2.43. *Para cada punto regular P de una curva algebráica irreducible plana el anillo local $\mathcal{O}_P$ es de valuación discreta.*

Demostración. $\mathcal{O}_P$ es un anillo noetheriano ([F, 2.4]). Por el Lema 2.4 es suficiente probar que $\mathcal{M}_P$ es principal. Sea $f(x,y)=0$ la ecuación polinomial que define a la curva y sea $P=(a,b)$. Haciendo el cambio de variables $x'=x-a, y'=y-b$ se puede suponer sin perder generalidad que $P=(0,0)$. Como P es un punto regular, se puede suponer que $D_y f(P)\neq 0$. Separando los términos que contienen sólo a x se escribe $f(x,y)$ de la forma $x\varphi(x)+y(\beta+h(x,y))=0$, con β constante no nula y $h(0,0)=0$. Sobre la curva $f(x,y)=0$ se tiene que $y(\beta+h(x,y))=-x\varphi(x)$, lo cual implica $y=vx$ con $v(x,y)=-\dfrac{\varphi(x)}{\beta+h(x,y)}$. v es regular en P pues $\beta+h(P)=\beta\neq 0$. Sea $u=\dfrac{p}{q}\in\mathcal{M}_P; p,q\in K[x,y]$. $p(P)=0, q(P)\neq 0$. Entonces $p(x,y)=p(x,vx)=xr$ para una función regular r, pues p no tiene término independiente. Luego $u=xu_1$ donde $u_1=\dfrac{r}{q}$ es una función racional regular en P. Luego $\mathcal{M}(P)$ está generado por x. □

De la demostración del Teorema 2.43 se concluye que si $D-yf(P)\neq 0$ entonces $x-P_1$ es un parámetro local. Si $z=ux^n$, a n se le denota por $ord_P(z)$, el orden de z en P. La definición de $ord_P(z)$ se puede extender de forma natural a $K(V)\setminus 0$ pues todo elemento de $K(V)$ es cociente de polinomios. Se verifica facilmente que estas definiciones no dependen del parámetro local T ni de el representante de un elemento de $K(V)$.

Definición 2.44. *Sea A una curva irreducible. $Div(A)$ es el grupo abeliano libre generado por los puntos de A. Sus elementos son llamados divisores de A. El grado de un divisor D es la suma de sus coeficientes y se denota por $deg(D)$.*

Definición 2.45. *Sea u una función racional sobre A. Se define el divisor de u como*

$$div(u)=\sum_{P\in A} ord_P(u)P.$$

Esta es en efecto una suma finita. La demostración se encuentra en [Sh2, III.1.]. Estas definiciones pueden extenderse a curvas proyectivas tomando entornos afines y deshomogenizando los polinomios correspondientes.

Definición 2.46. *Un divisor de la forma $div(u)$ para $u\in K(A)$ es un divisor principal. El conjunto $P(A)$ de divisores principales forma un subgrupo de $Div(A)$. El grupo cociente $Div(A)/P(A)$ es el grupo de clases de divisores de A y se denota por $Cl(A)$.*

Teorema 2.47. *El grado de un divisor principal en una curva proyectiva no singular es igual a cero.*

La demostración se encuentra en [Sh2, III.2].

El Teorema anterior muestra que se puede definir el homomorfismo

$$deg: Cl(A)\to\mathbb{Z}$$

del modo natural. Su kernel se denota por $Cl^0(A)$.

La demostración del siguiente teorema se encuentra en [F, 5.3] y [Sh2, III.2].

Teorema 2.48 (Teorema de Bezout). *Sean F y G curvas planas proyectivas que no tienen componentes comunes. Entonces*

$$FG = (deg\ F)(deg\ G)$$

donde deg X representa el grado del polinomio que define a la curva X y FG es el número de intersección de F y G que se define como

$$FG = \sum_{P \in F} ord_P(g).$$

donde g es el polinomio que define a G y $ord_P(g)$ se calcula sobre F.

2.4.3 La operación de grupo

Definición 2.49. *Sea K un campo algebráicamente cerrado y $t \in K, t \neq 0, 1$. Se define E_t como la curva cuya ecuación en coordenadas proyectivas es $Y^2Z = X(X-Z)(X-tZ)$. Su parte afín es $\{(x,y) \in K^2 | y^2 = x(x-1)(x-t)\}$ y tiene un punto en el infinito cuyas coordenadas proyectivas son $(0:1:0)$ y que será denotado por ∞.*

Teorema 2.50. *Sea $\alpha_0 \in E_t$. Se considera la aplicación $E_t \to Cl^0(E_t)$ que a cada $\alpha \in E_t$ le asigna la clase de divisores C_α que contiene a $\alpha - \alpha_0$. Esta asignación es una biyección entre E_t y $Cl^0(E_t)$.*

Demostración. Sea $\sim$ la relación de equivalencia entre los divisores inducida por $P(A)$. Es decir, dos divisores están relacionados si difieren por un divisor principal. La demostración de la inyectividad se encuentra en [Sh2, III.2, III.3].

Para la sobreyectividad se requiere la siguiente observación: Para cualesquiera $\beta, \gamma \in E_t$ existe $\alpha \in E_t$ tal que $\beta + \gamma \sim \alpha + \alpha_0$. Para comprobar la veracidad de esta afirmación, sea L la recta que pasa por los puntos β y γ (si $\beta = \gamma$ se toma la tangente). Por el Teorema de Bézout $divL = \beta + \gamma + \delta$ para algun $\delta \in L$. Sea L_1 la recta que pasa por los puntos δ y α_0 (nuevamente se toma la tangente si $\delta = \alpha_0$.). $div(L_1) = \delta + \alpha_0 + \alpha$ para algún α. Como $divL \sim divL_1$ se tiene que $\beta + \gamma + \delta \sim \delta + \alpha_0 + \alpha$ de donde se obtiene el resultado.

Para completar la demostración, sea D un divisor con $deg(D) = 0$. Separando coeficientes positivos y negativos D puede expresarse de la forma $D_1 - D_2$ donde todos los coeficientes en D_1 y D_2 son positivos. Aplicando la observación anterior sucesivamente se concluye que $D_1 \sim P + k\alpha_0$ y $D_2 \sim Q + k'\alpha_0$. Pero $deg(D_1) = deg(D_2)$, luego $k = k'$. Por lo tanto $D = D_1 - D_2 \sim P - Q$. Aplicando nuevamente la observación se obtiene α tal que $Q + \alpha \sim P + \alpha_0$ lo cual implica $\alpha - \alpha_0 \sim P - Q \sim D$.

□

Este resultado permite transferir la estructura de grupo de $Cl^0(E_t)$ a E_t. Para un α_0 fijo se define la adición $\oplus$ del siguiente modo: $P \oplus Q = R$ si y solo si $C_P + C_Q = C_R$.

Claramente α_0 es la identidad. La operación se puede definir en términos geométricos: Sea S el tercer punto de intersección de E_t con la recta que pasa por P y Q; y sea R el tercer punto de intersección de E_t con la recta que pasa por los puntos α_0 y S. Entonces

$$P + Q + S \sim S + R + \alpha_0$$

$$P + Q \sim R + \alpha_0$$

lo cual implica $C_P + C_Q = C_R$ y por lo tanto $P \oplus Q = R$.

Durante el resto de este trabajo se tomará $\alpha_0 = \infty$.

Teorema 2.51. *E_t es una variedad abeliana, con la operación $\oplus : E_t \times E_t \to E_t$ definida del modo anteriormente descrito. Si $(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$, la fórmula explícita para la operación es*

$$x_3 = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} + 1 + t - x_1 - x_2.$$

$$y_3 = -\frac{(y_1 - y_2)\left(\frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} + 1 + t - x_1 - 2x_2\right)}{x_1 - x_2} - y_2.$$

Demostración. La ecuación de una recta que pasa por ∞ es $x = c$. La ecuación de la línea que pasa por los puntos (x_1, y_1) y (x_2, y_2) es

$$y - y_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1). \tag{2.1}$$

Los tres puntos de intersección de la cúbica con esta recta están dados por

$$\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1) + y_1\right)^2 = x(x-1)(x-t).$$

Dos de las raíces de esta ecuación son x_1 y x_2. La tercera raíz es

$$x_3 = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} + 1 + t - x_1 - x_2.$$

Finalmente, $y_3 = -y$ donde y se obtiene reemplazando $x = x_3$ en la ecuación 2.1. $\square$

Definición 2.52. *Sea K un campo (no necesariamente algebraicamente cerrado) y $t \in K, t \neq 0, 1$. Sea $\bar{K}$ la clausura algebráica de K. Sobre $\bar{K}$ se puede definir la curva elíptica como en la Definición 2.49. Sea E el conjunto de puntos de E_t con coordenadas en K. De la definición de la operación se deduce que E es un subgrupo de E_t.*

La curva elíptica E_t es uno de los ejemplos clásicos de variedades abelianas. Otros ejemplos son $(K, +)$ y $(K \setminus 0, \cdot)$; pero estos son muy simples ya que su estructura de grupo está "explícita" y directamente relacionada con $(K, +, \cdot)$.

3 El homomorfismo de Manin para la curva elíptica

De ahora en adelante, sea $K = \mathbb{C}(t)$. K es un campo diferencial con la derivación usual ∂, es decir, $\partial t = 1$ y $\partial a = 0$ para todo $a \in \mathbb{C}$. En realidad, es posible tomar K como un campo que contenga a $k_0(t)$, si t es trascendente sobre k_0, donde k_0 es un campo de característica cero. Como ∂ se puede tomar cualquier derivación de K que se anule en k_0 y tal que $\partial(t) = 1$. E denotará E o E_t, según sea el caso. Sea $L = K(E)$, el campo de funciones racionales sobre E.

El objetivo de este capítulo es hallar de forma explicita un homomorfismo no trivial $M : (E, \oplus) \to (K, +)$.

Lema 3.1. *La extensión L/K tiene grado de trascendencia uno, y x, la primera proyección, es base de trascendencia.*

Demostración. Claramente x es trascendente sobre K. L como extensión de K está generado por x y y; pero son algebraicamente dependientes pues $y^2 = x(x-1)(x-t)$. □

3.1 Formas diferenciales sobre la curva elíptica

Lema 3.2. *Dada una derivación δ de K, una base de trascendencia v de L/K y un elemento arbitrario $a \in L$, existe una única derivación $\bar{\delta}$ de L que extiende a δ y tal que $\bar{\delta}(v) = a$.*

Esto se sigue de los Lemas 2.8 y 2.9. Nótese que para definir ∂ se ha utilizado este resultado, pues se ha definido ∂ para $\mathbb{C}$ y para t que es base de trascendencia de $K/\mathbb{C}$.

Definición 3.3. *Para v base de trascendencia de L/K sea δ_v la derivación que es trivial en K y tal que $\delta_v(v) = 1$.*

En realidad, esta es la derivada con respecto a v en el sentido usual, es decir, $\delta_v = \dfrac{d}{dv}$.

Lema 3.4. *Sea s base de trascendencia de L/K y sea $v \in L$. Entonces $dv = \delta_s v \ ds$.*

En la notación usual se tiene que $dv = \dfrac{dv}{ds}\ ds$.

Demostración. Se verifica facilmente que $D_x - (D_x s)\delta_s : L \to L$ es una derivación que se anula en K y en s, luego $D_x - (D_x s)\delta_s = 0$. En particular $D_x v = (D_x s)\delta_s v$. Similarmente $D_y v = (D_y s)\delta_s v$. Entonces, si $a \in E$ y $u = (u_1, u_2) \in T_a(E)$, se tiene que

$$\begin{aligned} dv_a(u) &= (D_x v)(a)u_1 + (D_y v)(a)u_2 \\ &= (D_x s)(a)\delta_s v(a)u_1 + (D_y s)(a)\delta_s v(a)u_2 = (\delta_s v)(a)\ ds_a(u). \end{aligned}$$

Esto concluye la demostración. $\square$

Un caso importante del teorema anterior es $dy = \delta_x y\ dx$. Para calcular $\delta_x y$ se aplica δ_x a la igualdad $y^2 = x(x-1)(x-t)$ para obtener

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

Luego

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

El conjunto de 1-formas diferenciales de L/K se denotará por Ω. Este conjunto está formado por elementos de la forma $\omega = g_1\ dx + g_2\ dy = (g_1 + g_2\delta_x y)\ dx$. Por esto todos los elementos de Ω son de la forma $\omega = g\ dx$. Se sigue que las formas de orden dos sobre la curva elíptica se anulan, ya que $g\ dx \wedge h\ dx = 0$.

Sean B y Z, respectivamente, los espacios de formas diferenciales exactas y cerradas sobre la curva elíptica.

Teorema 3.5. *Excepto por múltiplos escalares, la única forma diferencial invariante sobre E es $\omega = \dfrac{dx}{y}$.*

Demostración. Por el Teorema 2.38, el espacio de formas invariantes es de dimensión uno; así que es suficiente demostrar que $\omega = \dfrac{dx}{y}$ es invariante. En primer lugar, para toda $F = (F_1, F_2) : E \to E$ se tiene que $F^*\left(\dfrac{dx}{y}\right) = \dfrac{dF_1}{F_2}$; en efecto

$$F^*\left(\frac{dx}{y}\right)_P (u) = \left(\frac{dx}{y}\right)_{F(P)} (dF_P(u)) = \frac{1}{F_2(P)}\, dx\left((dF_1)_P(u), (dF_2)_P(u)\right) = \frac{(dF_1)_P}{F_2(P)}(u).$$

Luego para verificar que ω es invariante es suficiente comprobar que para todo $g \in E$ y $F = \lambda^g$ vale que

$$\frac{dx}{y} = \frac{dF_1}{F_2}.$$

Pero por el Lema anterior

$$dF_1 = \delta_x F_1\ dx$$

Un cálculo directo muestra que $\delta_x F_1 = \dfrac{F_2}{y}$, en efecto, si $g = (g_1, g_2)$ se tiene que

$$F_1(x,y) = \frac{(y-g_2)^2}{(x-g_1)^2} + 1 + t - x - g_1.$$

$$F_2(x,y) = -\frac{y-g_2}{x-g_1}\,(F_1 - g_1) - g_2.$$

Luego

$$F_2 + y = -\frac{y-g_2}{x-g_1}\,(F_1 - g_1) - g_2 + y = \frac{y-g_2}{x-g_1}\,(x - F_1)$$

$$\frac{F_2}{y}+1=\frac{y-g_2}{y(x-g_1)}\,(x-F_1)$$

Por otro lado

$$\delta_x(F_1)=2\left(\frac{y-g_2}{x-g_1}\right)\delta_x\left(\frac{y-g_2}{x-g_1}\right)-1.$$

Así que es suficiente demostrar que

$$\frac{x-F_1}{y}=2\delta_x\left(\frac{y-g_2}{x-g_1}\right). \tag{3.1}$$

Pero

$$x-F_1=-\frac{(y-g_2)^2}{(x-g_1)^2}-1-t+2x+g_1=\frac{-(y-g_2)^2+(x-g_1)^2(-1-t+2x+g_1)}{(x-g_1)^2}$$

y

$$\delta_x\left(\frac{y-g_2}{x-g_1}\right)=\frac{(x-g_1)\delta_x(y)-(y-g_2)}{(x-g_1)^2}.$$

Por lo que la ecuación (3.1) se convierte en

$$-(y-g_2)^2+(x-g_1)^2(-1-t+2x+g_1)=2y((x-g_1)\delta_x(y)-(y-g_2))$$

o equivalentemente

$$2y(x-g_1)\delta_x(y)=2y(y-g_2)-(y-g_2)^2+(x-g_1)^2(-1-t+2x+g_1). \tag{3.2}$$

El lado derecho es igual a

$$\begin{aligned}
&y^2-g_2^2+(x-g_1)^2(-1-t+2x+g_1)\\
&=x^3-(1+t)x^2+tx-g_1^3+(1+t)g_1^2-tg_1+(x-g_1)^2(-1-t+2x+g_1)\\
&=(x-g_1)\left(x^2+xg_1+g_1^2-(1+t)(x+g_1)+t+(x-g_1)(-1-t+2x+g_1)\right)\\
&=(x-g_1)\left(x^2+xg_1+g_1^2-2x(1+t)+t+(x-g_1)(2x+g_1)\right)\\
&=(x-g_1)\left(x^2+xg_1+g_1^2-2x-2xt+t+2x^2-xg_1-g_1^2\right)\\
&=(x-g_1)\left(3x^2-2x-2xt+t\right)=2y(x-g_1)\delta_x(y).
\end{aligned}$$

Esto concluye la demostración. □

3.2 Ecuaciones de Picard-Fuchs

Definición 3.6. *Para toda base de trascendencia v de L/K se define $\partial_v : L\to L$ como la derivación que extiende a ∂ y que satisface $\partial_v(v)=0$. Esta derivación se puede extender al L-módulo de formas diferenciales de L/K del siguiente modo:*

$$\partial_v\,(u\ dv)=\partial_v(u)\ dv.$$

Se verifica fácilmente que en efecto es una derivación.

Lema 3.7. *Para toda forma diferencial ω se tiene que $d(\partial_v \omega) = \partial_v(d\omega)$.*

Demostración. Se mostrará que $d \circ \partial_v - \partial_v \circ d : L \to \Omega$ es cero. Claramente $d \circ \partial_v - \partial_v \circ d$ es una derivación sobre L que se anula en K y en v. El Lema 3.2 muestra que $d \circ \partial_v - \partial_v \circ d = 0$. $\square$

Lema 3.8. *Sean v y s dos bases de trascendencia de L/K. Sea $\omega = u\ ds$. Entonces $(\partial_v - \partial_s)\omega = d\varphi$ donde $\varphi = u\partial_v s$.*

Demostración. Es fácil ver que $\partial_v - \partial_s - (\partial_v s)\delta_s : L \to L$ es una derivación que se anula en K y en s. Utilizando un argumento similar al de la demostración anterior se concluye que $\partial_v - \partial_s = \partial_v s \delta_s$ sobre L. Luego

$$
\begin{aligned}
(\partial_v - \partial_s)(u\ ds) &= (\partial_v u)\ ds + u\partial_v(ds) - (\partial_s u)\ ds \\
&= (\partial_v - \partial_s)u\ ds + u\ d(\partial_v s) \\
&= \partial_v s\,(\delta_s u)\ \ ds + u\ d(\partial_v s) \\
&= \partial_v s\,(du) + u\ d(\partial_v s) \\
&= d(u\partial_v s).
\end{aligned}
$$

$\square$

Definición 3.9. *$v \in L$ es un cuasiparámetro en $P \in E$ si $v - v(P)$ genera a $\mathcal{M}_P$, es decir, si $v - v(P)$ es parámetro local de $\mathcal{O}_P$. Dicho cuasiparámetro es admisible si además $\delta(v(P)) = 0$ para toda derivación δ sobre K.*

Lema 3.10. *Sea v un cuasiparámetro en P entonces $\partial_v(\mathcal{O}_P) \subset \mathcal{O}_P$ y $\delta_v(\mathcal{O}_P) \subset \mathcal{O}_P$.*

La demostración se encuentra en [Man].

Lema 3.11. *Si ω e una forma diferencial regular y cerrada en P y sea v un cuasiparámetro en P. Entonces $\partial_v \omega$ es regular y cerrada en P.*

Demostración. Que $\partial_v(\omega)$ es regular en P es inmediato por el Lema anterior; y que es cerrada se sigue del Lema 3.7. $\square$

Lema 3.12. *Sea v un cuasiparámetro admisible en P. Entonces $(\partial_v u)(P) = \partial(u(P))$ para todo $u \in \mathcal{O}_P$.*

Demostración. $\partial_v(v - v(P)) = \partial_v v - \partial_v(v(P)) = 0 - \partial(v(P)) = 0$. Esto implica que $\partial_v(\mathcal{M}_P) \subset \mathcal{M}_P$ pues todo elemento de $\mathcal{M}_P$ es de la forma $g(v - v(P))$. En particular, como $u - u(P) \in \mathcal{M}_P$, $\partial_v(u - u(P)) = \partial_v u - \partial_v(u(P)) = \partial_v u - \partial(u(P)) \in \mathcal{M}_P$. Luego $0 = (\partial_v u - \partial(u(P)))(P) = (\partial_v u)(P) - (\partial(u(P)))(P) = (\partial_v u)(P) - \partial(u(P))$. Esto concluye la demostración. $\square$

Definición 3.13. *Un operador diferencial* $\mathcal{L} : K \to K$ *es un operador de la forma* $\mathcal{L} = a_m\partial^m + a_{m-1}\partial^{m-1} + \cdots + a_1\partial + a_0$, *con* $a_0 \cdots, a_n \in K$. *El conjunto de los operadores diferenciales es un* K*-espacio vectorial que se llama el espacio de operadores en* K. *Para toda* v *base de trascendencia de* L/K *se define* $\mathcal{L}_v : L \to L$ *como el operador obtenido al reemplazar cada ocurrencia de* ∂ *en* $\mathcal{L}$ *por* ∂_v.

El operador $\mathcal{L}_v$ se puede extender al módulo de las formas diferenciales como se hizo anteriormente. Por el Lema 3.7 $\mathcal{L}_v$ induce una acción sobre Z/B que es independiente de v por el Lema 3.8 Esta acción será denotada por $\mathcal{L}$.

Definición 3.14. *Una ecuación de Picard-Fuchs es una relación de la forma*

$$\mathcal{L}\bar{\omega} = 0$$

donde $\mathcal{L}$ *es un operador diferencial y* $\bar{\omega}$ *es la clase de* ω *en* Z/B. *Una representación de la anterior ecuación de Picard-Fuchs es una relación de la forma*

$$\mathcal{L}_v\omega = dz_v$$

donde v *es una base de trascendencia de* L/K *y* z_v *es una 0-forma.*

3.3 La función μ

Lema 3.15. *Si existe un cuasiparámetro común para* $P, Q \in E$, *entonces existe un cuasiparámetro admisible común para esos puntos.*

Demostración. Sea v un cuasiparámetro en P y Q. Si $v(P) = v(Q)$ se toma $v' = v - v(P)$ que claramente es un cuasiparámetro admisible.

Si $v(P) \neq v(Q)$, sea $v' = \dfrac{v - v(P)}{v(Q) - v(P)}$. Claramente $v'(P) = 0, v'(Q) = 1$. v' es un cuasiparamertro admisible en P, Q. En efecto, es cuasiparámetro pues

$$v' - v'(P) = \frac{v - v(P)}{v(Q) - v(P)},\ v' - v'(Q) = \frac{v - v(Q)}{v(Q) - v(P)}$$

por lo que $v' - v'(P)$ y $v' - v'(Q)$ generan a $\mathcal{M}_P$ y $\mathcal{M}_Q$, respectivamente. Y es admisible pues $v'(P)$ y $v'(Q)$ están en el campo primo. □

De ahora en adelante sea $\mathcal{L}\bar{\omega} = 0$ una ecuación de Picard-Fuchs en E, donde $\omega = \frac{dx}{y}$ es la 1-forma invariante bajo traslaciones de E.

Definición 3.16. *Sea* v *un cuasiparámetro admisible en los puntos* $P, Q \in E$. *Supóngase que la ecuación de Picard-Fuchs* $\mathcal{L}\bar{\omega} = 0$ *tiene una representación* $\mathcal{L}_v\omega = dz_v$. *Se define*

$$\mu_v(P, Q) = z_v(Q) - z_v(P).$$

A continuación se demostrará que $\mu_v(P,Q)$ es independiente del cuasiparámetro admisible v.

Lema 3.17. *Sea $\omega \in Z$ una forma regular en P y Q y sea $\mathcal{L}$ cualquier operador diferencial. Sean v, s cuasiparámetros admisibles en P y Q. Sea z tal que $(\mathcal{L}_v - \mathcal{L}_s)\omega = dz$. Entonces $z \in \mathcal{O}_P \cap \mathcal{O}_Q$ y $z(P) = z(Q)$.*

Demostración. Sea $\omega = u\ dx$. Por el Lema 3.11 se tiene que dz es regular en P y Q, Luego $z \in \mathcal{O}_P \cap \mathcal{O}_Q$. Para la otra afirmación del Lema es suficiente demostrarla para monomios diferenciales, es decir, para $\mathcal{L} = \partial^m$. La prueba es por inducción en m. Para $m = 1$ se tiene por el Lema 3.8 que $(\partial_v - \partial_s)\omega = dz$ donde $z = u\partial_v s$. Por el Lema 3.12

$$z(P) = u(P)\left((\partial_v s)(P)\right) = u(P)\left(\partial(s(P))\right) = 0.$$

Un argumento similar muestra que $z(Q) = 0$.

Para el paso inductivo se considera el operador diferencial ∂^{m+1}. Por el Lema 3.11 $\partial_v^{m+1}\omega$ es cerrada y regular en P. Notese que

$$\left(\partial_v^{m+1} - \partial_s^{m+1}\right) = \partial_v\left(\partial_v^m - \partial_s^m\right) + \left(\partial_v - \partial_s\right)\partial_s^m$$

Por hipótesis de inducción y por el caso $m = 1$ se tiene que

$$\left(\partial_v^m - \partial_s^m\right)\omega = dz_1, \left(\partial_v - \partial_s\right)\partial_s^m\omega = dz_2$$

con $z_1(P) = z_1(Q)$ y $z_2(P) = z_2(Q)$. Luego

$$dz = \left(\partial_v^{m+1} - \partial_s^{m+1}\right)\omega = \partial_v\left(\partial_v^m - \partial_s^m\right)\omega + \left(\partial_v - \partial_s\right)\partial_s^m\omega = \partial_v(dz_1) + dz_2 = d(\partial_v(z_1) + z_2).$$

Se sigue que

$$z(P) = \left(\partial_v(z_1)\right)(P) + z_2(P) = \partial(z_1(P)) + z_2(P) = \partial(z_1(Q)) + z_2(Q) = z(Q).$$

Esto concluye la prueba para monomios diferenciales. □

Lema 3.18. *$\mu_v(P,Q)$ es independiente del cuasiparámetro admisible v.*

Demostración. Sean v, s cuasiparámetros admisibles en P y Q. Sean z_v, z_s tales que $\mathcal{L}_v\omega = dz_v$ y $\mathcal{L}_s\omega = dz_s$. Luego $d(z_v - z_s) = (\mathcal{L}_v - \mathcal{L}_s)\,\omega$ y por el Lema anterior $(z_v - z_s)(P) = (z_v - z_s)(Q)$, lo cual implica $\mu_v(P,Q) = \mu_s(P,Q)$. □

El valor común de $\mu_v(P,Q)$ se denotará por $\mu(P,Q)$.

Teorema 3.19. *Si P y Q tienen un cuasiparámetro común entonces $\mu(P,Q) = \mu(P \oplus R, Q \oplus R)$ para cualquier $R \in E$.*

Demostración. Sea v un cuasiparámetro para P, Q. Por el Lema 3.15 se puede suponer que v es admisible. Sea $\lambda = \lambda^{\ominus R}$, es decir, $\lambda : E \to E, S \mapsto S \ominus R$. λ induce un automorfismo de L mediante la composición, es decir, $u \mapsto u \circ \lambda$, el cual es la identidad en K. Por esto $v \circ \lambda$ es cuasiparámetro admisible en $P \oplus R$ y $Q \oplus R$.

A continuación se mostrará que

$$\partial_{v\circ\lambda}(u \circ \lambda) = (\partial_v u) \circ \lambda.$$

Se considera la aplicación $\gamma : L \to L, u \mapsto (\partial_{v\circ\lambda}(u \circ \lambda)) \circ \lambda^{-1}$. Se verifica facilmente que γ es una derivación. Además

$$\gamma(v) = (\partial_{v\circ\lambda}(v \circ \lambda)) \circ \lambda^{-1} = 0 \circ \lambda^{-1} = 0$$

y para todo $k \in K$ se tiene que

$$\gamma(k) = (\partial_{v\circ\lambda}(k \circ \lambda)) \circ \lambda^{-1} = (\partial(k)) \circ \lambda^{-1} = \partial(k)$$

pues $\partial(k) \in K$. Se concluye que $\gamma = \partial_v$ y por lo tanto $\partial_{v\circ\lambda}(u \circ \lambda) = (\partial_v u) \circ \lambda$.

Ahora se mostrará que $\partial_{v\circ\lambda}(\lambda^*\omega') = \lambda^*(\partial_v\omega')$ para toda 1-forma ω'. Sea $\omega' = u\ dv$. Por las propiedades en 2.33 se tiene que

$$\lambda^*\left(\omega'\right) = \lambda^*(u\ dv) = (u \circ \lambda)\lambda^*(dv) = (u \circ \lambda)\ d(u \circ \lambda).$$

Luego

$$\partial_{v\circ\lambda}(\lambda^*\omega') = \partial_{v\circ\lambda}((u \circ \lambda)\ d(u \circ \lambda)) = \partial_{v\circ\lambda}((u \circ \lambda))\ \ d(u \circ \lambda).$$

Por otro lado

$$\lambda^*\left(\partial_v\omega'\right) = \lambda^*(\partial_v(u\ dv)) = \lambda^*(\partial_v u\ dv) = (\partial_v u \circ \lambda) \cdot \lambda^*(dv) = (\partial_v u \circ \lambda)\ \ d(v \circ \lambda)$$

y ambas expresiones coinciden pues $\partial_{v\circ\lambda}(u \circ \lambda) = (\partial_v u) \circ \lambda$.

Ahora, volviendo a la representación de la ecuacion de Picard-Fuchs

$$\mathcal{L}_v\omega = dz_v, \mathcal{L} = a_m\partial^m + a_{m-1}\partial^{m-1} + \cdots + a_1\partial + a_0$$

y aplicando λ^* se obtiene al lado izquierdo

$$\lambda^*(\mathcal{L}_v\omega) = \lambda^*\left(\sum a_i\partial_v^i\omega\right) = \sum a_i\lambda^*\left(\partial_v^i\omega\right) = \sum a_i\left(\partial_{v\circ\lambda}^i\omega\right) = \mathcal{L}_{v\circ\lambda}\omega$$

y al lado derecho, por 2.33, $\lambda^*(dz_v) = d(\lambda^* z_v) = d(z_v \circ \lambda)$.

Por lo tanto $d(z_v \circ \lambda) = \mathcal{L}_{v\circ\lambda}\omega = dz_{v\circ\lambda}$, así que se puede tomar $z_{v\circ\lambda} = z_v \circ \lambda$.

Finalmente,

$$\begin{aligned}\mu(P \oplus R, Q \oplus R) &= z_{v\circ\lambda}(Q \oplus R) - z_{v\circ\lambda}(P \oplus R)\\ &= (z_v \circ \lambda)(Q \oplus R) - (z_v \circ \lambda)(P \oplus R) = z_v(Q) - z_v(P) = \mu(P, Q).\end{aligned}$$

□

Nótese que si P, Q, R tienen un sistema común de cuasiparámetros, entonces se obtiene trivialmente de la definición de μ que.

$$\mu(P,Q) + \mu(Q,R) = \mu(P,R).$$

En el artículo de Manin([Man]) una vez se ha definido $\mu(P,Q)$ y se ha demostrado la igualdad anterior para cualquier par de puntos, el homomorfismo de Manin se define del siguiente modo:

$$\mu(P) = \mu(O,P)$$

donde O es la identidad del grupo. Esto es en efecto homomorfismo pues

$$\mu(P) + \mu(Q) = \mu(O,P) + \mu(O,Q) = \mu(O,P) + \mu(P, P \oplus Q) = \mu(O, P \oplus Q) = \mu(P \oplus Q).$$

3.4 El cálculo explícito

Teorema 3.20. *En E vale la ecuación de Picard-Fuchs $\mathcal{L}\bar{\omega} = 0$, donde $\mathcal{L} = 2t(1-t)\partial^2 + 2(1-2t)\partial - \frac{1}{2}$. Una representación de la ecuación anterior es*

$$\mathcal{L}_x \omega = d\frac{y}{(x-t)^2}.$$

Un desarrollo completo de esta ecuación de Picard-Fuchs se encuentra en [Po]. En este trabajo sólo se mostrará la validez de esta fórmula.

Demostración. Aplicando ∂_x a $y^2 = x(x-1)(x-t)$ se obtiene

$$2y\partial_x y = (\partial_x x)(x-1)(x-t) + (\partial_x(x-1))x(x-t) + (\partial_x(x-t))x(x-1) = -x(x-1).$$

Luego

$$\partial_x y = -\frac{x(x-1)}{2y} = -\frac{y}{2(x-t)}.$$

Se sigue que

$$\partial_x\left(\frac{1}{y}\right) = \frac{1}{2(x-t)y}$$

y

$$\begin{aligned}\partial_x^2\left(\frac{1}{y}\right) = \partial_x\left(\frac{1}{2(x-t)y}\right) &= -\frac{\partial_x(x-t)y + (x-t)\partial_x y}{2(x-t)^2y^2} \\ &= \frac{y + (x-t)\dfrac{y}{2(x-t)}}{2(x-t)^2y^2} = \frac{3y}{4(x-t)^2y^2} = \frac{3}{4(x-t)^2y}\end{aligned}$$

Entonces

$$\partial_x(\omega) = \frac{1}{2(x-t)y}\ dx$$

y

$$\partial_x^2(\omega) = \frac{3}{4(x-t)^2 y}\, dx.$$

Por otra parte,

$$\begin{aligned}
d\left(\frac{y}{(x-t)^2}\right) &= \delta_x\left(\frac{y}{(x-t)^2}\right)\, dx = \frac{\delta_x y(x-t)^2 - y\delta_x((x-t)^2)}{(x-t)^4}\, dx \\
&= \frac{\delta_x y(x-t) - 2y}{(x-t)^3}\, dx = \frac{y\delta_x y(x-t) - 2x(x-1)(x-t)}{y(x-t)^3}\, dx \\
&= \frac{y\delta_x y - 2x(x-1)}{y(x-t)^2}\, dx = \frac{(x-1)(x-t) + x(x-t) + x(x-1) - 4x(x-1)}{2y(x-t)^2}\, dx \\
&= \frac{(x-1)(x-t) + x(x-t) - 3x(x-1)}{2y(x-t)^2}\, dx.
\end{aligned}$$

Reemplazando x por $(x-t)+t$ donde sea necesario se obtiene

$$\begin{aligned}
&(x-1)(x-t) + x(x-t) - 3x(x-1) \\
&= ((x-t)+t-1)(x-t) + ((x-t)+t)(x-t) - 3((x-t)+t)((x-t)+t-1) \\
&= -(x-t)^2 - 2(x-t)(2t-1) - 3t(t-1).
\end{aligned}$$

Se sigue que

$$\begin{aligned}
d\left(\frac{y}{(x-t)^2}\right) &= \frac{-(x-t)^2 - 2(x-t)(2t-1) - 3t(t-1)}{2y(x-t)^2}\, dx \\
&= -\frac{1}{2y}\, dx - \frac{2t-1}{y(x-t)}\, dx - 3\frac{t(t-1)}{2y(x-t)^2}\, dx = -\frac{1}{2}\omega + 2(1-2t)\partial_x(\omega) + 2t(1-t)\partial_x^2(\omega)
\end{aligned}$$

□

A continuación se realizará el cálculo explícito del homomorfismo de Manin. La ecuación que define a la curva elíptica es $y^2 - x(x-1)(x-t) = 0$ y la derivada parcial con respecto a y del lado izquierdo de esta igualdad es $2y$. De la observación después del Teorema 2.43 se sigue que x es un cuasiparámetro para todos aquellos puntos afines de E para los cuales $y \neq 0$. De ahora en adelante sean $P = (P_1, P_2), Q = (Q_1, Q_2)$ puntos de E distintos de $\infty, (0,0), (1,0), (t,0)$. La primera proyección x es cuasiparámetro para P y Q. Como en 3.15,

$$v = \frac{x(P) - x}{x(P) - x(Q)} = \frac{P_1 - x}{P_1 - Q_1}$$

es un cuasiparámetro admisible para P y Q. Se encontrará la representación de la ecuación de Picard-Fuchs para el cuasiparámetro v.

Como v es un cuasiparámetro admisible

$$(\partial_v x)(P) = \partial(P_1),\ (\partial_v x)(Q) = \partial(Q_1)$$

y

$$(\partial_v^2 x)(P) = \partial^2(P_1),\ (\partial_v^2 x)(Q) = \partial^2(Q_1).$$

Por el Lema 3.8 se tiene que $(\partial_v - \partial_x)\,\omega = d\varphi$ donde $\varphi = \dfrac{\partial_v x}{y}$. Por otro lado,

$$\left(\partial_v^2 - \partial_x^2\right)\omega = \partial_v\left(\partial_v - \partial_x\right)\omega + \left(\partial_v - \partial_x\right)\partial_x\omega.$$

Se analizarán por aparte ambos sumandos.

$$\partial_v\left(\partial_v - \partial_x\right)\omega = \partial_v\left(d\varphi\right) = d\left(\partial_v\varphi\right)$$

por el Lema 3.7. Utilizando nuevamente el Lema 3.8 se obtiene

$$\left(\partial_v - \partial_x\right)\partial_x\omega = \left(\partial_v - \partial_x\right)\partial_x\left(\frac{dx}{y}\right) = \left(\partial_v - \partial_x\right)\left(\partial_x\left(\frac{1}{y}\right)dx\right) = d\left(\partial_x\left(\frac{1}{y}\right)\partial_v x\right).$$

Luego

$$\left(\partial_v^2 - \partial_x^2\right)\omega = d\left(\partial_v\varphi\right) + d\left(\partial_x\left(\frac{1}{y}\right)\partial_v x\right) = d\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \partial_x\left(\frac{1}{y}\right)\partial_v x\right).$$

Con estos resultados es posible hacer el cálculo. Sea $\mathcal{L}$ el operador diferencial del enunciado del Teorema 3.20.

$$\begin{aligned}
(\mathcal{L}_v - \mathcal{L}_x)\omega &= \left(2t(1-t)\left(\partial_v^2 - \partial_x^2\right) + 2(1-2t)\left(\partial_v - \partial_x\right)\right)\omega \\
&= 2t(1-t)d\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \partial_x\left(\frac{1}{y}\right)\partial_v x\right) + 2(1-2t)d\left(\frac{\partial_v x}{y}\right) \\
&= d\left(2t(1-t)\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \partial_x\left(\frac{1}{y}\right)\partial_v x\right) + 2(1-2t)\left(\frac{\partial_v x}{y}\right)\right) \\
\mathcal{L}_v\omega &= \mathcal{L}_x\omega + d\left(2t(1-t)\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \partial_x\left(\frac{1}{y}\right)\partial_v x\right) + 2(1-2t)\left(\frac{\partial_v x}{y}\right)\right) \\
&= d\left(\frac{y}{(x-t)^2} + 2t(1-t)\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \partial_x\left(\frac{1}{y}\right)\partial_v x\right) + 2(1-2t)\left(\frac{\partial_v x}{y}\right)\right)
\end{aligned}$$

Así que utilizando la identidad $\partial_x\left(\dfrac{1}{y}\right) = \dfrac{1}{2(x-t)y}$, la cual se mostró al comienzo de la demostración del Teorema 3.20, se obtiene que

$$\begin{aligned}
z_v &= \frac{y}{(x-t)^2} + 2t(1-t)\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \partial_x\left(\frac{1}{y}\right)\partial_v x\right) + 2(1-2t)\left(\frac{\partial_v x}{y}\right) \\
&= \frac{y}{(x-t)^2} + 2t(1-t)\left(\partial_v\left(\frac{\partial_v x}{y}\right) + \frac{\partial_v x}{2(x-t)y}\right) + 2(1-2t)\left(\frac{\partial_v x}{y}\right) \\
&= \frac{y}{(x-t)^2} + 2t(1-t)\left(\frac{(\partial_v^2 x)y - (\partial_v x)(\partial_v y)}{y^2} + \frac{\partial_v x}{2(x-t)y}\right) + 2(1-2t)\left(\frac{\partial_v x}{y}\right)
\end{aligned}$$

Se sigue que

$$z_v(P) = \frac{P_2}{(P_1-t)^2}+2t(1-t)\left(\frac{(\partial^2 P_1)P_2-(\partial P_1)(\partial P_2)}{P_2^2}+\frac{\partial P_1}{2(P_1-t)P_2}\right)+2(1-2t)\left(\frac{\partial P_1}{P_2}\right)$$

o equivalentemente

$$z_v(P) = \frac{P_2}{(P_1-t)^2}+2\partial\left(t(1-t)\frac{\partial P_1}{P_2}\right)+t(1-t)\left(\frac{\partial P_1}{(P_1-t)P_2}\right). \qquad (3.3)$$

Nótese que esta expresión no depende de Q, ni de v.

Con esto se puede calcular

$$\mu_v(P,Q) = z_v(Q)-z_v(P)$$

$$\mu(P,Q) = \frac{Q_2}{(Q_1-t)^2}+2t(1-t)\left(\frac{(\partial^2 Q_1)Q_2-(\partial Q_1)(\partial Q_2)}{Q_2^2}+\frac{\partial Q_1}{2(Q_1-t)Q_2}\right)+2(1-2t)\left(\frac{\partial Q_1}{Q_2}\right)$$

$$-\frac{P_2}{(P_1-t)^2}-2t(1-t)\left(\frac{(\partial^2 P_1)P_2-(\partial P_1)(\partial P_2)}{P_2^2}+\frac{\partial P_1}{2(P_1-t)P_2}\right)-2(1-2t)\left(\frac{\partial P_1}{P_2}\right).$$

Es conveniente expresar este resultado de otra forma para eliminar indeterminaciones. Aplicando ∂ a la igualdad $P_2^2 = P_1(P_1-1)(P_1-t)$ se obtiene

$$2P_2\partial P_2 = (\partial P_1)(3P_1^2-2P_1(t+1)-t)-P_1(P_1-1).$$

Luego

$$\partial P_1 = \frac{2P_2\partial P_2+P_1(P_1-1)}{3P_1^2-2P_1(t+1)-t}$$

y

$$\begin{aligned}\frac{\partial P_1}{P_2} &= \frac{2P_2\partial P_2+P_1(P_1-1)}{P_2(3P_1^2-2P_1(t+1)-t)}\\ &= \frac{2\partial P_2}{3P_1^2-2P_1(t+1)-t}+\frac{P_2}{(P_1-t)(3P_1^2-2P_1(t+1)-t)}.\end{aligned}$$

Sea $\gamma(P)$ igual a esta última expresión. Reemplazando en la ecuación 3.3 se obtiene

$$z_v(P) = \frac{P_2}{(P_1-t)^2}+2\partial\left(t(1-t)\gamma(P)\right)+t(1-t)\left(\frac{\gamma(P)}{P_1-t}\right). \qquad (3.4)$$

Luego

$$\begin{aligned}\mu(P,Q) = \frac{Q_2}{(Q_1-t)^2}&+2\partial\left(t(1-t)\gamma(Q)\right)+t(1-t)\left(\frac{\gamma(Q)}{Q_1-t}\right)\\ &-\frac{P_2}{(P_1-t)^2}2\partial\left(t(1-t)\gamma(P)\right)-t(1-t)\left(\frac{\gamma(P)}{P_1-t}\right).\end{aligned}$$

Esta fórmula es valida para $P,Q\in E\setminus\{(t,0),\infty\}$.

3.4.1 El homomorfismo

Sea $P \in E$ arbitrario. Por el Teorema 3.19 $\mu(R, R \oplus P)$ es independiente de R. Sea $M(P)$ este valor común. El dominio de M es E, ya que siempre es posible encontrar R de modo que $R, R \oplus P \neq (t,0), \infty$.

Lema 3.21. *M es homomorfismo de grupos.*

Demostración. Para mostrar que M es homomorfismo, sean $P, Q \in E$ elementos arbitrarios y sea R tal que $R, R\oplus P, R \oplus P \oplus Q \neq (t,0), \infty$. Entonces

$$\begin{aligned} &M(P) + M(Q) = \mu(R, R\oplus P) + \mu(R\oplus P, R\oplus P\oplus Q) \\ &= z_v(R\oplus P) - z_v(R) + z_v(R\oplus P\oplus Q) - z_v(R\oplus P) = \mu(R, R\oplus P\oplus Q) = M(P\oplus Q). \end{aligned}$$

□

Ahora solo falta hallar la fórmula explícita para el homomorfismo.

Lema 3.22. *Sean $P, Q \in E \setminus \{(t,0), \infty\}$. Entonces $M(P) - z_v(P) = M(Q) - z_v(Q)$.*

Demostración. Si $P\oplus Q \neq (t,0), \infty$ entonces $M(P) = \mu(Q, P\oplus Q) = z_v(P\oplus Q) - z_v(Q)$ y $M(P) + z_v(Q) = z_v(P\oplus Q)$. Analogamente $M(Q) + z_v(P) = z_v(P\oplus Q)$. Se concluye que $M(P) - z_v(P) = M(Q) - z_v(Q)$. Si $P\oplus Q = (t,0), \infty$ se escoge R tal que $P\oplus R, Q\oplus R \neq (t,0), \infty$. Por el razonamiento anterior se tiene que $M(P) - z_v(P) = M(R) - z_v(R) = M(Q) - z_v(Q)$. □

Por la ecuación 3.4 se tiene que $z_v(0,0) = z_v(1,0) = 0$. De la fórmula para la operación de grupo se verifica facilmente que $(0,0) \oplus (0,0) = \infty$, luego $M(0,0) = 0$ pues la característica del campo es cero. Luego $M(P) - z_v(P) = 0$ para todo $P \in E \setminus \{(t,0), \infty\}$. Del hecho que $(t,0) \oplus (t,0) = \infty$ se sigue que $M(t,0) = 0$. En conclusión

$$M(P) = \begin{cases} 0 & P = (t,0), \infty \\ \dfrac{P_2}{(P_1 - t)^2} + 2\partial\left(t(1-t)\gamma(P)\right) + t(1-t)\left(\dfrac{\gamma(P)}{P_1 - t}\right) & P \neq (t,0), \infty \end{cases}$$

o equivalentemente

$$M(P) = \begin{cases} 0 & P = (0,0), (1,0), (t,0), \infty \\ \frac{P_2}{(P_1-t)^2} + 2t(1-t)\left(\frac{(\partial^2 P_1)P_2 - (\partial P_1)(\partial P_2)}{P_2^2} + \frac{\partial P_1}{2(P_1-t)P_2}\right) & \\ \qquad\qquad + 2(1-2t)\left(\frac{\partial P_1}{P_2}\right) & P \neq (0,0), (1,0), (t,0), \infty \end{cases}$$

4 El kernel de Manin en general

Este capítulo muestra la aproximación de Pillay al kernel de Manin, como se muestra en [Pi1]. Se asumen conceptos de teoría de modelos como definibilidad, rango de Morley, saturacion y estabilidad. Estos conceptos pueden encontrarse en [Z].

4.1 Rango de Morley en grupos ω-estables

Definición 4.1. *Un grupo ω-estable es un grupo G, posiblemente con estructura adicional, tal que la teoría de G, con su estructura adicional, es ω-estable.*

En los grupos ω-estables, el rango de Morley es una herramienta muy fuerte.

Es fácil probar el siguinte Lema utilizando las propiedades del rango y el grado de Morley.

Lema 4.2. *Sea G un grupo ω-estable, y sean $H' \subseteq H$ subgrupos definibles de G.*

1. *Si $[H' : H]$ es finito, $MR(H) = MR(H')$ y $Md(H) = Md(H') \cdot [H' : H]$.*
2. *Si $[H' : H]$ es infinito, $MR(H) > MR(H')$.*

De esto se sigue inmediatamente el siguiente Lema.

Lema 4.3. *No existe una cadena decreciente infinita de subgrupos definibles de un grupo ω-estable. En particular la intersección de cualquier clase de subgrupos definibles es igual a una subintersección finita.*

Lema 4.4. *Un grupo algebraico es conexo si no tiene subgrupos propios definibles de índice finito*

Este Lema se demuestra utilizando el hecho de que todo grupo ω-estable tiene un único subgrupo de índice finito minimal y que las componente irreducibles son exactamente las clases laterales de este subgrupo minimal. La demostración completa se encuentra en [Pi2].

El Lema 4.2 prueba una implicación del siguiente Lema. La otra implicación requiere más trabajo y se encuentra en [Las]

Lema 4.5. *Sea G ω-estable. G es conexo si y sólo si $Md(G) = 1$.*

De ahora en adelante K será un campo diferencial de característica cero, lo suficientemente saturado. Abusando de la notación, K también representará la estructura $(K, +, \cdot, \partial)$ y K^- representará a la estructura $(K, +, \cdot)$. Además sean MR, MR^- el rango de Morley en K y K^-, respectivamente. La palabra definible se reservará para definible en K^-, y ∂-definible se utilizará para definible en K.

Del Lema anterior se deduce que el grado de Morley(en K^-) de toda variedad abeliana es igual a uno pues por definición una veriedad abeliana es un grupo conexo. Para calcular el rango de Morley se necesita el siguiente resultado.

Lema 4.6.

1. *Sea* $a \in K^n$. *Entonces* $MR^-(a/K) = tr.deg(K(a)/K)$.
2. *Sea* V *una variedad irreducible. Entonces* $MR^-(V) = tr.deg(K(V)/K)$.

La demostración está en [Pi2]. De esto se deduce que el rango de Morley(en K^-) de una variedad abeliana es igual a su dimensión.

Para encontrar el rango y el grado de Morley en K de una variedad abeliana, se necesitan los siguientes Lemas

Lema 4.7. *Sea* X *un conjunto definible en* K^-. *Entonces* $MR(X) = \omega MR^-(X)$.

Lema 4.8. *Un grupo definible y conexo es* ∂*-conexo.*

Las demostraciones de estos Lemas están en [Wo] y [Mar2], respectivamente.

4.2 El caso de la curva elíptica.

Por los resultados de la sección anterior se tiene que para una curva elíptica E vale que $MR^-(E) = 1, Md^-(E) = 1, MR(E) = \omega, Md(E) = 1$.

Lema 4.9. *Sea* K *un campo algebraicamente cerrado y sea* A *una variedad abeliana sobre* K. *Entonces la torsión de* A *es infinita, pero para cada entero positivo* n *la* n*-torsión de* A *es finita.*

En [Sh2, III.3] se muestra que el numero de soluciones de la ecuación $nx = 0$ en la curva elíptica es exactamente n^2.

Teorema 4.10. *Sea* E *una curva elíptica definida sobre* k.

1. *El kernel del homomorfismo de Manin tiene rango de Morley finito.*
2. *Además existe un subgrupo infinito* ∂*-definible* G *de* E *de rango de Morley finito que es* ∂*-conexo,* ∂*-definible sobre* k *y no contiene subgrupos propios infinitos* ∂*-definibles sobre* k.

Demostración. $\ker(M)$ es un subgrupo ∂-definible sobre k propio de E, luego $MR(\ker(M))$ es finito pues E es ∂-conexo. Claramente $\ker(M)$ contiene la torsión de E, que es infinita. Sea B la intersección de todos los subgrupos ∂-definibles sobre k de E que contienen la torsión de E. B es ∂-definible sobre k, conexo y de rango de Morley finito. B tiene un subgrupo conexo infinito G que es ∂-definible sobre k y que no tiene subrupos infinitos propios ∂-definibles sobre k, pues de lo contrario habría una cadena descendente infinita de subgrupos ∂-definibles. □

4.3 El caso general

El propósito de esta sección es demostrar un análogo del Teorema anterior para variedades abelianas simples. La parte más difícil es encontrar un subgrupo ∂-definible de rango de Morley finito que contenga la torsión de la variedad abeliana. Para esto se encontrará un homomorfismo ∂-definible cuyo kernel será el subgrupo buscado.

Definición 4.11. *Sea G un grupo conexo ∂-definible sobre $k \subset K$. Para $a = (a_1, \cdots, a_n)$ se define $a' = (a_1', \cdots, a_n')$. Para $m \geq 0$ se define $e_m(G)$ como el grupo $\left(\{(a, a', \cdots, a^{(m)}) | a \in G\}, *_{(m)}\right)$ donde*

$$(a, a', \cdots, a^{(m)}) *_{(m)} (b, b', \cdots, b^{(m)}) = (a * b, (a * b)', \cdots, (a * b)^{(m)}).$$

Sea $e_m : G \to e_m(G), a \mapsto (a, a', \cdots, a^{(m)})$.

Claramente cada $e_m(G)$ es ∂-definiblemente isomorfo a G. Lo interesante es ver qué pasa cuando la operación $*$ no sólo es ∂-definible si no definible. Esto no implica que $e_m(G)$ sea definible, pero su operación de grupo si lo es.

Es posible encontrar un grupo definible $G_m \supset e_m(G)$ tal que la operación de grupo de G coincide con $*$ sobre $e_m(G)$. Además existen homomorfismos sobreyectivos $\pi_m : G_m \to G_{m-1}$. La construcción de G_m y la demostración de los dos siguientes Lemas se encuentra en [Pi1].

Lema 4.12.

1. *$RM^-(G_m) = (m+1)RM^-(G)$ para todo m.*
2. *Si X es un subconjunto ∂-definible de G entonces para algún m existe un subconjunto definible Y de G_m tal que $e_m(X) = Y \subseteq e_m(G)$.*
3. *Si H es un subgrupo ∂-definible (conexo) de G, entonces para algún m existe un subgrupo definible (conexo) H_m de G_m tal que $e_m(H) = H_m \cap e_m(G)$.*

Sea $\rho_m = \pi_1 \circ \cdots \circ \pi_m : G_m \to G$.

Lema 4.13. *Sea G un grupo algebráico conmutativo de dimensión n(es decir, $MR^{-}(G) = n$). Entonces* $\ker(\rho_r)$ *es un grupo vectorial de dimensión nr.*

Lema 4.14. *Si G es un grupo algebráico conmutativo y B es un subgrupo algebráico ∂-conexo, ∂-definible y Zariski-denso de G, entonces G/B es ∂-definiblemente isomorfo a un grupo vectorial.*

Demostración. Por el Lema 4.12 existe un entero m y un subgrupo conexo B' de G_m tal que $e_m(B) = B' \cap e_m(G)$. Sea $J_m = \ker(\rho_m)$ que es un grupo vectorial por el Lema 4.13. Como B es Zariski-denso en G, $\rho_m(B') = G$ y $G_m = J_m \cdot B'$. Se puede encontrar un complemento J de $J_m \cap B'$ en J_m. Entonces G_m es el producto directo de J y B'. Sea $\pi : G_m \to J$ la proyección. Sea $\varphi : G \to J$ el homomorfismo definido por $\varphi(a) = \pi(a, a', \cdots, a^{(m)})$. Este homomorfismo tiene como kernel a B. □

Para acotar el rango de Morley de ciertos subgrupos se necesita el siguiente Teorema.

Teorema 4.15 (Teorema de Rosenlicht). *Sean A una variedad abeliana, B un grupo vectorial y G una extensión de A por B; es decir, se tiene la secuencia exacta de grupos*

$$0 \to B \to G \to A \to 0$$

donde A es una variedad abeliana, G es un grupo algebráico y B es un grupo vectorial, hay un subgrupo algebráico conexo G_1 de G tal que G_1 se proyecta sobreyectivamente en A y $MR^{-}(G_1) \leq 2MR^{-}(G)$.

Los siguientes Lemas técnicos se necesitarán para la demostración del teorema principal.

Lema 4.16. *Sean A y B un grupos conmutativos. Sea $\nu : B \to A$ un homomorfismo sobreyectivo y sea C subgrupo de B. Entonces $A/\nu(C) \simeq B/(C + \ker(\nu))$.*

Demostración. Por el primer Teorema del isomorfismo existe una biyección entre los subgrupos de B que contienen a $\ker(\nu)$ y los subgrupos de A. En particular $C + \ker(\nu)$ se corresponde con $\nu(C)$. Entonces $A/\nu(C) \simeq B/(C + \ker(\nu))$. □

Lema 4.17. *Sea A una variedad abeliana y B un grupo algebráico conmutativo. Sea $\nu : B \to A$ un homomorfismo sobreyectivo tal que* $\ker(\nu)$ *es un grupo vectorial. Sea C subgrupo de B. Son equivalentes las siguientes afirmaciones:*

1. *$\nu(C) = A$.*
2. *B/C es isomorfo a un grupo vectorial.*

Demostración. "*1.⇒ 2.*" Si $\nu(C) = A$, por el Lema anterior $B = C + \ker(\nu)$. Luego

$$B/C = (C + \ker(\nu))/C \simeq \ker(\nu)/(\ker(\nu) \cap C)$$

por el segundo Teorema del isomorfismo. Pero $\ker(\nu)/(\ker(\nu) \cap C)$ es isomorfo a un grupo vectorial pues $\ker(\nu)$ lo es.

'*2.⇒ 1.*" Si B/C es isomorfo a un grupo vectorial entonces $B/(C+\ker(\nu))$ también lo es pues por el tercer teorema del isomorfismo $B/(C+\ker(\nu)) \simeq (B/C)/(C+\ker(\nu)/C)$. Por el Lema anterior $A/\nu(C)$ es isomorfo un grupo vectorial K^n. Sea $f : A \to K^n$ definida como la composición de la proyección de A en $A/\nu(C)$ y el isomorfismo entre $A/\nu(C)$ y K^n. f es sobreyectiva pues es composición de funciones sobreyectivas. Pero por el Lema 2.40 y la observación que se encuentra después, f es constante. Luego $n = 0$ y por lo tanto $A = \nu(C)$. □

El siguiente Teorema proporciona el homomorfismo que se necesita.

Teorema 4.18. *Sea A una variedad abeliana. Entonces existe un homomorfismo ∂-definible de A a K^n, para algún n, tal que su kernel es un grupo infinito de rango de Morley finito.*

Demostración. Sean A_m y ρ_m como se definieron anteriormente. Sean B y B' subgrupos definibles de A_m cuya imagen por ρ_m es todo A. Por el Lema 4.17 se concluye que A_m/B y A_m/B' son isomorfos a grupos vectoriales. Pero $A_m/(B \cap B')$ se sumerge en la suma directa de A_m/B y A_m/B', así que también es isomorfo a un grupo vectorial. Utilizando nuevamente el Lema 4.17 se concluye que la imagen de $B \cap B'$ bajo ρ_m es todo A. Se sigue que hay un único subgrupo definible B_m minimal entre aquellos cuya imagen bajo ρ_m es A. Por unicidad $\pi_m(B_m) = B_{m-1}$. Como A_m/B_m se sumerge en un grupo vectorial, B_m contiene los elementos de torsión de A_m, pero A tiene infinitos elementos de torsión, así que B_m debe contener las imágenes bajo e_m de estos elementos. Luego B_m es infinito. Sea

$$B = \bigcap_m \{a \in A | (a, \partial a, \cdots, \partial^m a) \in B_m\}.$$

B es intersección de subgrupos ∂-definibles en A, luego es igual a una subintersección finita. Sea m tal que $B = B_m$. Para m suficientemente grande sea $\varphi : A \to A_m/B_m \subset K^n$. Entonces φ es ∂-definible y su kernel es B.

Sólo falta verificar que B tiene rango de Morley finito. Por el Teorema 4.15 se tiene que $MR^-(B_m) \leq 2MR^-(A)$ para todo m. Sea k un campo pequeño sobre el cual B está definido. Para todo $b \in B$ se tiene que $tr.deg(k(b, b', \cdots, b^{(m)}, \cdots)/k)$ es menor o igual que $2MR^-(A)$. Luego $MR(b/k)$ es finito para todo $b \in B$ y por lo tanto $MR(B)$ es finito. □

Definición 4.19. *Una variedad abeliana es simple si no contiene una subvariedad abeliana no trivial.*

Teorema 4.20. *Si A es una variedad abeliana simple, A contiene un subgrupo H ∂-conexo y ∂-definible que es minimal entre todos los subgrupos infinitos ∂-definibles de A. Además H tiene rango de Morley finito y contiene a los puntos de torsión de A.*

Demostración. Sea B un subgrupo infinito ∂-conexo y ∂-definible de A. La clausura de Zariski $\overline{B}$ de B es una subvariedad de A, luego $\overline{B} = A$. Por el Lema 4.14 B contiene a la torsión de A, pues en caso contrario A/B contendría elementos de torsión. El kernel del homomorfismo del Teorema 4.18 es un subgrupo ∂-definible infinito y de rango de Morley finito. Sea H la intersección de todos los subgrupos infinitos ∂-conexos y ∂-definibles de A. Esta intersección es igual a una subintersección finita y por lo tanto H es ∂-conexo y ∂-definible. Claramente H contiene a la torsión de A y tiene rango de Morley finito. Claramente H es minimal entre todos los subgrupos infinitos ∂-definibles de A. □

Se finaliza este capítulo con una consecuencia importante del Teorema 4.18. Un subgrupo (no necesariamente definible o ∂-definible)Γ de A tiene "rango finito" si contiene un subgrupo finitamente generado Γ_0 tal que para todo $x \in \Gamma$ existe $n \geq 1$ tal que $nx \in \Gamma_0$.

Teorema 4.21. *Sea K diferencialmente cerrado. Sea A una variedad abeliana sobre K y sea Γ un subgrupo de A de "rango finito". Entonces existe un subgrupo ∂-definible H de A tal que $\Gamma \subset H$ y H tiene rango de Morley finito.*

Demostración. Sea φ como en el Teorema 4.18. Sean $a_1, \cdots, a_l$ los generadores de Γ_0. $\varphi(\Gamma)$ es un subconjunto de "rango finito" del un grupo vectorial K^n y está contenido en el $\mathbb{Q}$-espacio vectorial X generado por $\varphi(a_1), \cdots, \varphi(a_l)$. La imagen inversa $H = \varphi^{-1}(X)$ es un subgrupo de A que contiene a Γ. Además es ∂-definible de rango de Morley finito. □

Este Teorema es fundamental para la demostración de la conjetrua de Mordell-Lang, que se presenta en forma reducida en el apéndice.

A Apéndice: La conjetura de Mordell-Lang

En este apéndice se presenta esquematicamente la demostración de Hrushovski de la conjetura de Mordell-Lang para campos de funciones, en la cual se utiliza el kernel de Manin. Más precisamente el Teorema 4.21. En la demostración de Hrushovski se utilizan herramientas complejas de teoría de modelos, las cuales se presentarán parcialmente en la sección A.1. En algunos casos simplemente se hará referencia a [Bo]. Este es el texto que se usará como guía para esta presentación. El kernel de Manin juega un papel importante en la primera demostración de la conjetura de Mordell-Lang, dada por Manin en 1966 en [Man], y en demostraciones posteriores, como por ejemplo las que se encuentran en [Bu] y [Hr].

Definición A.1. *Sean $k_0 \subset K$ campos de característica cero y sea $V \subset K^n$ una variedad definida sobre k_0. Se define $V(k_0) = V \cap k_0^n$, el conjunto de los puntos racionales de V sobre k_0.*

Teorema A.2 (Conjetura de Mordell-Lang para campos de funciones). *Sean $k_0 \subseteq K$ campos algebraicamente cerrados y distintos. Sea A una variedad abeliana definida sobre K y sea X una subvariedad de A definida sobre K. Sea Γ un subrupo de "rango finito" de $A(K)$. Si $X \cap \Gamma$ es Zariski-denso en X y el estabilizador de X en A es finito, entonces hay una subvariedad abeliana B de A, una variedad abeliana S definida sobre k_0, una subvariedad X_0 de S definida sobre k_0 y un morfismo biyectivo $h : B \to S$ tal que $X = a_0 + h^{-1}(X_0)$ para algún $a_0 \in A$.*

El estabilizador de X en A es el subgrupo algebráico $\{a \in A | a + X \subset X\}$.

A.1 Preliminares

Definición A.3. *Una clase es fuertemente minimal si es infinita y todos sus subconjuntos definibles son finitos o cofinitos. Equivalentemente una clase es fuertemente minimal si su rango y su grado de Morley son iguales a 1. Una clase es casi fuertemente minimal si está contenida en la clausura algebraica de una clase fuertemente minimal.*

Lema A.4. *Sean $k_0 \subset K$ campos algebraicamente cerrados de característica cero. Sea $A \subset k_0^n$. Entonces la clausura de Zariski de A es k_0-definible.*

Se necesitan algunas propiedades de las variadades abelianas, como las siguientes. Las demostraciones de esto se encuentran en [Hi].

Teorema A.5. *Si una variedad abeliana A está definida sobre $k \subset K$ y G es un subgrupo cerrado de A, entonces G está definido sobre la clausura algebraica de k.*

Teorema A.6 (Teorema de Chevalley). *Sea G un grupo algebráico definido sobre K. Entonces existe un subgrupo cerrado minimal M de G definido sobre K tal que G/M es una variedad abeliana.*

Definición A.7. *Una teoría ω-estable T es uno-basada si para todo $n \in \omega$, todo modelo M de T, todo tipo completo $p \in S_n(M)$ y toda realización $\bar{a}$ de p, la base canónica de p es algebráica sobre $\bar{a}$.*

En este trabajo no se entrará en detalles sobre las teorías o los grupos uno-basados. Sólo se necesitan los siguientes Teoremas:

Teorema A.8. *Sea $\mathcal{C}$ fuertmente minimal. Entonces $\mathcal{C}$ es localmente modular si y sólo si es uno-basado.*

Teorema A.9. *Sea G un grupo uno-basado. Entonces cualquier subconjunto definible de G^n es combinación booleana de clases laterales de subgrupos definibles de G.*

Las demostración están en [Z] y [Las], respectivamente.

Definición A.10. *Dos clases definibles D y E son ortogonales si para cualesquiera $d \in D$ y $e \in E$ se tiene que d y e son independientes sobre cualquier conjunto de parámetros sobre el cual D y E pueden ser definidos.*

Teorema A.11. *Asumiendo eliminación de imaginarios, un grupo casi fuertemente minimal G es no ortogonal a la clase E si y solo si existe un grupo definible H contenido en la clausura definible de E y un homomorfismo definible sobreyectivo $h : G \to H$ con kernel finito.*

La demostración se encuentra en [Z].

A.1.1 Indecomponibilidad

Sea G un grupo ω-estable.

Definición A.12. *Sea X un subconjunto definible de G. X es indecomponible si para todo subgrupo definible H de G, el conjunto $X/H = \{xH | x \in X\}$ es infinito o de cardinalidad 1.*

Lema A.13. *Sea X fuertemente minimal. Entonces existe un conjunto indecomponible $X_0 \subset X$ tal que $X \setminus X_0$ es finito.*

Demostración. Se considera la familia
$\mathcal{K} = \{H | H$ es subgrupo definible de G y X/H es finito$\}$.

Sea

$$H_0 = \bigcap_{H \in \mathcal{K}} H.$$

H_0 es igual a una subintersección finita y por lo tanto X/H_0 es finito. Como X es fuertemente minimal, uno y solo uno de los conjuntos $xH_0 \cap X$, para $x \in X$, es infinito, y su complemento en X es finito. Sea X_0 este conjunto infinito. Se mostrará que X_0 es indecomponible. Sea H un subgrupo definible de G. Si X/H es infinito, X_0/H también lo es pues $X \setminus X_0$ es finito. Si X/H es finito, $H_0 \subset H$ y X_0/H tiene sólo un elemento pues X_0/H_0 tiene sólo un elemento. $\square$

Teorema A.14 (Teorema de indecomponibilidad de Zilber). *Sea $(X_i|i \in I)$ un conjunto de subconjuntos indecomponibles del grupo de rango de Morley finito G, tal que cada uno de ellos contiene a la identidad de G. Entonces el grupo H generado por $\bigcup_{i \in I} X_i$ es definible y conexo.*

La demostración se encuentra en [Las].

A.1.2 Campos diferencialmente cerrados

Definición A.15. *Dado un anillo diferencial R, su anillo de polinomios diferenciales es $R\{y\} = R[y, \delta y, \delta^2 y, \cdots]$. Este es un anillo diferencial extendiendo δ de la manera natural. Para $f \in R\{y\}$ no nulo se define $ord(f)$ como el máximo n tal que $\delta^n y$ aparece en f con coeficiente no nulo. Para $a \in R$ se define $ord(a) = -1$.*

Definición A.16. *Un campo diferencial K es diferencialmete cerrado si para cualesquiera $f, g \in K\{y\}$ con $ord(f) > ord(g)$ existe $a \in K$ tal que $f(a) = 0$ y $g(a) \neq 0$.*

Es claro que todo campo diferencialmente cerrado es algebraicamente cerrado. La demostración de los siguientes teoremas se encuentra en [Wo].

Teorema A.17. *Todo campo diferencial K tiene clausura diferencial L, que es única módulo isomorfismo, y el campo de constantes de L es algebráico sobre el campo de constantes de K.*

Teorema A.18. *La teoría de campos diferencialmente cerrados admite eliminación de cuantificadores, eliminación de imaginarios, es completa y ω-estable.*

Lema A.19. *El campo de constantes k_0 de un campo diferencialmente cerrado K no tiene estructura adicional a la de un campo algebraicamente cerrado; es decir, para subconjuntos de k_0^n las nociones de ∂-definible sobre K y definible sobre k_0 coinciden.*

Lema A.20. *Sea k_0 el campo de constantes del campo diferencialmente cerrado K. Sea H un grupo ∂-definible sobre K, $H \subset k_0^n$ y sea $g : H \to K^m$ una función ∂-definible.*

1. *Hay un grupo algebráico G definido sobre k_0 tal que $H = G(k_0)$.*

2. *Sea D un subconjunto finito de K tal que g está definido sobre D. Entonces H se puede particionar de la forma $E_1 \cup \cdots \cup E_r$ donde cada E_i es es un subconjunto de k_0^n definible sobre k_0 y para cada i $g \restriction_{E_i}$ es una función racional definida sobre cierto $D' \supset D$.*

Teorema A.21 (Teorema de Cassidy-Sokolovic). *Un campo infinito de rango de Morley finito que es ∂-definible en un campo diferencialmente cerrado K es ∂-definiblemente isomorfo al campo de constantes de K.*

A.2 La versión reducida

Nótese que en el enunciado del Teorema A.2 Γ no es definible. A continuación se harán algunas reducciones para cambiar a Γ por un subgrupo H "pequeño". Para esto se enriquecerá la estructura de K con una derivación.

Sea ∂ una derivación de K tal que k_0 es su campo de constantes y sea L la clausura diferencial de K. Por ser algebraicamente cerrado k_0 es el campo de constantes de L y por lo tanto es definible. Claremente se puede reemplazar a K por L en el enunciado del Teorema, así que se puede suponer que K es diferencialmente cerrado. Además se puede suponer que K es ω-saturado: Sea L' una extensión ω-saturada de K y sea k_0' el campo de constantes de L'. Claramente $k_0 \subset k_0'$. Supóngase que el resultado se tiene para L' y k_0'. Entonces existe una subvariedad abeliana B de A, una variedad abeliana S' definida sobre k_0', una subvariedad X_0' de S' definida sobre k_0' y un morfismo biyectivo $h' : B \to S'$ tal que $X = a_0' + {h'}^{-1}(X_0')$.

Por el Teorema A.5, B está definido sobre K. Nótese que la afirmación

"$h' : B \to S'$ es un morfismo biyectivo definido sobre K, X_0' es subvariedad de S', siendo ambos definibles sobre k_0' y $X = a_0' + {h'}^{-1}(X_0')$"

se puede expresar en primer orden. Para esto se utilizan explicitamente las fórmulas que definen a B y a h'; también se utilizan las fórmulas que definen a S y a X y se indica que los parámetros que aparecen están en k_0' que es definible sobre L'. Como $K \preccurlyeq L'$, existe una variedad abeliana S definido sobre k_0, una subvariedad X_0 de S definida sobre k_0 y un morfismo biyectivo h tal que $X = a_0 + h^{-1}(X_0)$ para algún $a_0 \in A(L)$.

Entonces de ahora en adelante se asumirá que K es diferencialmente cerrado y que k_0 es su campo de constantes. Además se usará el Teorema 4.21 con el fin de reemplazar el subgrupo Γ del enunciado del Teorema A.2 por un subgrupo H de A que es ∂-definible, de rango de Morley finito y que contiene a Γ.

La parte más difícil de la demostración del Teorema A.2, la cual no se hará en este trabajo, es mostrar que se puede reducir al caso en que H es un subgrupo conexo ∂-definible casi fuertemente minimal y no uno-basado de A. El propósito de esta reducción es utilizar el hecho de que en la teoría de campos diferencialmente cerrados, los subconjntos fuertemente minimales inducen geometrías de Zariski y por esto se pueden aplicar los resultados de Hrushovski y Zilber que se citan sin demostración en los preliminares. Módulo la reducción mencionada para H, se concluye la demostración del Teorema A.2 demostrando el siguiente Teorema.

Teorema A.22. *Sean K un campo algebraicamente cerrado ω-saturado y $k_0 < K$ el campo de constantes de K. Sea A una variedad abeliana definida sobre K y sea H un subgrupo conexo ∂-definible casi-fuertemente minimal y no uno-basado de A.*

1. *Existe una variedad abeliana S definida sobre k y un morfismo biyectivo $f : \overline{H} \to S$ tal que $f(H) = S(k_0)$. (Acá $\overline{H}$ denota la clausura de Zariski de H).*

2. *Sea X una subvariedad abeliana de A definida sobre K tal que $X \cap H$ es Zariski-denso en H. Entonces existe una subvariedad X_0 de S, definida sobre k_0, tal que $X = f^{-1}(X_0)$*

Demostración. Sea B un conjunto ∂-definible fuertemente minimal tal que $H \subset acl(B)$. B no es uno-basado y por el Teorema A.8 no es localmente modular.

En [Mar3] se muestra que B, quitando posiblemente un número finito de puntos, es una geometría de Zariski. Del Teorema de dicotomía para geometrías de Zariski y del hecho que B no es localmente modular se tiene que B interpreta un campo algebraicamente cerrado L. Este campo algebraicamente cerrado tiene rango de Morley finito puesto que es interpretable en una clase de rnago de Morley uno. Luego por el Teorema A.21 se tiene que L es ∂-definiblemente isomorfo al campo de constantes k_0. Por esto B y k_0, y por lo tanto H y k_0 no son ortogonales. Del Teorema A.11 y del hecho de que la teoría de campos diferencialmente cerrados posee eliminación de imagimarios se sigue que existe un grupo $G \subset k_0^m$ ∂-definible sobre k_0 y un homomorfismo sobreyectivo ∂-definible $h : H \to G$ con kernel finito.

A continuación se definirá un homomorfismo $g_0 : G \to H$. Sea $n = |\ker(h)|$. Para $y \in G$, con $y = h(x)$, se define $g_0(y) = nx$. g_0 está bien definido pues si $h(x) = h(x')$ entonces $x - x' \in \ker(h)$ y $nx = nx$. Claramente g_0 es un homomorfismo. El kernel de g_0 está contenido en la n-torsión de H que es finita por el Lema 4.9 y el hecho de que H es subgrupo de una variedad abeliana. Se mostrará que g_0 es sobreyectivo. Por la finitud de la n-torsión, nH y H tienen el mismo rango de Morley y por el Lema 4.2 nH tiene índice finito en H. Pero H es conexo, luego $nH = H$.

Sea $G_1 = G/\ker(g_0)$. Como $G \subset k_0^m$ es ∂-definible con parámetros en k_0 y $\ker(g_0)$ es finito, entonces G_1 también es ∂-definible con parámetros en k_0(por eliminación de imaginarios en campos diferencialmente cerrados) y $G_1 \subset k_0^k$ para algún k. Se considerará el isomorfismo ∂-definible $g : G_1 \to H$ inducido por g_0.

Por el Teorema A.19 k_0 es un campo que no tiene estructura adicional. Así que exisre un grupo algebráico conexo G_2, definido sobre k_0, tal que $G_2(k_0) = G_1$ y $g \restriction_{G_2(k_0)}$ es racional sobre ciertos parámetros de L.

El homomorfismo racional sobreyectivo g se extiende de manera natural a la clausura de Zariski, $\overline{g} : \overline{G_2(k_0)} = G_2(L) \to \overline{H}$. $\overline{g}$ es un morfismo sobreyectivo. $\overline{H}$ es un subgrupo cerrado conexo de A, luego es una variedad abeliana.

Se mostrará que $\ker \bar{g}$ es trivial. Sea N el subgrupo de G_2 definido sobre k_0 minimal tal que G_2/N es una variedad abeliana, por el Teorema A.6. Como $G_2/\ker \bar{g}$ es isomorfo a $\overline{H}$ que es una variedad abeliana, $N \subset \ker \bar{g}$. Luego $M(k_0) \subseteq (\ker \bar{g})(k_0) = \{0\}$ pues $\ker \bar{g} \restriction_{k_0}$ es inyectivo. Como M está definido sobre k_0, M es trivial y por lo tanto G_2 es una variedad abeliana. Pero por el Teorema A.5, $\ker \bar{g}$ que es un subgrupo cerrado de G_2, también está definido sobre k_0 y por lo tanto es trivial.

Sea $f : \overline{H} \to S = G_2$ la inversa de $\bar{g}$. f es un morfismo biyectivo y $f(H) = g_2(k_0)$. Con esto queda demostrado *1.*

Sea $X_0 = f(X)$. Como X es cerrado, irreducible y $\overline{X \cap H} = X$, entonces $f(X)$ es cerrado, irreducible y $\overline{f(X \cap H)} = f(X)$. $f(X \cap H) \subset f(H)$ que está contenido en k_0. Su clausura de Zariski está por lo tanto contenida en k_0 por el Lema A.4 Luego $X_0 = f(X) = \overline{f(X \cap H)}$ está definido sobre k_0. Esto concluye la demostración. □

A.3 Un caso sencillo

A continuacion se mostrará como se utiliza el kernel de Manin para un caso particular de la conjetura de Mordell-Lang. Las hipótesis adicionales permiten reducir fácilmente la situación a la del Teorema A.22.

Teorema A.23. *Sean $k_0 \subset K$ campos algebraicamente cerrados de característica cero. Sea A una variedad abeliana simple definida sobre K y sea $X \subseteq A$ una curva definida sobre K. Sea T la torsión de A. Entonces pasa alguno de los siguientes casos:*

1. *X=A.*
2. *$X \cap T$ es finito.*
3. *Hay un isomorfismo $f : A \to S$, donde S es una variedad abeliana definida sobre k_0, y una curva X_0 en S definida sobre k_0, tal que $X = f^{-1}(X_0)$.*

Demostración. Se puede suponer que K es un diferencialmente cerrado y ω-saturado al igual que se hizo anteriormente. Como A es simple debe tenerse que $\overline{H} = A$. De aquí se deduce que $X \cap H$ es Zariski-denso en X. Además por el Teorema 4.20 existe un subgrupo H ∂-definible que contiene a T, minimal entre lo subgrupos infinitos ∂-definibles de A y tal que $MR(H)$ es finito.

A continuación se considerarán dos casos:

• H es uno-basado. Entonces todos los subconjuntos ∂-definibles de H son combinaciones booleanas de clases laterales de de subgrupos ∂-definibles de H, pero por la minimalidad de H estos subgrupos deben ser finitos. Así que todos los subconjntos definibles de H son finitos o cofinitos. En particular $X \cap H$ es finito o cofinito en H. Si es finito entonces $T \cap X \subseteq X \cap H$ es finito. Si $X \cap H = H \setminus E$ con E finito, entonces $A = \overline{H} = \overline{(H \setminus E) \cup E} = \overline{(H \setminus E)} \cup E$. Pero A es irreducible. Se sigue que $A = \overline{(H \setminus E)} = X$.

• H no es uno-basado. Sea $B' \subset H$ de rango y grado de Morley uno. Este B existe pues H tiene rango de Morley finito. B' es fuertemente minimal. Por el Lema A.13 existe $B \subset B'$ ∂-definible, indecomponible y tal que $B' \setminus B$ finito. Por el Teorema de indecomponibilidad de Zilber, para todo $b_0 \in B$ el grupo C generado por $B - b_0 = \{b - b_0 | b \in B\}$ es ∂-definible. Por la minimalidad de H se tiene que $C = H$. Pero claramente $C \subseteq acl(B)$. Así que H es casi fuertemente minimal.

Aplicando directamente el Teorema A.22 se obtiene el resultado.

$\square$

Bibliografía

[Bo] Bouscaren, Elisabeth. *Model theory and algebraic geometry, an introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture.* LNM 1996, Springer-Verlag 1998.

[Bu] Buiunm, A. *Effective boundes for geometric Lang conjeture.* Duke j. Math 71(1993), 475-499.

[F] Fulton, William. *Curvas Algebráicas.* Reverte, 1971.

[Hi] Hindry, Marc. *Introduction to abelian varieties and the Mordell-Lang conjeture.*

[Hr] Hrushovski, E. *The Mordell-Lang conjeture for functions fields.* Journal AMS 9(1996), 667-690.

[Hu] Humphreys, James E. *Linear algebraic groups.* Springer-Verlag, 1975.

[K] Kunz, Ernest. *Introduction to conmutative algebra and algebraic geometry.* Birkhäuser, 1985.

[Lan] Lang, Serge. *Introduction to algebraic geometry.* Interscience publishers 1958.

[Las] Lascar, Daniel. *Omega-stable groups* en *Model theory and algebraic geometry.* LNM 1996, Springer-Verlag 1998.

[Man] Manin, Yuri. *Rational Points of algebraic curves over functions fields.* Isvetzia 27(1963), 1395-1440 (AMS Transl. Ser II 50 (1966), 189-234).

[Mar1] Marker, David. *Manin Kernels* en *Connections betwen Model theory and analytic geometry*, editado por A. Macintyre, Quaderni di matematica, vol 6, U de Nápoles, 2000.

[Mar2] Marker, David. *Model theory of diferential fields* en *Model theory of fields, Lecture notes in logic 5.* Springer-Verlag, 1996.

[Mar3] Marker, David. *Zariski geometries* en *Model theory and algebraic geometry.* LNM 1996, Springer-Verlag 1998.

[Pi1] Pillay, Annad. *Differential algebraic groups and the number of countable differentially closed fields* en *Model Theory of fields, Lecture notes in Logic 5.* Springer-Verlag.

[Pi2] Pillay, Anand. *Model theory of algebraic closed fields* en *Model theory and algebraic geometry.* LNM 1996, Springer-Verlag 1998.

[Po] Pong, Wai Yan. *Ordinal dimension and differential completeness.* Ph. D. Thesis, University of Illinois at Chicago, 1999.

[Sh1] Shafarevich, Igor. *Basic algebraic geometry.* Springer-Verlag, 1974.

[Sh2] Shafarevich, Igor. *Basic algebraic geometry.* Dos volúmenes. Springer-Verlag, 1994.

[Sp] Springer, T.A. *Jordan algebras and algebraic curves.* Springer-Verlag, 1973.

[Wa] Warner, Frank. *Foundations of differenciable Manifold and Lie groups.* Glenview 1971.

[Wo] Wood, Carol. *Differentialy closed fields* en *Model theory and algebraic geometry.* LNM 1996, Springer-Verlag 1998.

[Z] Ziegler, Martin. *Introduction to stability theory and Morley rank* en *Model theory and algebraic geometry.* LNM 1996, Springer-Verlag 1998.