

ESTUDIO DE CONJUNTOS DIOFANTINOS Y
NO DIOFANTINOS SOBRE $\mathbb{C}(z)$, CON LOS
GRADOS DE SUS ELEMENTOS
CUMPLIENDO RELACIONES POLINOMIALES
EN DOS VARIABLES

por

Cristóbal Villalobos Acuña



Tesis presentada en cumplimiento parcial
del Requisitos para la Maestría en Matemáticas
en la Facultad de Matemáticas de la
Pontificia Universidad Católica de Chile.

Supervisor : Natalia García-Fritz (Pontificia Universidad Católica de Chile)
Comité : Ricardo Menares (Pontificia Universidad Católica de Chile)
Xavier Vidaux (Universidad de Concepción)

Abril, 2024
Santiago, Chile

Agradecimientos

En primer lugar, agradezco a Dios por los talentos y oportunidades que me ha dado y gracias a Su ayuda pude concretar esta tesis.

Agradezco también a la Profesora Natalia García-Fritz por acompañarme durante este proceso, por responder mis preguntas, por su paciencia para conmigo y por todo el tiempo que le dedicó para que este trabajo pudiera concluirse de buena manera. Aprendí mucho de Matemáticas y de la vida en general.

Destaco la contribución de los profesores Ricardo Menares y Xavier Vidaux por la revisión de la tesis y los comentarios realizados. Ayudaron a que este trabajo sea mejor, estoy muy agradecido por el tiempo que le dedicaron.

Agradezco a mi familia, que me apoyaron en todo momento y me permitieron dedicarme a completar esta tesis.

Agradezco a la Facultad y a la Universidad debido al apoyo brindado durante el Pregrado de Licenciatura en Matemáticas y durante el estudio del Magíster en Matemáticas. Por la infraestructura que pusieron a mi disposición, por las personas que se preocuparon de mi bienestar y por las becas que me posibilitaron investigar en Matemáticas.

Reconozco el aporte del Profesor Renato Lewin, por abrirme las puertas a este mundo y por su preocupación cuando fui su estudiante, su ayudante y también cuando dejé de serlo.

Expreso mi gratitud, finalmente, a todas las personas que estuvieron apoyándome durante este proceso, especialmente a mis amistades, que hicieron más sencillo el esfuerzo de escribir esta tesis.

Esta tesis fue parcialmente financiada por el proyecto Fondecyt regular N°1211004.

Índice general

Introducción	3
1. Preliminares	8
1.1. Conjuntos diofantinos	8
1.2. Resultantes	10
1.3. Curva elíptica de Denef	13
1.4. Alturas	14
1.4.1. Grado de funciones racionales	14
1.4.2. Altura canónica	14
1.4.3. Altura en $\mathbb{C}(z)$	15
1.5. Dimensión Diofantina	16
1.6. Un conjunto no diofantino sobre $\mathbb{C}(z)$	17
2. Lemas previos y notaciones	19
2.1. ¿Por qué $\mathbb{Q}[x, y]$ y no $\mathbb{C}[x, y]$?	19
2.2. Conjuntos diofantinos con condiciones de congruencia para el grado	22
3. Grado 1	25
4. Grado 2	29
5. Comentarios finales	34
5.1. Parábola	34
5.2. Hipérbola	38
5.3. Conjetura	39
Bibliografía	41

Introducción

Este trabajo se enmarca en los desarrollos inspirados por el décimo problema de Hilbert planteado en el 1900, ver en [6], que buscaba lo siguiente

Décimo problema: Dada una ecuación diofantina con cualquier número de incógnitas y coeficientes enteros, encontrar un algoritmo que determine en finitos pasos si la ecuación tiene solución en los números enteros.

Una *ecuación diofantina* con n variables es una ecuación de la forma $P(x_1, \dots, x_n) = 0$ con P un polinomio de coeficientes enteros. Gracias a los trabajos de Robinson, Davis, Putnam y Matiyasevich, desde 1970 sabemos que no existe tal algoritmo que determine si tiene o no solución una ecuación diofantina dada (se puede ver [2]).

A partir de las ecuaciones diofantinas se introduce el concepto de conjunto diofantino, que son aquellos definidos por una ecuación diofantina aceptando cuantificar de forma existencial.

Una vez respondida (de forma negativa) la cuestión de un algoritmo en el caso de ecuaciones con coeficientes enteros, se generaliza la pregunta a otros anillos y el concepto de conjunto diofantino se vuelve más general. Así, en esta tesis consideramos que un *conjunto diofantino*, dado un anillo R y k entero positivo, es $S \subset R^k$, para el cual existe n número entero positivo, con $k < n$, y $P(x_1, \dots, x_k, x_{k+1}, \dots, x_n)$ polinomio con coeficientes en R tales que

$$S = \{(a_1, \dots, a_k) \in R^k : P(a_1, \dots, a_k, x_{k+1}, \dots, x_n) = 0 \text{ tiene solución en } R\},$$

lo cual también podemos escribir con existenciales de la siguiente forma

$$S = \{(a_1, \dots, a_k) \in R^k : \exists x_{k+1}, \dots, x_n (P(a_1, \dots, a_k, x_{k+1}, \dots, x_n) = 0)\}.$$

A lo largo de los años muchas personas han trabajado con este tipo de conjuntos y avanzado en esta área. La siguiente es una pequeña lista de algunos ejemplos que podemos encontrar en [5], con conjuntos diofantinos en anillos de polinomios y en cuerpos de funciones racionales, que nos sirven para conocer el estado actual del conocimiento en conjuntos diofantinos.

- Sea L un cuerpo grande (*large*). Entonces, L es diofantino en $L(z)$. (Koenigsmann, 2002, [8])
- Sea K cuerpo de característica 0. Entonces, \mathbb{Z} y \mathbb{Q} son diofantinos sobre $K[z]$. (Denef, 1978, [4])

- El anillo de valuación $\mathcal{O}_\infty(\mathbb{R}) = \{f \in \mathbb{R}(z) : v_\infty(f) \geq 0\} \subseteq \mathbb{R}(z)$ es diofantino sobre $\mathbb{R}(z)$. (pequeña modificación del Lema 3.5 en [4], Denef, 1978)
- El conjunto $\{(f, g) \in \mathbb{R}(z)^2 : v_\infty(f) = v_\infty(g)\}$ es diofantino sobre $\mathbb{R}(z)$. (corolario del anillo de valuación)
- El conjunto $\{(f, g) \in \mathbb{R}[z]^2 : \deg f = \deg g\}$ es diofantino sobre $\mathbb{R}[z]$. (corolario del anillo de valuación)
- El anillo $\mathbb{Q}[z]$ es diofantino sobre $\mathbb{R}[z]$. (los dos ejemplos anteriores además de resultados de [3], Demeyer, 2010)

El penúltimo ejemplo es interesante, pues en [5] se prueba que el conjunto $\{(f, g) \in L(z)^2 : \deg f = \deg g\}$ es diofantino sobre $L(z)$, para L cuerpo grande no numerable de característica 0. Así, tenemos un resultado similar en polinomios y funciones racionales.

Este resultado será generalizado en esta tesis para el caso de $\mathbb{C}(z)$, el cuerpo de funciones racionales de \mathbb{C} .

Vamos a considerar para un polinomio $G \in \mathbb{C}[x, y]$ el conjunto

$$A_G = \{(f, g) \in \mathbb{C}(z)^2 : G(\deg f, \deg g) = 0\}$$

y vamos a decir que una solución para $G(x, y) = 0$ es una *solución natural* cuando ambas coordenadas son números naturales (esto pues los grados son naturales). De cierta manera, las soluciones naturales nos dan las posibilidades para los grados de f y g .

Los dos resultados principales de esta tesis nos permiten entender en qué situaciones los conjuntos A_G son diofantinos o no diofantinos.

En el caso del grado de G igual a 1, los conjuntos diofantinos son los que tienen a lo más finitas soluciones naturales o que son rectas horizontales o verticales. Mientras que los conjuntos no diofantinos son los que tienen infinitas soluciones naturales. El resultado es el teorema 3.0.1:

Teorema: Sea $G \in \mathbb{Q}[x, y]$ de grado 1.

Escribimos $G(x, y) = ax + by + c$; con $a, b, c \in \mathbb{Q}$ tales que $a \neq 0$ ó $b \neq 0$. Así,

1. *Si $b = 0$ ó $a = 0$ entonces A_G es diofantino.*

Consideremos ahora $a \neq 0$ y $b \neq 0$.

2. *Sea $c = 0$.*

a) *Si $-\frac{b}{a} < 0$ entonces A_G es diofantino.*

b) *Si $-\frac{b}{a} > 0$ entonces A_G es no diofantino.*

3. *Sea $c \neq 0$.*

a) *Si $-\frac{a}{b} < 0$ entonces A_G es diofantino.*

b) *Si $-\frac{a}{b} > 0$, se tiene que A_G es no diofantino si y solo si $bk + c \equiv 0 \pmod{a}$ tiene solución $k \in \{0, \dots, a - 1\}$.*

En el caso del grado de G igual a 2 los conjuntos diofantinos son los que tienen a lo más finitas soluciones naturales y los no diofantinos son los que tienen infinitas soluciones naturales. En efecto, obtenemos el Teorema 4.0.1:

Teorema: Sea $G(x, y) \in \mathbb{Q}[x, y]$ de grado 2.

Escribimos $G(x, y) = a_5x^2 + a_4xy + a_3y^2 + a_2x + a_1y + a_0$ con $a_i \in \mathbb{Q}$ y a_5, a_4, a_3 no todos cero. Tenemos que

1. *Si $G(x, y) = 0$ tiene a lo más finitas soluciones naturales o si las infinitas soluciones están dadas por una coordenada fija y la otra libre, entonces A_G es diofantino.*

2. *Si $G(x, y) = 0$ tiene infinitas soluciones naturales entonces A_G es no diofantino.*

Para las demostraciones de estos teoremas se separarán casos de forma geométrica según pendiente para el grado de G igual a 1, o según la clasificación de las cónicas para el grado de G igual a 2. En cada caso se buscará separar las ecuaciones $G(x, y) = 0$ con a lo más finitas soluciones de las que tienen infinitas soluciones, utilizando propiedades geométricas y divisibilidad. Para concluir que a lo más finitas soluciones es un conjunto diofantino, usaremos el lema [2.1.3](#). Para concluir en el caso de infinitas soluciones utilizaremos una contradicción con la dimensión diofantina de un conjunto definido a partir de suponer que A_G es diofantino.

En el capítulo 1 de esta tesis se comentan definiciones y resultados presentes en la literatura que son utilizados en el resto de la tesis. En el capítulo 2 definimos la notación utilizada en el resto de este trabajo, además de demostrar dos lemas fundamentales para verificar si ciertos conjuntos A_G son diofantinos o no diofantinos. En el capítulo 3 se demuestra el Teorema 3.0.1. En el capítulo 4 se demuestra el Teorema 4.0.1. En el capítulo 5 se muestran ejemplos concretos donde G representa parábolas o hipérbolas, además de justificar en detalle algunas afirmaciones realizadas en el capítulo 4.

Capítulo 1

Preliminares

Para esta tesis el lenguaje \mathcal{L} utilizado es el lenguaje de anillos con z una variable independiente trascendente sobre el anillo correspondiente, es decir, $\mathcal{L} = \{=, +, \cdot, 0, 1, z\}$. En esta sección veremos; en primer lugar; lo básico de conjuntos diofantinos; luego; algunos conceptos utilizados en esta tesis y; finalmente; el resultado que inspira este trabajo.

1.1. Conjuntos diofantinos

Definición 1.1.1. Sea R anillo (de aquí en adelante, conmutativo y con unidad) y k entero positivo. Decimos que $S \subset R^k$ es *diofantino sobre R* si y sólo si existen n, k números enteros positivos, con $k < n$, y $P(x_1, \dots, x_k, x_{k+1}, \dots, x_n)$ polinomio con coeficientes en R tales que

$$S = \{(a_1, \dots, a_k) \in R^k : P(a_1, \dots, a_k, x_{k+1}, \dots, x_n) = 0 \text{ tiene solución en } R\}.$$

Escribiremos también $S = \{(a_1, \dots, a_k) \in R^k : \exists x_{k+1}, \dots, x_n (P(a_1, \dots, a_k, x_{k+1}, \dots, x_n) = 0)\}$. En este caso diremos que S está definido por la ecuación $P = 0$.

Para el caso de \mathbb{Z} tenemos el siguiente ejemplo:

Ejemplo: Por el teorema de los cuatro cuadrados, \mathbb{N} es diofantino sobre \mathbb{Z} pues

$$x \in \mathbb{N} \Leftrightarrow \exists x_1, \dots, x_4 \text{ tal que } x_1^2 + x_2^2 + x_3^2 + x_4^2 - x = 0.$$

Luego, $\mathbb{N} = \{x \in \mathbb{Z} : \exists x_1, \dots, x_4 (P(x, x_1, x_2, x_3, x_4) = 0)\}$, con $P(x, x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2 - x$, que es un polinomio con coeficientes en \mathbb{Z} .

Definición 1.1.2. Una función $f : R^k \rightarrow R^n$ es *diofantina sobre R* si y sólo si el conjunto $\{(X, f(X)) \in R^{k+n} : X \in R^k\}$ es diofantino sobre R . Similar es la definición para las relaciones.

Ejemplo: El máximo común divisor en \mathbb{Z} , que denotamos (\cdot, \cdot) , es una relación ternaria diofantina. Esto pues $(a, b) = c \Leftrightarrow ((\exists x : cx = a) \wedge (\exists y : cy = b) \wedge (\exists w, z : aw + bz = c))$.

Veamos más ejemplos de conjuntos diofantinos que también serán útiles más adelante.

Lema 1.1.3. *El conjunto vacío es diofantino sobre R anillo no trivial.*

Demostración. Lo siguiente define al vacío

$$\emptyset = \{a \in R : \exists y((a = y + 1) \wedge (a = y))\}$$

y por ende, el conjunto vacío es diofantino. \square

Lema 1.1.4. *Sea R un dominio entero. Luego, la unión de dos conjuntos diofantinos $S_1, S_2 \subseteq R^k$ es un conjunto diofantino.*

Demostración. Si $S_1 \subseteq R^k$ está definido por $P_1(a_1, \dots, a_k, x_1, \dots, x_n)$ y $S_2 \subseteq R^k$ está definido por $P_2(a_1, \dots, a_k, y_1, \dots, y_m)$ entonces

$$(a_1, \dots, a_k) \in S_1 \cup S_2 \Leftrightarrow \exists x_1, \dots, x_n \exists y_1, \dots, y_m \\ P_1(a_1, \dots, a_k, x_1, \dots, x_n)P_2(a_1, \dots, a_k, y_1, \dots, y_m) = 0$$

Es decir, la unión es definida por el producto de los polinomios que definen a cada elemento. \square

Corolario 1.1.5. *Para R como en el lema 1.1.4, la unión finita de conjuntos diofantinos es diofantino.*

Lema 1.1.6. *Sea R un dominio entero tal que su cuerpo de fracciones no es algebraicamente cerrado. Luego, la intersección de dos conjuntos diofantinos $S_1, S_2 \subseteq R^k$ es un conjunto diofantino.*

Demostración. Sea $h(x) = \sum_{i=0}^d c_i x^i \in R[x]$ de grado $d > 0$ sin raíces en el cuerpo de fracciones de R (no es algebraicamente cerrado, así que existe este h). Luego, probaremos que si $S_1 \subseteq R^k$ está definido por $P_1(a_1, \dots, a_k, x_1, \dots, x_n)$ y $S_2 \subseteq R^k$ está definido por $P_2(a_1, \dots, a_k, y_1, \dots, y_m)$ entonces

$$(a_1, \dots, a_k) \in S_1 \cap S_2 \Leftrightarrow \exists x_1, \dots, x_n \exists y_1, \dots, y_m \\ \sum_{i=0}^d c_i P_1(a_1, \dots, a_k, x_1, \dots, x_n)^{d-i} P_2(a_1, \dots, a_k, y_1, \dots, y_m)^i = 0$$

Es claro que si $P_1(a_1, \dots, a_k, x_1, \dots, x_n) = 0$ y $P_2(a_1, \dots, a_k, y_1, \dots, y_m) = 0$ (es decir, si $(a_1, \dots, a_k) \in S_1 \cap S_2$), entonces (a_1, \dots, a_k) es solución de la ecuación diofantina.

Para la otra implicancia, por un lado, si existen $x_1, \dots, x_k, y_1, \dots, y_m$ tales que

$$P_1(a_1, \dots, a_k, x_1, \dots, x_n) = 0,$$

al expandir el polinomio nos queda $0 = c_d P_2(a_1, \dots, a_k, y_1, \dots, y_m)$. Así,

$$P_1(a_1, \dots, a_k, x_1, \dots, x_n) = P_2(a_1, \dots, a_k, y_1, \dots, y_m) = 0.$$

Por otro lado, si suponemos que existen $x_1, \dots, x_k, y_1, \dots, y_m$ tales que

$$P_1(a_1, \dots, a_k, x_1, \dots, x_n) \neq 0$$

tenemos que

$$\begin{aligned}
0 &= \sum_{i=0}^d c_i P_1(a_1, \dots, a_k, x_1, \dots, x_n)^{d-i} P_2(a_1, \dots, a_k, y_1, \dots, y_m)^i \\
&= P_1(a_1, \dots, a_k, x_1, \dots, x_n)^d \sum_{i=0}^d c_i \frac{P_2(a_1, \dots, a_k, y_1, \dots, y_m)^i}{P_1(a_1, \dots, a_k, x_1, \dots, x_n)^i} \\
&= P_1(a_1, \dots, a_k, x_1, \dots, x_n)^d h \left(\frac{P_2(a_1, \dots, a_k, y_1, \dots, y_m)}{P_1(a_1, \dots, a_k, x_1, \dots, x_n)} \right).
\end{aligned}$$

Así, como h no tiene raíces, se tiene que $P_1(a_1, \dots, a_k, x_1, \dots, x_n) = 0$, lo cual contradice la suposición. Por ende, $P_1(a_1, \dots, a_k, x_1, \dots, x_n) = 0$ y $P_2(a_1, \dots, a_k, y_1, \dots, y_m) = 0$, lo cual prueba que la ecuación define $S_1 \cap S_2$. \square

Corolario 1.1.7. *Para R como en el lema 1.1.6, la intersección finita de conjuntos diofantinos es diofantino.*

Consideremos $\mathbb{C}(z)$ el cuerpo de funciones racionales. El siguiente lema está en [8].

Lema 1.1.8. *\mathbb{C} es diofantino en $\mathbb{C}(z)$.*

Demostración. Teorema 2 de [8]. \square

Finalmente, notemos lo siguiente

Lema 1.1.9. *La relación $a \neq 0$ en \mathbb{C} es diofantina.*

Demostración.

$$a \neq 0 \Leftrightarrow \exists b \quad ab = 1$$

\square

Además, por el mismo argumento podemos decir que ser no nulo es diofantino en $\mathbb{C}(z)$.

1.2. Resultantes

Utilizaremos el concepto de resultante para determinar si dos polinomios son o no coprimos en la definición de ciertos conjuntos diofantinos. Para esto vamos a ver también que la resultante es diofantina. Veamos primero el siguiente resultado presente en [1] capítulo 3 sección 5.

Lema 1.2.1. *Sean $f, g \in \mathbb{C}[z]$ polinomios de grados $l \geq 1$ y $m \geq 1$ respectivamente. Luego, f, g tienen un factor común no constante si y sólo si existen polinomios $A, B \in \mathbb{C}[z]$ que cumplen*

1. *A y B no son ambos cero.*

2. A tiene grado a lo más $m - 1$ y B tiene grado a lo más $l - 1$.

3. $Af + Bg = 0$.

Corolario 1.2.2. Sean f, g como en el Lema 1.2.1 y escribimos

$$f = a_l z^l + \dots + a_0$$

$$g = b_m z^m + \dots + b_0.$$

Existen A, B como en el Lema 1.2.1 si y sólo si el siguiente sistema de ecuaciones tiene solución no nula,

$$\left(\begin{array}{r} a_l c_{m-1} + b_m d_{l-1} = 0 \\ a_l c_{m-2} + a_{l-1} c_{m-1} + b_m d_{l-2} + b_{m-1} d_{l-1} = 0 \\ \vdots \\ a_l c_{m-k} + \dots + a_{l-k+1} c_{m-1} + b_m d_{l-k} + \dots + b_{m-k+1} d_{l-1} = 0 \\ \vdots \\ a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 = 0 \\ a_0 c_0 + b_0 d_0 = 0 \end{array} \right),$$

con $c_0, \dots, c_{m-1}, d_0, \dots, d_{l-1}$ indeterminadas.

Demostración. Por un lado, dados A, B como en el lema 1.2.1, podemos escribir

$$A = c_{m-1} z^{m-1} + \dots + c_0$$

$$B = d_{l-1} z^{l-1} + \dots + d_0.$$

Luego, a partir de $Af + Bg = 0$ con las notaciones anteriores se obtiene el sistema

$$\left(\begin{array}{r} a_l c_{m-1} + b_m d_{l-1} = 0 \text{ (coeficiente de } z^{m+l-1}) \\ a_l c_{m-2} + a_{l-1} c_{m-1} + b_m d_{l-2} + b_{m-1} d_{l-1} = 0 \text{ (coeficiente de } z^{m+l-2}) \\ \vdots \\ a_l c_{m-k} + \dots + a_{l-k+1} c_{m-1} + b_m d_{l-k} + \dots + b_{m-k+1} d_{l-1} = 0 \text{ (coeficiente de } z^{m+l-k}) \\ \vdots \\ a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 = 0 \text{ (coeficiente de } z^1) \\ a_0 c_0 + b_0 d_0 = 0 \text{ (coeficiente de } z^0) \end{array} \right).$$

Por ende, dada la existencia de A y B , este sistema tiene solución, que es no nula porque A, B no son ambos nulos.

Por otro lado, si el sistema tiene solución no nula, la denotamos $(\widetilde{c}_0, \dots, \widetilde{c}_{m-1}, \widetilde{d}_0, \dots, \widetilde{d}_{l-1})$ y podemos definir los polinomios

$$A = \widetilde{c}_{m-1} z^{m-1} + \dots + \widetilde{c}_0$$

$$B = \widetilde{d}_{l-1} z^{l-1} + \dots + \widetilde{d}_0.$$

Así, se tiene que A, B no son ambos nulos, con grado de A a lo más $m - 1$, grado de B a lo más $l - 1$ y cumpliendo $Af + Bg = 0$, ya que al desarrollar esta expresión se obtiene el sistema anterior. \square

Como sabemos por álgebra lineal que el sistema del corolario anterior tiene solución si y sólo si el determinante de la matriz del sistema es nulo; realizamos la siguiente definición.

Definición 1.2.3. Sean $f, g \in \mathbb{C}[z]$ de grado positivo. Escribimos

$$f = a_0 z^l + \dots + a_l.$$

$$g = b_0 z^m + \dots + b_m.$$

Luego, definimos la *resultante* de f y g , denotada $res(f, g)$ como

$$res(f, g) = \det \begin{pmatrix} a_0 & & & b_0 & & & \\ a_1 & a_0 & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & \vdots & & \ddots & b_0 \\ & \vdots & \ddots & a_0 & \vdots & & \\ a_l & & & b_m & & & \\ & a_l & & & b_m & & \\ & & \ddots & & & \ddots & \\ & & & a_l & & & b_m \end{pmatrix},$$

donde los espacios en blanco son ceros y las primeras m columnas se forman con los coeficientes de f y las siguientes l columnas se forman con los coeficientes de g . Es decir, es el determinante de una matriz $(m+l) \times (m+l)$ formada con los coeficientes de f y g . Esta matriz es llamada matriz de Sylvester.

Lema 1.2.4. *Dados $f, g \in \mathbb{C}(z)$, se tiene que $res(f, g)$ es un polinomio con coeficientes en \mathbb{C} evaluado en los coeficientes de f y g . Además, f, g tienen un divisor común no constante si y sólo si $res(f, g) = 0$*

Demostración. Recordemos que la expresión clásica para el determinante de $A = (a_{ij})_{1 \leq i, j \leq n}$ una matriz $n \times n$ es

$$\sum_{\sigma \text{ permutación de } \{1, \dots, n\}} \text{sgn}(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \dots \cdot a_{n\sigma(n)},$$

donde sgn es la función signo que toma el valor 1 para permutaciones pares y -1 para permutaciones impares. Luego, los coeficientes del determinante son enteros. Además, $res(f, g)$ es un polinomio que tiene por entradas los coeficientes de f y g .

Para la segunda parte, notemos que el resultante es cero si y sólo si la matriz de Sylvester para f y g tiene determinante cero. Esto último ocurre si y sólo si el sistema de ecuaciones del Corolario 1.2.2 tiene solución no nula. Como esto último es equivalente a la existencia de A y B como en el Lema 1.2.1 (probado en el Corolario 1.2.2); la conclusión se obtiene por lo probado en este Lema. \square

Ejemplo: Los polinomios $x^3 + x - 1$ y $2x^2 + 3x + 7$ no tienen factores comunes. Esto pues,

$$\text{res}(x^3 + x - 1, 2x^2 + 3x + 7) = \det \begin{pmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 1 & 0 & 7 & 3 & 2 \\ -1 & 1 & 0 & 7 & 3 \\ 0 & -1 & 0 & 0 & 7 \end{pmatrix} = 159 \neq 0.$$

Para esta tesis es fundamental el siguiente lema

Lema 1.2.5. *res(f, g) es una relación diofantina sobre $\mathbb{C}(z)$*

Demostración. Por el Lema 1.2.4, sabemos que la resultante es un polinomio con coeficientes en \mathbb{C} . Por ende, la resultante es diofantina. \square

1.3. Curva elíptica de Denef

Vamos a definir una curva elíptica especial y exponer un par de propiedades para ella demostradas por Denef en [4].

Recordemos que las curvas elípticas sobre \mathbb{Q} tienen una operación de grupo conmutativo denotada “+” con neutro el punto al infinito $\mathbf{0}$. Dado P punto de la curva elíptica, denotaremos $m \cdot P$ a la suma de P repetida m veces.

Es un hecho conocido que si el j invariante de una curva elíptica definida sobre \mathbb{Q} no es entero, entonces esa curva no tiene multiplicación compleja, por lo que los únicos mapeos \mathbb{C} -racionales de E en E que fijan el $\mathbf{0}$ de E son $P \mapsto m \cdot P$. Así, sea E_0 curva elíptica definida sobre \mathbb{Q} sin multiplicación compleja con ecuación $y^2 = x^3 + ax + b$ (se puede verificar que existen curvas que cumplen esto en [12]) y asociemos a ella la curva elíptica E de ecuación

$$(z^3 + az + b)y^2 = x^3 + ax + b$$

definida sobre $\mathbb{Q}(z)$ (esta curva se puede pensar también como superficie elíptica sobre \mathbb{Q}). Tenemos que el punto $(z, 1)$ es pertenece a E . Denotamos $P_1 = (z, 1)$. Como \mathbb{C} es de característica 0 tenemos que

Lema 1.3.1. *El punto P_1 es de orden infinito y genera el grupo $E(\mathbb{C}(z))$ salvo puntos de torsión (que tienen orden 2).*

Demostración. Lema 3.1 de [4]. \square

Denotando $P_n = (x_n, y_n) = n \cdot P_1$ tenemos que

Lema 1.3.2. *Para cualquier n entero no nulo tenemos que $\frac{x_n}{zy_n} - n$ toma el valor cero al infinito.*

Demostración. Lema 3.2 de [4]. \square

1.4. Alturas

En esta sección veremos algunas propiedades de las alturas que serán utilizadas más adelante, para una visión más detallada se puede revisar [7] y [10].

Nuestro objetivo es utilizar alturas para entender el crecimiento del grado de funciones racionales. Para eso veamos primero cómo extendemos el grado de los polinomios a $f \in \mathbb{C}(z)$

1.4.1. Grado de funciones racionales

Existen distintas maneras de extender la definición de grado desde polinomios a funciones racionales. En este caso tendremos la siguiente definición para el grado.

Definición 1.4.1. Para $f \in \mathbb{C}(z)$ diremos que $\deg(f)$ es el grado del mapeo $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ inducido por f .

En el caso de funciones racionales esta definición se corresponde con el máximo entre los grados de numerador y denominador de f .

Algunas propiedades del grado son las siguientes

1. Las constantes tienen grado 0, incluso para $f = 0$.
2. Si $g \in \mathbb{C}[z]$ es no constante, entonces $\deg(g)$ coincide con la definición usual del grado de los polinomios, pues el grado del denominador sería 0.

Para $f \in \mathbb{C}(z)$ consideramos $\text{Pole}(f)$ como el divisor de polos de f , que es la suma de las multiplicidades de cada polo. Así, tenemos la siguiente igualdad.

Lema 1.4.2. Si $f \in \mathbb{C}(z)$, se tiene que $\deg(f) = \deg \text{Pole}(f)$.

Demostración. Sea $f(z) = P(z)/Q(z)$, con $P(z), Q(z)$ polinomios coprimos.

Así, $\deg(f) = \max\{\deg(P), \deg(Q)\}$.

Para calcular el divisor de polos necesitamos la versión homogénea de f . Como el grado del divisor de polos es la multiplicidad de cada polo tenemos que $\deg \text{Pole}(f) = \max\{\deg P, \deg Q\}$, pues este máximo es el grado de la versión homogénea.

Por ende, $\deg(f) = \deg \text{Pole}(f)$. □

1.4.2. Altura canónica

El siguiente teorema se encuentra en [10] página 106.

Teorema 1.4.3. Para cualquier clase de divisores $c \in \text{Pic}(A)$, la altura h_c es cuasi-cuadrática. Existen una única forma cuadrática q_c y una única forma lineal l_c tales que

$$h_c = q_c + l_c + O(1)$$

Si c es par, entonces $l_c = 0$.

En este teorema, $\text{Pic}(A)$ es el grupo de Picard de A variedad abeliana. Para más detalles revisar [10].

Este teorema es similar al caso planteado en [7] página 199 (que sólo sirve para cuerpos de números).

En la misma página 106 de [10] se define la altura canónica (altura Néron-Tate) asociada a c como $q_c + l_c$.

De este modo, podemos afirmar que

Lema 1.4.4. *Dada E una curva elíptica sobre $\mathbb{Q}(z)$ y P_1 punto racional. Denotamos h a la altura canónica. Considerando $P_n = n \cdot P_1 = P_1 + \dots + P_1$ (n veces), se tiene que*

$$h(P_n) \sim cn^2$$

Demostración. Tenemos que $h(P_n) = q_c(P_n) + l_c(P_n)$ y como son formas cuadrática y lineal respectivamente tenemos que $h(P_n) \sim n^2 h(P_1) + O(n)$. Considerando $c = h(P_1)$ se deduce que $h(P_n) \sim cn^2$. \square

1.4.3. Altura en $\mathbb{C}(z)$

Notemos primero que una función racional $f = \frac{a}{b} \in \mathbb{C}(z)$ con a, b polinomios coprimos se puede entender como un punto en $\mathbb{P}_{\mathbb{C}(z)}^1$ dado por $[\frac{a}{b} : 1] = [a : b]$. En la página 62 de [10] se define la altura H para un punto $P = [a : b] \in \mathbb{P}_{\mathbb{C}(z)}^1$ como

$$H(P) = \prod_{\mathfrak{p}} \max\{|a|_{\mathfrak{p}}, |b|_{\mathfrak{p}}\}.$$

En esta definición, $|\cdot|_{\mathfrak{p}}$ es el valor absoluto asociado al divisor racional primo \mathfrak{p} , se puede ver [10], a partir de la página 21.

Aplicando logaritmo obtenemos la altura h dada por

$$h_{\mathbb{P}_{\mathbb{C}(z)}^1} = \sum_{z \in \mathbb{P}_{\mathbb{C}}^1} \max\{v_z(a), v_z(b)\},$$

donde v_z son los valores absolutos asociados a $|\cdot|_{\mathfrak{p}}$.

Luego, tenemos el siguiente lema

Lema 1.4.5. *Dada $f \in \mathbb{C}(z)$, tenemos que $h_{\mathbb{P}_{\mathbb{C}(z)}^1}(f) = \deg(f)$*

Demostración. Tenemos el siguiente cálculo,

$$\begin{aligned} h_{\mathbb{P}_{\mathbb{C}(z)}^1}(f) &= h_{\mathbb{P}_{\mathbb{C}(z)}^1}([a : b]) = \sum_{z \in \mathbb{P}_{\mathbb{C}}^1} \max\{v_z(a), v_z(b)\} \\ &= \sum_{z \in \mathbb{C}} \max\{v_z(a), v_z(b)\} + \max\{v_{\infty}(a), v_{\infty}(b)\} \\ &= \deg(a) + \deg(b) + \max\{-\deg(a), -\deg(b)\} = \max\{\deg(a), \deg(b)\}. \end{aligned}$$

Como a, b son coprimos tenemos que $v_z(a), v_z(b)$ no pueden ser ambos no nulos para cada $z \in \mathbb{C}$. Luego, si $v_z(a)$ o $v_z(b)$ son no nulos es porque z es raíz del polinomio y así, al sumar sobre $z \in \mathbb{C}$ se recorren todas las raíces y se obtiene el grado, de ahí que la última igualdad se cumple.

Por la definición de v_∞ se tiene que $\max\{v_\infty(a), v_\infty(b)\} = \max\{-\deg(a), -\deg(b)\}$. \square

Luego, (ver página 77 de [10]) podemos definir para $\varphi : X \rightarrow \mathbb{P}^1$, con $X/\mathbb{C}(z)$ curva suave proyectiva, la altura para un punto $P \in X$ como

$$h_\varphi(P) = h_{\mathbb{P}^1_{\mathbb{C}(t)}}(\varphi(P)).$$

Finalmente, si asociamos un divisor D a $\varphi : X \rightarrow \mathbb{P}^1$ de modo que $D = \varphi^*(\infty)$ (ver página 88 de [10]), podemos definir la siguiente altura

$$h_D(P) = h_\varphi(P).$$

Así, tenemos el siguiente lema

Lema 1.4.6. Sean $\varphi, \psi : X \rightarrow \mathbb{P}^1$ morfismos no constantes de grados m, n , respectivamente. Luego,

$$h_\varphi(P) \sim \frac{m}{n} h_\psi(P).$$

Demostración. Denotando $D = \varphi^*(\infty)$ y $C = \psi^*(\infty)$ tenemos que $h_D = h_\varphi$ y $h_C = h_\psi$. Por el corolario 3.3.5 de [10], se deduce que $h_\varphi(P) \sim \frac{m}{n} h_\psi(P)$. \square

1.5. Dimensión Diofantina

La dimensión diofantina es clave para las demostraciones por contradicción que se realizan en los capítulos siguientes. Introduzcamos primero una notación.

Definición 1.5.1. Para $D \subseteq \mathbb{C}(z)$ y $\alpha \geq 0$, definimos $D_\alpha = \{f \in D : \deg(f) \leq \alpha\}$.

Podemos notar que $\mathbb{C}(z)_\alpha$ es una variedad algebraica sobre \mathbb{C} . Esto pues, $\mathbb{C}(z)_\alpha$ son las fracciones de polinomios coprimos con grado a lo más α , así que considerando los coeficientes se tiene la estructura de variedad.

Denotaremos la dimensión diofantina de $D \subseteq \mathbb{C}(z)$ por $\text{ddim}(D)$ y se define como sigue

Definición 1.5.2. La *dimensión diofantina* de $D \subseteq \mathbb{C}(z)$ es el $d \in \{-1, 0, 1, 2, \dots, \infty\}$ más pequeño tal que para cada $\alpha \geq 0$, el conjunto D_α está contenido en una unión numerable de subvariedades de $\mathbb{C}(z)_\alpha$ definidas sobre \mathbb{C} con dimensión menor o igual que d .

Ejemplos:

1. $\text{ddim}(D) = -1$ si y sólo si $D = \emptyset$.

Por un lado, como $\emptyset \subseteq \emptyset$ y como $\dim \emptyset = -1$, tenemos que $\text{ddim}(\emptyset) = -1$.

Por otro lado, si $\text{ddim}(D) = -1$ tenemos que D está contenido en una unión numerable de conjuntos vacíos, pues es la única variedad con dimensión -1, es decir, $D \subseteq \emptyset$. Esto implica que $D = \emptyset$.

2. $\text{ddim}(D) = 0$ si y sólo si D es numerable.

Si $\text{ddim}(D) = 0$ entonces D está contenido en una unión numerable de conjuntos finitos, lo cual implica que D es numerable.

Si D es numerable, podemos escribir $D = \{d_n \in D : n \in \mathbb{N}\}$ y por ende, $D \subseteq \cup_{n \in \mathbb{N}} \{d_n\}$. Así, $\text{ddim}(D) = 0$.

3. $\text{ddim}(\{\lambda z^d : \lambda \in \mathbb{C}, d \in \mathbb{Z}\}) = 1$.

Notemos primero que $\{\lambda z^d : \lambda \in \mathbb{C}, d \in \mathbb{Z}\}_\alpha$ es no numerable, pues para cada $n \leq \alpha$, con $n \in \mathbb{Z}$ la cardinalidad depende de los coeficientes, que son complejos. Por ende, $\{\lambda z^d : \lambda \in \mathbb{C}, d \in \mathbb{Z}\}_\alpha$ no se puede contener en una unión numerable de subvariedades de dimensión 0 (que son finitas).

Como para $d \in \mathbb{Z}$ fijo, el conjunto $\{\lambda z^d : \lambda \in \mathbb{C}\}$ tiene dimensión 1, podemos contener $\{\lambda z^d : \lambda \in \mathbb{C}, d \in \mathbb{Z}\}_\alpha$ en una unión numerable de subvariedades de dimensión 1 de la forma $\{\lambda z^d : \lambda \in \mathbb{C}\}$ para $d \in \mathbb{Z}$ fijo (incluso finita al considerar los $d \leq \alpha$, con $d \in \mathbb{Z}$). Por ende, $\text{ddim}(\{\lambda z^d : \lambda \in \mathbb{C}, d \in \mathbb{Z}\}) = 1$.

4. $\text{ddim}(\mathbb{C}[z]) = \infty$

Notemos primero que $\mathbb{C}[z]_1 = \{\lambda_1 z + \lambda_0 : \lambda_i \in \mathbb{C}\}$. Como es un conjunto no numerable no se puede contener con subvariedades de dimensión 0. Las subvariedades de dimensión 1 tendrían fijo uno de los coeficientes, por lo que sigue siendo no numerable. Así, como $\mathbb{C}[z]_1$ tiene dimensión 2, se concluye que $\mathbb{C}[z]_1$ está contenido en una unión numerable con dimensión menor o igual a 2.

Para un α fijo se puede repetir el mismo argumento que en $\mathbb{C}[z]_1$ y concluir que $\mathbb{C}[z]_{\lfloor \alpha \rfloor}$ está contenido en una unión numerable de subvariedades de dimensión a lo más $\lfloor \alpha \rfloor$ y que no se puede contener con dimensión $\lfloor \alpha \rfloor - 1$.

Como la definición requiere que α sea cualquiera, se concluye que $\text{ddim}(\mathbb{C}[z]) = \infty$.

1.6. Un conjunto no diofantino sobre $\mathbb{C}(z)$

En esta sección veremos el resultado que se busca extender en esta tesis. Se puede revisar con más detalle en [5].

En el trabajo de García-Fritz, Pastén y Pheidias; se considera un cuerpo no numerable grande (*large*) de característica 0. En nuestro caso, lo reduciremos a \mathbb{C} , que cumple con estas tres condiciones. Además, la extensión del grado para las funciones racionales que utilizan es la que mencionamos en la sección 1.5 de esta tesis.

El siguiente teorema es el resultado principal de Kollar en [9]; escrito en una forma menos general, pero más sencilla de usar en el contexto de $\mathbb{C}(z)$ que se puede revisar en [5].

Teorema 1.6.1. *Sea $D \subseteq \mathbb{C}(z)$ un subconjunto diofantino sobre $\mathbb{C}(z)$. Si $\text{ddim}(D) = \infty$, entonces existe $a \geq 0$, $P_a \in S^a \mathbb{P}^1(\mathbb{C})$ y $r \geq 1$ tal que para todo $m \geq 1$ se tiene*

$$P_a + r \cdot S^m \mathbb{P}^1 \subseteq \overline{\text{Pole}_{a+rm}(D)}$$

en $S^{a+rm} \mathbb{P}^1$.

Aquí $S^a\mathbb{P}^1$ es la potencia simétrica de \mathbb{P}^1 y $\text{Pole}_\ell(D) = \{\text{Pole}(f) : \deg(f) = \ell\}$; para más detalles ver [5].

Los siguientes resultados se encuentran en [5] con su correspondiente demostración.

Lema 1.6.2. *Sea $D \subseteq \mathbb{C}(z)$ subconjunto diofantino sobre $\mathbb{C}(z)$. Si $\text{ddim}(D) = \infty$, entonces el conjunto $\{\deg(f) : f \in D\}$ contiene una progresión aritmética infinita.*

Demostración. Corolario 4.2 de [5]. □

Teorema 1.6.3. *Sea E curva elíptica sobre $\mathbb{Q}(z)$ definida por la ecuación de Weierstrass $y^2 = x^3 + zx + 1$ y fijamos el punto $\mathbb{Q}(z)$ -racional $P_1 = (x, y) = (0, 1)$. Para cada $n \in \mathbb{Z}$ sea $P_n = n \cdot P_1$ y para $n \neq 0$ definimos $x_n, y_n \in \mathbb{Q}(z)$ como $P_n = (x_n, y_n)$. Entonces tenemos lo siguiente:*

1. *Para $n \neq 0$ tenemos la fórmula asintótica $\deg(x_n) \sim n^2/2$.*
2. *Para todo cuerpo K de característica 0, el conjunto de los puntos $K(z)$ -racionales de E es $\{P_n : n \in \mathbb{Z}\}$.*

Demostración. Lema 4.3 de [5]. □

Como corolario del teorema 1.6.3 se tiene lo siguiente, al considerar los x_n .

Teorema 1.6.4. *Sea K cuerpo de característica 0. Existe un conjunto $D \subseteq K(z)$ diofantino sobre $K(z)$ cumpliendo que el conjunto $\{\deg(f) : f \in D\} \subseteq \mathbb{N}$ está formado por una secuencia de crecimiento cuadrático.*

Demostración. Corolario 4.4 de [5]. □

Con todo esto tenemos las herramientas para ver la demostración del teorema 1.8 de [5] que escribimos aquí.

Teorema 1.6.5. *El conjunto*

$$\text{Deg} = \{(f, g) \in \mathbb{C}(z)^2 : \deg(f) = \deg(g)\}$$

es no diofantino sobre $\mathbb{C}(z)$.

Demostración. Supongamos por contradicción que Deg es diofantino sobre $\mathbb{C}(z)$. Sea D como en el Teorema 1.6.4 con $K = \mathbb{C}$. Luego,

$$D' = \{f \in \mathbb{C}(z) : \exists g \in D, \deg(f) = \deg(g)\}$$

es diofantino sobre $\mathbb{C}(z)$, pues D y Deg lo son.

Por un lado, como $\{\deg(g) : g \in D\}$ tiene crecimiento cuadrático, este conjunto no contiene una progresión aritmética infinita. Así, por el Lema 1.6.2, $\text{ddim}(D')$ es finita.

Por otro lado, como $\{\deg(g) : g \in D\}$ es un subconjunto infinito de \mathbb{N} y como D' es unión de $\{f \in \mathbb{C}(z) : \deg(f) = n\}$ para $n \in \{\deg(g) : g \in D\}$; tenemos que $\text{ddim}(D') = \infty$.

Esto es una contradicción, por lo que Deg es no diofantino sobre $\mathbb{C}(z)$. □

El mismo esquema de demostración utilizado aquí es el que usaremos en los capítulos posteriores.

Capítulo 2

Lemas previos y notaciones

En este capítulo vamos a ver algunos resultados que nos van a permitir trabajar en casos concretos para los próximos capítulos.

En primer lugar, vamos a considerar $\mathbb{N} = \{0, 1, 2, 3, \dots, n, \dots\}$ y $\mathbb{C}(z)$ el cuerpo de funciones racionales. Así,

$$f \in \mathbb{C}(z) \Leftrightarrow f(z) = \frac{P(z)}{Q(z)},$$

con $P(z), Q(z) \in \mathbb{C}[z]$ coprimos y $Q(z)$ no es el polinomio nulo.

En segundo lugar, el lenguaje utilizado en esta tesis es el lenguaje de anillos conmutativos con unidad ($\{=, +, \cdot, 0, 1\}$), junto con z como trascendente sobre el anillo correspondiente, la cual representará a la variable. Así, $\mathcal{L} = \{=, +, \cdot, 0, 1, z\}$.

Finalmente, de aquí en adelante vamos a considerar conjuntos diofantinos sobre $\mathbb{C}(z)$ y no lo repetiremos en cada ocasión.

2.1. ¿Por qué $\mathbb{Q}[x, y]$ y no $\mathbb{C}[x, y]$?

La siguiente definición busca generalizar el resultado del Teorema [1.6.5](#).

Definición 2.1.1. Dado $G \in \mathbb{C}[x, y]$ definimos

$$A_G = \{(f, g) \in \mathbb{C}(z)^2 : G(\deg f, \deg g) = 0\}.$$

Así, el conjunto $\text{Deg} = \{(f, g) \in \mathbb{C}(z)^2 : \deg(f) = \deg(g)\}$, se escribe como $A_G \subseteq \mathbb{C}(z)^2$ para $G(x, y) = x - y$.

Vamos a analizar si este tipo de conjuntos son o no son diofantinos. Para esto, a lo largo de esta sección, vamos a definir conceptos y notaciones utilizados en esta tesis, y a demostrar lemas que usaremos en las secciones posteriores. Además, vamos a justificar el porqué en las secciones siguientes pasamos de $G \in \mathbb{C}[x, y]$ a $G \in \mathbb{Q}[x, y]$.

Como los grados de los elementos en $\mathbb{C}(z)$ son siempre naturales, el siguiente concepto se repite en las demostraciones de esta tesis.

Definición 2.1.2. Diremos que $(m, n) \in \mathbb{C}^2$ es *solución natural* de $G(x, y) \in \mathbb{C}[x, y]$ si y sólo si $G(m, n) = 0$ y $m, n \in \mathbb{N}$.

El siguiente lema nos permite concluir que ciertos A_G son diofantinos, para gran parte de los $G(x, y) \in \mathbb{C}[x, y]$.

Lema 2.1.3. *Sea $G(x, y) \in \mathbb{C}[x, y]$. Si G tiene a lo más finitas soluciones naturales entonces A_G es diofantino.*

Demostración. Si $f, g \in \mathbb{C}(z)$ tenemos que, como $\deg f, \deg g \in \mathbb{N}$, nos interesa conocer las soluciones naturales de $G(x, y) = 0$. Luego, para cada solución natural $(m, n) = (\deg f, \deg g)$ tenemos el conjunto

$$\begin{aligned} A_{(m,n)} &= \{(f, g) \in \mathbb{C}(z)^2 : \deg f = m \wedge \deg g = n\} \\ &= \{(f, g) \in \mathbb{C}(z)^2 : (\exists c_0, \dots, c_m, d_0, \dots, d_m \in \mathbb{C} \\ &\quad (d_m z^m + \dots + d_0)f = c_m z^m + \dots + c_0 \wedge \text{res}(c_m z^m + \dots + c_0, d_m z^m + \dots + d_0) \neq 0) \\ &\quad \wedge (\exists a_0, \dots, a_n, b_0, \dots, b_n \in \mathbb{C} \\ &\quad (b_n z^n + \dots + b_0)g = a_n z^n + \dots + a_0 \wedge \text{res}(a_n z^n + \dots + a_0, b_n z^n + \dots + b_0) \neq 0)\} \end{aligned}$$

que es diofantino por Lema 1.1.8, Lema 1.2.5 y Lema 1.1.9. Luego, si $(m_1, n_1), \dots, (m_k, n_k)$ son las finitas soluciones naturales de G tenemos que

$$A_G = \bigcup_{j=1}^k A_{(m_j, n_j)},$$

que al ser unión finita de conjuntos diofantinos es diofantino por Corolario 1.1.5. □

Utilizaremos la siguiente notación, con (\cdot, \cdot) el máximo común divisor de \mathbb{Z} :

Notación 2.1.4. Si $a, a_i \in \mathbb{Q}$, definimos $p_a, q_a, p_i, q_i \in \mathbb{Z}$ de modo que

1. $a = \frac{p_a}{q_a}$ y $a_i = \frac{p_i}{q_i}$, con $q_a, q_i \neq 0$.
2. $(p_a, q_a) = 1$ y $(p_i, q_i) = 1$.
3. Si $a, a_i \leq 0$ entonces, $p_a, p_i \leq 0$ y $q_a, q_i > 0$.

Es decir, esta notación nos permite escribir la fracción reducida correspondiente a cada racional.

La siguiente definición es útil para quedarnos solamente con los $G(x, y) \in \mathbb{Q}[x, y]$.

Definición 2.1.5. Dado $G \in \mathbb{C}[x, y]$, sea K/\mathbb{Q} el cuerpo generado por los coeficientes de G y sea \mathcal{B} base de K sobre \mathbb{Q} (como espacio vectorial). Denotamos $r = |\mathcal{B}|$. Definimos $G_{q_i}(x, y) \in \mathbb{Q}[x, y]$ para cada $q_i \in \mathcal{B}$ con $i \in \{1, \dots, r\}$ de modo que

$$G(x, y) = G_{q_1}(x, y)q_1 + \dots + G_{q_r}(x, y)q_r.$$

Notemos que $r < \infty$, porque los coeficientes del polinomio son finitos. Tenemos así el siguiente lema.

Lema 2.1.6. *Sea $G \in \mathbb{C}[x, y]$. Con la notación de la definición 2.1.5, si existe $q \in \mathcal{B}$ tal que $G_q(x, y) = 0$ tiene a lo más finitas soluciones naturales, entonces A_G es diofantino.*

Demostración. Consideremos \mathcal{B} como en la Definición 2.1.5.

Para $f, g \in \mathbb{C}(z)$ tenemos que $(\deg f, \deg g) \in \mathbb{N}^2$ y de ahí que $G(\deg f, \deg g)$ es una combinación lineal en \mathbb{Q} de los elementos de \mathcal{B} . Luego, $G(\deg f, \deg g) = 0 \Leftrightarrow G_q(\deg f, \deg g) = 0$ para todo $q \in \mathcal{B}$, por la independencia lineal sobre \mathbb{Q} .

Así, si existe $q \in \mathcal{B}$ con a lo más finitas soluciones naturales, tenemos que las soluciones naturales de $G(x, y) = 0$ son a lo más las soluciones naturales de $G_q(x, y) = 0$.

Por Lema 2.1.3 se concluye que A_G es diofantino. \square

Veamos un ejemplo concreto.

Ejemplo: Sea

$$G(x, y) = (5 + 3i - 2\sqrt{5})x + (9 - 2i - 5\sqrt{5} + 3\sqrt{3})y \in \mathbb{C}[x, y].$$

En este caso tenemos que $\{1, i, \sqrt{5}, \sqrt{3}\}$ es un conjunto de elementos linealmente independientes sobre \mathbb{Q} y que los coeficientes de $G(x, y)$ están contenidos en $\mathbb{Q}(i, \sqrt{3}, \sqrt{5})$. Podemos escribir lo siguiente:

$$G(x, y) = (5x + 9y) \cdot 1 + (3x - 2y)i + (-2x - 5y)\sqrt{5} + (3y)\sqrt{3}.$$

Así, por ejemplo, $G_{\sqrt{5}}(x, y) = -2x - 5y$.

Luego, como vamos a evaluar en pares naturales, se tiene que

$$G(\deg f, \deg g) = 0 \Leftrightarrow \begin{pmatrix} 5 \deg f + 9 \deg g = 0 \wedge \\ 3 \deg f - 2 \deg g = 0 \wedge \\ -2 \deg f - 5 \deg g = 0 \wedge \\ 3 \deg g = 0 \end{pmatrix}.$$

Con esta equivalencia, pasamos de un polinomio con coeficientes complejos, a finitos polinomios con coeficientes racionales (que deben ser todos anulados simultáneamente). La única solución natural en este caso sería $(0, 0)$.

En el Lema 3.0.2 tenemos soluciones naturales infinitas (Una de las coordenadas de $(f, g) \in \mathbb{C}(z)^2$ queda libre) descritas de forma diofantina.

Por el Lema 2.1.6, si A_G es no diofantino entonces todos los $G_q(x, y)$ (como en Definición 2.1.5) tienen infinitas soluciones naturales, que además son comunes entre ellos. Así, que un conjunto A_G sea diofantino o no diofantino, depende de si es posible describir las soluciones de los $G_q(x, y) = 0$ de forma diofantina o no. Es decir, si las soluciones comunes se pueden escribir de forma diofantina, entonces el conjunto A_G es diofantino. Mientras que si las soluciones comunes no se pueden escribir de forma diofantina, se puede adaptar la misma demostración que prueba que no se pueden escribir de forma diofantina para los G_q .

Nos centraremos en $G(x, y) \in \mathbb{Q}[x, y]$ porque nos basta con saber las soluciones de los finitos

polinomios que obtenemos según la Definición 2.1.5.

La idea original era que a lo más finitas soluciones naturales implican diofantino e infinitas soluciones naturales implican no diofantino, dados los resultados (ver Lema 3.0.2) lo correcto debería ser la siguiente conjetura

Conjetura 2.1. *Dado $G(x, y) \in \mathbb{C}[x, y]$ se tiene que*

1. *Si $G(x, y) = 0$ tiene a lo más finitas soluciones o si las infinitas soluciones están dadas por una coordenada fija y la otra libre, entonces A_G es diofantino.*
2. *En otro caso, A_G es no diofantino.*

En el capítulo 5 se comenta un poco más esta idea.

En los capítulos siguientes; para probar que un conjunto A_G , con $G(x, y) \in \mathbb{Q}[x, y]$, es no diofantino; vamos a asumir que es diofantino y veremos que las infinitas soluciones a $G(x, y) = 0$, forman con sus grados una secuencia infinita de crecimiento al menos cuadrático, y concluiremos la contradicción con los siguientes dos lemas.

Lema 2.1.7. *Sea $\{r_i : i \in \mathbb{N}\} \subseteq \mathbb{N}$ subconjunto infinito. Sea $D = \{f \in \mathbb{C}(z) : \exists i, \deg f = r_i\}$. Entonces, $\text{ddim}(D) = \infty$.*

Demostración. Para cada r_i fijo tenemos que $\{f \in \mathbb{C}(z) : \deg f = r_i\}$ tiene dimensión $2r_i + 1$ y no es posible contenerlo en una unión numerable de subvariedades con dimensión a lo más $2r_i$, porque esta dimensión nos deja libre un coeficiente de f que, al tomar valores en \mathbb{C} , tiene no numerables posibilidades. Luego, si para α fijo se tiene que $D_\alpha = \{f \in \mathbb{C}(z) : \deg f = r_1 \vee \dots \vee \deg f = r_n\}$, entonces $D_{\{\alpha\}}$ se puede contener en una unión numerable de subvariedades de dimensión a lo más $2r_n + 1$ y no menos.

Como los grados de los elementos de D son infinitos se tiene que $\text{ddim}(D) = \infty$. □

Lema 2.1.8. *Sea $D \subseteq \mathbb{C}(z)$. Si $\{\deg f : f \in D\}$ forma una secuencia de crecimiento al menos cuadrático, entonces $\text{ddim}(D) < \infty$.*

Demostración. Notemos que si $\{\deg f : f \in D\}$ forma una secuencia de crecimiento al menos cuadrático, entonces no es posible que contenga una progresión aritmética. Por Lema 1.6.2 se deduce que $\text{ddim}(D) < \infty$. □

2.2. Conjuntos diofantinos con condiciones de congruencia para el grado

En esta sección demostraremos que dados enteros positivos a, k , existe un conjunto diofantino $D_a^k \subset \mathbb{C}(z)$ tal que para cada $f \in D_a^k$ se cumple que $\deg f \equiv k \pmod{a}$.

Con este objetivo, consideremos la curva elíptica sobre $\mathbb{Q}(z)$ de la sección 1.3 con $a = b = 1$ (se puede verificar en [12] que cumple con lo pedido por Deneff)

$$E : (z^3 + z + 1)y^2 = x^3 + x + 1.$$

Definimos a partir de $P_1 = (z, 1)$ el punto P_n como $P_n = (x_n, y_n) = n \cdot P_1$.

Lema 2.2.1. *Existe $c > 0$ tal que $\deg(x_n) \sim cn^2$*

Demostración. Por Lema 1.4.4 se tiene que $h(P_n) \sim cn^2$. Como $P_n = (x_n, y_n)$ se tiene que $\deg(x_n) \sim cn^2$. \square

Definimos $f_n = \frac{x_n}{zy_n}$ para la cual tenemos el siguiente resultado.

Lema 2.2.2. *Existe una constante $d > 0$ tal que $\deg(x_n) \sim d \cdot \deg(f_n)$*

Demostración. Definimos $f : E \rightarrow \mathbb{P}^1$ como $f(x, y) = \frac{x}{zy}$ y $\varphi : E \rightarrow \mathbb{P}^1$ como la función coordenada x . Así, $\varphi(x_n, y_n) = x_n$ y $f(x_n, y_n) = f_n$. Luego, por las definiciones dadas en la subsección 1.4.3 tenemos que

$$\deg(x_n) = h_{\mathbb{P}^1_{\mathbb{C}(z)}}(\varphi(x_n, y_n)) = h_\varphi(x_n, y_n)$$

$$\deg(f_n) = h_{\mathbb{P}^1_{\mathbb{C}(z)}}(f(x_n, y_n)) = h_f(x_n, y_n)$$

Se concluye por el Lema 1.4.6 que $\deg(x_n) \sim d \cdot \deg(f_n)$ con d la fracción de los grados de los morfismos φ, f . \square

Lema 2.2.3. $\deg(x_n) = \deg(zy_n)$

Demostración. Por Lema 1.3.2; tenemos que, para cualquier n no nulo, $f_n - n$ toma el valor cero en el infinito, de donde deducimos que el denominador de $f_n - n$ tiene grado mayor que su numerador. Luego, como

$$f_n - n = \frac{x_n}{zy_n} - n = \frac{x_n - nzy_n}{zy_n},$$

se tiene que $\deg(x_n - nzy_n) < \deg(zy_n)$. Así, $\deg(x_n) = \deg(nzy_n) = \deg(zy_n)$, pues es necesario que los términos de mayor grado se cancelen en la resta. \square

Lema 2.2.4. *Para todo $n \geq 1$ se tiene que $y_n(1) \neq 0$.*

Demostración. Supongamos por contradicción que $y_n(1) = 0$ para algún n . Así,

$$0 = (z^3 + z + 1)y_n^2(1) = x_n^3(1) + x_n(1) + 1.$$

Como P_n es un $\mathbb{C}(z)$ -punto racional (Lema 1.3.1) tenemos que $x_n(1) \in \mathbb{Q}$, pero como $x^3 + x + 1$ es irreducible en \mathbb{Q} , esto no es posible. Por lo tanto, $y_n \neq 0$ para cualquier n . \square

Lema 2.2.5. *Dado a entero positivo y $k \in \{0, \dots, a - 1\}$ existe un conjunto $D_a^k \subset \mathbb{C}(z)$ diofantino sobre $\mathbb{C}(z)$ tal que $\{\deg f : f \in D_a^k\}$ está formado por una secuencia de crecimiento cuadrático, cuyos elementos cumplen que $\deg f \equiv k \pmod{a}$.*

Demostración. Los puntos (x_n, y_n) definidos en esta sección se obtienen de forma diofantina, por lo que $F = \{f_n : n > 1\}$ es diofantino. Así, definimos $D_a^k = \{g \in \mathbb{C}(z) : \exists f_n \in F : g = f_n^a(z - 1)^k\}$ el cual es diofantino, pues tomar potencia y multiplicar lo es (z es parte del lenguaje).

Luego, tenemos que, por Lema 2.2.3 y Lema 2.2.4, $\deg(g_n) = a \deg(f_n) + k$. Esto pues, al no tener polo en 1, $(z - 1)$ no reduce el grado, sino que se suma completamente y, al tener igual grado en numerador y denominador para f_n , el grado de g_n es el grado del numerador.

Por Lema 2.2.1 y Lema 2.2.2 tenemos que $\deg(g_n) \sim \frac{c}{d}an^2$. Así, la secuencia de los grados forma una secuencia de crecimiento cuadrático.

Por último, tenemos que $\deg(g_n) \equiv a \deg(f_n) + k \equiv k \pmod{a}$.

Por lo tanto, D_a^k cumple con todo lo pedido. □

Capítulo 3

Grado 1

En este capítulo vamos a ver los casos en que A_G es diofantino o no diofantino para $\deg G = 1$. El resultado es el siguiente.

Teorema 3.0.1. *Sea $G \in \mathbb{Q}[x, y]$ de grado 1.*

Escribimos $G(x, y) = ax + by + c$; con $a, b, c \in \mathbb{Q}$ tales que $a \neq 0$ ó $b \neq 0$. Así,

1. *Si $b = 0$ ó $a = 0$ entonces A_G es diofantino.*

Consideremos ahora $a \neq 0$ y $b \neq 0$.

2. *Sea $c = 0$.*

a) *Si $-\frac{b}{a} < 0$ entonces A_G es diofantino.*

b) *Si $-\frac{b}{a} > 0$ entonces A_G es no diofantino.*

3. *Sea $c \neq 0$.*

a) *Si $-\frac{c}{b} < 0$ entonces A_G es diofantino.*

b) *Si $-\frac{c}{b} > 0$, se tiene que A_G es no diofantino si y solo si $bk + c \equiv 0 \pmod{a}$ tiene solución $k \in \{0, \dots, a-1\}$.*

Vamos a ver cada caso por separado. Fijamos $G(x, y) \in \mathbb{Q}[x, y]$, $G(x, y) = ax + by + c$.

Lema 3.0.2. *Si $b = 0$, entonces A_G es diofantino.*

Demostración. Con $b = 0$ tenemos que $G(x, y) = ax + c$. Luego, notemos que

$$G(\deg f, \deg g) = 0 \Rightarrow \deg f = -\frac{c}{a}.$$

Como $\deg f$ es natural, si $-\frac{c}{a} \notin \mathbb{N}$ entonces $A_G = \emptyset$, y por ende es diofantino (Lema 1.1.3). Por otro lado, si $-\frac{c}{a} = n \in \mathbb{N}$ entonces g puede ser cualquier elemento de $\mathbb{C}(z)$ (pues su grado queda libre) y

$$f = \frac{c_n z^n + \dots + c_0}{d_n z^n + \dots + d_0},$$

sin factores comunes entre numerador y denominador, y con $c_n \neq 0$ ó $d_n \neq 0$. Entonces, considerando $n = -\frac{c}{a}$, tenemos lo siguiente

$$\begin{aligned} A_G &= \{(f, g) \in \mathbb{C}(z) \mid G(\deg f, \deg g) = 0\} \\ &= \{(f, g) \in \mathbb{C}(z) \mid \exists c_n, \dots, c_0, d_n, \dots, d_0 \in \mathbb{C} \left(((d_n z^n + \dots + d_0)f = c_n z^n + \dots + c_0) \wedge \right. \\ &\quad \left. \wedge (\text{res}(d_n z^n + \dots + d_0, c_n z^n + \dots + c_0) \neq 0) \wedge (c_n \neq 0 \vee d_n \neq 0) \right)\}, \end{aligned}$$

el cual es diofantino por Lema 1.1.8, Lema 1.1.9 y por Lema 1.2.5. \square

De aquí en adelante, dentro de este capítulo, vamos a considerar para todos los lemas que $a \neq 0$ y $b \neq 0$.

Además, notemos que basta con considerar $a, b, c \in \mathbb{Z}$. Esto pues podemos escribir los coeficientes con la Notación 2.1.4, obteniendo $a = \frac{p_a}{q_a}, b = \frac{p_b}{q_b}, c = \frac{p_c}{q_c}$, y de ahí que

$$\frac{p_a}{q_a} \deg f + \frac{p_b}{q_b} \deg g + \frac{p_c}{q_c} = 0 \Leftrightarrow p_a q_b q_c \deg f + p_b q_a q_c \deg g + p_c q_a q_b = 0.$$

Por ende, basta con ver el caso en que $a, b, c \in \mathbb{Z}$ con $(a, b, c) = 1$, pues las soluciones no cambian al simplificar la ecuación.

Para los Lemas 3.0.3, 3.0.4, 3.0.5 y 3.0.6 vamos a considerar sin pérdida de generalidad que $a > 0$.

Lema 3.0.3. *Si $c = 0$ y $-\frac{b}{a} < 0$ entonces A_G es diofantino.*

Demostración. Con $c = 0$ tenemos que $G(x, y) = ax + by = 0$ y así,

$$G(\deg f, \deg g) = 0 \Rightarrow a \deg f + b \deg g = 0 \Rightarrow \deg f = -\frac{b}{a} \deg g.$$

Dado esto, como $\deg f, \deg g$ son naturales y $-\frac{b}{a} < 0$, no puede existir una solución natural. Por ende, $A_G = \emptyset$ que es diofantino por Lema 1.1.3. \square

Lema 3.0.4. *Si $c = 0$ y $-\frac{b}{a} > 0$ entonces A_G es no diofantino.*

Demostración. Sea $c = 0$ y $-\frac{b}{a} > 0$. Supongamos por contradicción que A_G es diofantino. Sean, sin pérdida de generalidad, $a > 0$ y $b < 0$. Sea D como en Teorema 1.6.4 (diofantino y con los grados de sus elementos formando una secuencia de crecimiento cuadrático) y definimos D^a para el coeficiente a como

$$D^a = \{g \in \mathbb{C}(z) : \exists h \in D, g = h^a\},$$

el cual es diofantino pues D lo es y, como $a > 0$ está fijo, la potencia también lo es.

Sea $D' = \{f \in \mathbb{C}(z) : \exists g \in D^a, a \deg f + b \deg g = 0\}$, el cual es diofantino (pues D^a y G son diofantinos).

Como $a \mid \deg g$ para $g \in D^a$, escribiendo $\deg g = ak$ ($k = \deg h$ para $h \in D$), tenemos que $D' = \{f \in \mathbb{C}(z) : \deg f = -bk\}$. Así, como el crecimiento de k es al menos cuadrático, entonces el crecimiento de $\deg f$, con $f \in D'$, también es al menos cuadrático. Por Lema 2.1.8 tenemos que $\text{ddim}(D') < \infty$.

Pero, por otro lado, como $a \mid \deg g$ tenemos que $\{\deg f : f \in D'\}$ es un subconjunto infinito de \mathbb{N} , por lo que $\dim(D') = \infty$ usando el Lema 2.1.7. Esto es una contradicción.

Por ende, si $-\frac{b}{a} > 0$ entonces $A_G = \{(f, g) \in \mathbb{C}(z)^2 : a \deg f + b \deg g = 0\}$ es no diofantino. \square

Lema 3.0.5. *Si $c \neq 0$ y $-\frac{a}{b} < 0$ entonces A_G es diofantino.*

Demostración. Supongamos, sin pérdida de generalidad, que $a, b > 0$.

Si $-c < 0$ entonces $G(x, y) = 0$ determina una recta de pendiente negativa y coeficiente de posición negativo, es decir, no existen soluciones naturales para $G(x, y) = 0$. Por lo que $A_G = \emptyset$, que es diofantino por el Lema 1.1.3.

Si $-c \geq 0$ sólo hay finitos naturales m para los cuales (m, n) podría ser solución natural de $G(x, y) = 0$. Así, para cada $m \in \{m \in \mathbb{N} : 0 \leq m \leq -\frac{c}{a}\}$ hay que ver si $y = \frac{-am-c}{b} \in \mathbb{N}$ o no. Si no tenemos soluciones naturales por, Lema 1.1.3, se concluye que A_G es diofantino y si tenemos (como serían finitas), por Lema 2.1.3, se concluye que A_G es diofantino. Por lo tanto; si $-\frac{a}{b} < 0$ y $c \neq 0$, entonces A_G es diofantino. \square

Lema 3.0.6. *Si $c \neq 0$ y $-\frac{a}{b} > 0$, se tiene que A_G es no diofantino si y solo si $bk+c \equiv 0 \pmod{a}$ tiene solución $k \in \{0, \dots, a-1\}$.*

Demostración. Si $bk+c \equiv 0 \pmod{a}$ no tiene solución, entonces no tenemos soluciones naturales para $G(x, y) = 0$ y por 1.1.3 se deduce que A_G es diofantino.

Si $bk+c \equiv 0 \pmod{a}$ tiene solución, vamos a razonar por contradicción. Supongamos que para $c \neq 0$ y $-\frac{a}{b} > 0$, el conjunto A_G es diofantino. Supongamos, sin pérdida de generalidad, que $a > 0$ y $b < 0$. Sea $k \in \{0, \dots, a-1\}$ tal que $bk+c \equiv 0 \pmod{a}$. Sea D_a^k como en el Lema 2.2.5. Definimos

$$D' = \{f \in \mathbb{C}(z) : \exists g \in D_a^k, a \deg f + b \deg g + c = 0\},$$

que es diofantino pues A_G y D_a^k lo son.

Por un lado, como $\deg g$, con $g \in D_a^k$, crece al menos cuadráticamente, entonces $\deg f$, con $f \in D'$, crece al menos cuadráticamente. Así, por Lema 2.1.8, tenemos que $\dim(D') < \infty$. Por otro lado, como $|\{\deg g : g \in D_a^k\}| = \infty$, tenemos que $|\{\deg f : f \in D'\}| = \infty$, ya que por cada $g \in D_a^k$ se tiene un $f \in D'$. Así, por Lema 2.1.7, tenemos que $\dim(D') = \infty$. Esto es una contradicción.

Por lo tanto; si $-\frac{a}{b} > 0$, entonces $A_G = \{(f, g) \in \mathbb{C}(z)^2 : a \deg f + b \deg g + c = 0\}$ no es diofantino. \square

Juntando los lemas de este capítulo tenemos la demostración del teorema 3.0.1.

DEMOSTRACIÓN DEL TEOREMA 3.0.1. Consideremos $G \in \mathbb{Q}[x, y]$ de grado 1, escrito $G(x, y) = ax + by + c$; con $a, b, c \in \mathbb{Q}$ tales que $a \neq 0$ ó $b \neq 0$. Vamos punto por punto.

1. Por el lema 3.0.2 tenemos el caso $b = 0$. Si $a = 0$ se obtiene el mismo resultado que en el lema 3.0.2, considerando $f \in \mathbb{C}(z)$ y $g = \frac{cnz^n + \dots + c_0}{d_n z^n + \dots + d_0}$ (es el mismo razonamiento pues no se utiliza de forma significativa si la variable es x o y).
2. El caso (a) es por el lema 3.0.3 y el caso (b) es por el lema 3.0.4.

3. El caso (a) es por el lema 3.0.5 y el caso (b) es por el lema 3.0.6

□

Capítulo 4

Grado 2

En esta sección demostraremos para cuáles $G(x, y) \in \mathbb{Q}[x, y]$ de grado 2 nuestro conjunto A_G es diofantino o es no diofantino. El teorema de esta sección es el siguiente.

Teorema 4.0.1. *Sea $G(x, y) \in \mathbb{Q}[x, y]$ de grado 2. Escribimos $G(x, y) = a_5x^2 + a_4xy + a_3y^2 + a_2x + a_1y + a_0$ con $a_i \in \mathbb{Q}$ y a_5, a_4, a_3 no todos cero. Tenemos que*

1. *Si $G(x, y) = 0$ tiene a lo más finitas soluciones naturales o si las infinitas soluciones están dadas por una coordenada fija y la otra libre, entonces A_G es diofantino.*
2. *Si $G(x, y) = 0$ tiene infinitas soluciones naturales entonces A_G es no diofantino.*

Separaremos también esta demostración en casos. Los casos que analizaremos estarán determinados por la cónica que define $G(x, y) = 0$. Para esto, recordamos la clasificación de las cónicas que dice que $G(x, y) = 0$ puede definir vacío, un punto, una recta, dos rectas, una elipse, una parábola o una hipérbola. En cada caso veremos si $G(x, y) = 0$ tiene a lo más finitas o infinitas soluciones naturales y en el caso de infinitas soluciones naturales, llegaremos a la conclusión de que es no diofantino.

Lema 4.0.2. *Si $G(x, y) = 0$ define vacío o un punto tenemos que A_G es diofantino.*

Demostración. Sabemos que el vacío es diofantino por Lema 1.1.3 y si $G(x, y) = 0$ define solo un punto, por el lema 2.1.3 tenemos que también es diofantino. \square

Lema 4.0.3. *Si $G(x, y) = 0$ define una recta o dos rectas tenemos dos casos.*

1. *Si $G(x, y) = 0$ tiene a lo más finitas soluciones naturales o si las infinitas soluciones están dadas por una coordenada fija y la otra libre entonces A_G es diofantino.*
2. *Si $G(x, y) = 0$ tiene infinitas soluciones naturales entonces A_G es no diofantino.*

Demostración. Notemos que si $G(x, y) = 0$ define una recta, el análisis es el mismo que ya se realizó en el Teorema 3.0.1. Por lo que se concluyen 1 y 2 en este caso.

Mientras que si $G(x, y) = 0$ define dos rectas tenemos que; si $L_1(x, y) = 0, L_2(x, y) = 0$ determinan a estas rectas, entonces

$$A_G = \{(f, g) \in \mathbb{C}(x, y) : L_1(\deg f, \deg g) = 0\} \cup \{(f, g) \in \mathbb{C}(x, y) : L_2(\deg f, \deg g) = 0\}.$$

Así, si ambas rectas tienen a lo más finitas soluciones naturales se concluye, por Lema 1.1.5, que A_G es diofantino. Si alguna de las dos rectas contiene infinitas soluciones naturales, entonces se puede realizar el mismo esquema de demostración que en el capítulo anterior (ver Lemas 3.0.4 y 3.0.6), llegando a una contradicción con Lema 2.1.7 y Lema 2.1.8. \square

Lema 4.0.4. *Si $G(x, y) = 0$ define una elipse entonces A_G es diofantino.*

Demostración. Sea C el conjunto de puntos de la elipse en \mathbb{R}^2 . Como existen $M, N \in \mathbb{N}$ tales que para todo $(x, y) \in C, |x| < M$ y $|y| < N$, tenemos que las soluciones naturales de G son finitas pues deben cumplir estas desigualdades. Así, por Lema 2.1.3 se concluye que A_G es diofantino. \square

Recordemos que en las parábolas solamente tenemos un elemento de segundo grado, que puede ser a_5x^2 o a_3y^2 . Luego, podemos reescribir, en este caso, las ecuaciones $G(x, y) = 0$ del siguiente modo:

$$a_5x^2 + a_2x + a_1y + a_0 = 0 \Rightarrow y = -\frac{a_5}{a_1}x^2 - \frac{a_2}{a_1}x - \frac{a_0}{a_1}.$$

$$a_3y^2 + a_2x + a_1y + a_0 = 0 \Rightarrow -\frac{a_3}{a_2}y^2 - \frac{a_1}{a_2}y - \frac{a_0}{a_2}.$$

Luego, si $G(x, y) = 0$ define una parábola, escribimos $y = ax^2 + bx + c$ o $x = ay^2 + by + c$, donde $a, b, c \in \mathbb{Q}$. A partir de aquí utilizamos la Notación 2.1.4.

Lema 4.0.5. *Si $G(x, y) = 0$ determina una parábola tenemos que*

1. *Si $a < 0$ entonces A_G es diofantino.*
2. *Si $a > 0$ tenemos los siguientes casos:*
 - a) *Si $c \in \mathbb{Z}$ entonces A_G es no diofantino.*
 - b) *Si $c \in \mathbb{Q} - \mathbb{Z}, (q_a, q_c) = 1, (q_b, q_c) = 1$ entonces A_G es diofantino.*

Demostración. Sea $G(x, y) = 0$ tal que determina una parábola.

1. Si $a < 0$, las posibles soluciones naturales de $G(x, y) = 0$ son a lo más finitas por la concavidad de la parábola (las ramas se abren en los cuadrantes II, III y IV). Así, por el Lema 2.1.3 tenemos que A_G es diofantino.
2. Sea $a > 0$. Vamos a analizar $y = ax^2 + bx + c$, pues el otro caso es análogo. Luego,

- a) Sea $c \in \mathbb{Z}$ y supongamos por contradicción que A_G es diofantino. Sea $\lambda = q_a q_b$. Sea D como en Teorema 1.6.4, que es diofantino y los grados de sus elementos forman una secuencia de crecimiento cuadrático. Definimos $D^\lambda = \{g \in \mathbb{C}(z) : \exists h \in D, g = h^\lambda\}$. Así, D^λ es diofantino (pues D lo es y tomar potencia también) donde $\{\deg g : g \in D^\lambda\}$ es una secuencia de crecimiento al menos cuadrático. Definimos

$$D' = \{f \in \mathbb{C}(z) : \exists g \in D^\lambda, G(\deg g, \deg f) = 0\},$$

el cual es diofantino, pues D^λ y G lo son.

Luego, $\{\deg f : f \in D'\}$ crece al menos como n^4 . Se concluye que $\text{ddim}(D') < \infty$ por Lema 2.1.8.

Por otro lado, notemos que para cada $f \in D'$ tenemos que

$$\deg f = a(\lambda \deg h)^2 + b\lambda \deg h + c,$$

con $h \in D$. Sea $k = \deg h$ y entonces

$$\deg f = \frac{p_a}{q_a} \lambda^2 k^2 + \frac{p_b}{q_b} \lambda k + c = p_a q_a q_b^2 k^2 + p_b q_a k + c \in \mathbb{Z}.$$

Como $\{\deg h : h \in D\}$ crece cuadráticamente; tenemos que existe $k_0 \in \mathbb{N}$ tal que, para todos los $k \geq k_0$ con $k \in \{\deg h : h \in D\}$, se tiene que $\deg f \in \mathbb{N}$. Luego, tenemos infinitos valores naturales para $\deg f$. Por ende, $\text{ddim}(D') = \infty$ por Lema 2.1.7.

Esto es una contradicción, por lo tanto, A_G es no diofantino.

- b) Notemos que en este caso, si (m, n) es solución natural de $G(x, y) = 0$ entonces

$$\frac{p_a}{q_a} m^2 + \frac{p_b}{q_b} m + \frac{p_c}{q_c} = \frac{p_a q_b q_c m^2 + p_b q_a q_c m + p_c q_a q_b}{q_a q_b q_c} = n \in \mathbb{N}.$$

Tenemos dos casos en los que se cumple lo anterior;

$$q_a q_b q_c | p_a q_b q_c m^2 + p_b q_a q_c m + p_c q_a q_b \quad \text{ó} \quad p_a q_b q_c m^2 + p_b q_a q_c m + p_c q_a q_b = 0.$$

Por la transitividad de la divisibilidad tenemos que

$$q_c | p_a q_b q_c m^2 + p_b q_a q_c m + p_c q_a q_b.$$

Pero, $q_c | p_a q_b q_c m^2 + p_b q_a q_c m$ y $q_c \nmid p_c q_a q_b$, lo cual es una contradicción.

Como a partir de $p_a q_b q_c m^2 + p_b q_a q_c m + p_c q_a q_b = 0$ tenemos a lo más dos soluciones para $m \in \mathbb{N}$, se deduce que $G(x, y) = 0$ tiene a lo más finitas soluciones naturales.

Por lo tanto A_G es diofantino Por los Lemas 1.1.3 y 2.1.3.

□

El resto de casos de la parábola se subdividen en pequeños casos según si ecuaciones en congruencia (de primer y segundo grado) o sistemas de ecuaciones en congruencias tienen solución. En el capítulo 5 se desarrollan algunos ejemplos para mostrar el proceso, cómo surgen los diversos casos y por qué podemos afirmar que las infinitas soluciones cumplen con una condición de congruencia $m \equiv k(a)$ como la del Lema 2.2.5.

Por ende, tenemos lo siguiente para el resto de casos de la parábola.

Lema 4.0.6. *Sea $G(x, y) = 0$ que define una parábola, con $a > 0$. Si tenemos $c \in \mathbb{Q} - \mathbb{Z}$, cumpliendo que $(q_a, q_c) \neq 1, (q_b, q_c) = 1$ ó $(q_a, q_c) = 1, (q_b, q_c) \neq 1$ ó $(q_a, q_c) \neq 1, (q_b, q_c) \neq 1$; entonces se dan los siguientes casos*

1. *Si $G(x, y) = 0$ tiene a lo más finitas soluciones naturales entonces A_G es diofantino.*
2. *Si $G(x, y) = 0$ tiene infinitas soluciones naturales entonces A_G es no diofantino.*

Demostración. El primer caso se deduce por el Lema 2.1.3.

Para el segundo caso, supongamos por contradicción que A_G es diofantino.

Las infinitas soluciones (m, n) cumplen con una condición de congruencia $m \equiv k \pmod{a}$ (esta afirmación se justifica en el capítulo 5). Sea D_a^k como en el Lema 2.2.5 (diofantino y los grados de D_a^k crecen de forma cuadrática) y definimos

$$D' = \{f \in \mathbb{C}(z) : \exists g \in D_a^k, G(\deg g, \deg f) = 0\},$$

el cual es diofantino, pues D_a^k y G lo son. Luego, $\{\deg f : f \in D_a^k\}$ crece al menos cuadráticamente, por lo que $ddim(D') < \infty$, por Lema 2.1.8.

Por otro lado, como son infinitas las duplas $(\deg f, \deg g)$ con coordenadas naturales, tenemos que $ddim(D') = \infty$, por Lema 2.1.7.

Esto es una contradicción, por lo tanto A_G es no diofantino. \square

El siguiente lema nos permite concluir la situación de A_G cuando $G(x, y) = 0$ representa una hipérbola. Las afirmaciones realizadas se justifican en el capítulo 5.

Lema 4.0.7. *Si $G(x, y) = 0$ define una hipérbola entonces tenemos dos casos.*

1. *Si $G(x, y) = 0$ tiene a lo más finitas soluciones naturales entonces A_G es diofantino.*
2. *Si $G(x, y) = 0$ tiene infinitas soluciones naturales entonces A_G es no diofantino.*

Demostración. Si tenemos a lo más finitas soluciones aplicamos el Lema 2.1.3 y concluimos que A_G es diofantino.

Vamos a considerar $G(x, y) = a_5x^2 + a_4xy + a_3y^2 + a_2x + a_1y + a_0$ con a_2, a_1, a_0 no todos nulos y con $a_5a_3 \leq 0$. En el capítulo 5 se justifica la razón de que en estas condiciones podemos tener infinitas soluciones.

Luego, tenemos los siguientes casos con la posibilidad de tener infinitas soluciones (justificado en el capítulo 5):

1. Sean $a_5 \neq 0$ y $a_3 \neq 0$. Supongamos por contradicción que A_G es diofantino. Sea D como en Teorema 1.6.4 (diofantino y con los grados formando una secuencia de crecimiento cuadrático). Definimos

$$D' = \{f \in \mathbb{C}(z) : \exists g \in D, G(\deg f, \deg g) = 0\},$$

el cual es diofantino pues D y A_G lo son.

Luego, como los grados de $g \in D$ crecen de forma cuadrática y a_5, a_3 son no nulos,

tenemos que $\{\deg f : f \in D'\}$ forman una secuencia infinita de naturales con crecimiento cuadrático (miramos los términos $a_5(\deg f)^2$, $a_3(\deg g)^2$ y $a_4 \deg f \deg g$ para llegar a esta conclusión). Por Lema 2.1.7, se deduce que $\text{ddim}(D') = \infty$ y por Lema 2.1.8 se deduce que $\text{ddim}(D') < \infty$. Esto es una contradicción, por lo tanto, A_G es no diofantino.

2. Sean $a_5 = 0$ ó $a_3 = 0$, pero no ambos. Sin pérdida de generalidad, consideremos $a_3 = 0$. Supongamos por contradicción que A_G es diofantino. Sea D como en Teorema 1.6.4 (diofantino y con los grados formando una secuencia de crecimiento cuadrático). Definimos

$$D' = \{f \in \mathbb{C}(z) : \exists g \in D, G(\deg f, \deg g) = 0\},$$

el cual es diofantino pues D y A_G lo son.

Como $\{\deg g : g \in D\}$ crece cuadráticamente y $(\deg f, \deg g)$ es solución natural para $G(x, y) = 0$, se deduce que $\{\deg f : f \in D'\}$ forman una secuencia infinita de naturales con crecimiento cuadrático (miramos los términos $a_5(\deg f)^2$ y $a_4 \deg f \deg g$ para llegar a esta conclusión). Por Lema 2.1.7, se deduce que $\text{ddim}(D') = \infty$ y por Lema 2.1.8 se deduce que $\text{ddim}(D') < \infty$. Esto es una contradicción, por lo tanto, A_G es no diofantino.

□

Juntando los lemas de este capítulo obtenemos la demostración del teorema 4.0.1.

DEMOSTRACIÓN DEL TEOREMA 4.0.1. Juntando los Lemas 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6 y 4.0.7 se concluye el Teorema. □

Capítulo 5

Comentarios finales

En este capítulo vamos a ver el desarrollo de los casos abreviados en capítulos anteriores y algunos ejemplos concretos.

5.1. Parábola

Veamos que los casos con infinitas soluciones cumplen con condiciones de congruencia. Esto para el Lema 4.0.6.

Sea $G(x, y) = 0$ que representa una parábola de la forma $y = ax^2 + bx + c$, con $a > 0$, y usamos la Notación 2.1.4.

1. Sea $(q_a, q_c) \neq 1$ y $(q_b, q_c) \neq 1$.

Sea (m, n) tal que $G(m, n) = 0$. Vamos a analizar esta situación y exponer los casos en los que se tienen a lo más finitas soluciones y en los que se tienen infinitas soluciones (y cómo surge la afirmación de que las infinitas soluciones cumplen con una condición de congruencia).

Supongamos primero que $q_c = \lambda$ es primo. Luego, por nuestra suposición, tenemos que $q_a = \lambda q'_a$, $q_b = \lambda q'_b$. Luego,

$$n = \frac{p_a}{\lambda q'_a} m^2 + \frac{p_b}{\lambda q'_b} m + \frac{p_c}{\lambda} = \frac{p_a q'_b m^2 + p_b q'_a m + p_c q'_a q'_b}{\lambda q'_a q'_b}.$$

Como queremos que el lado derecho sea natural (pues $n \in \mathbb{N}$) existen dos casos; que el numerador sea cero (son a lo más dos valores para m , así que nos centraremos en el segundo caso) o que el denominador divida al numerador. En este segundo caso, denotando por $Num = p_a q'_b m^2 + p_b q'_a m + p_c q'_a q'_b$, por la transitividad de la divisibilidad tenemos que

- $q'_a | Num \Rightarrow q'_a | p_a q'_b m^2 \Rightarrow q'_a | q'_b m^2$, por la coprimalidad de la representación fraccionaria que estamos usando ($(q_a, p_a) = 1 \Rightarrow (q'_a, p_a) = 1$).
- $q'_b | Num \Rightarrow q'_b | p_b q'_a m \Rightarrow q'_b | q'_a m$, por la coprimalidad de la representación fraccionaria que estamos usando ($(q_b, p_b) = 1 \Rightarrow (q'_b, p_b) = 1$).

- $\lambda | Num.$

De la primera afirmación obtenemos dos casos; $q'_a | q'_b$ o $q'_a | m$. De la segunda afirmación tenemos los casos $q'_b | q'_a$ o $q'_b | m$. Esto nos da diversas combinaciones de casos posibles. Veamos primero el caso $q'_a | m, q'_b | m$ por lo que tenemos $m = q'_a q'_b \tilde{m}$. Luego, con esta reescritura tenemos que

$$n = \frac{p_a q'_a (q'_b)^2 (\tilde{m})^2 + p_b q'_a \tilde{m} + p_c}{\lambda}.$$

Como \tilde{m} está elevada al cuadrado podemos pedir que sea suficientemente grande de modo que n sea positivo ($a > 0$ implica que $p_a > 0$). Renombrando $A = p_a q'_a (q'_b)^2, B = p_b q'_a, C = p_c$, lo que queremos son las soluciones de

$$A\tilde{m}^2 + B\tilde{m} + C \equiv (\lambda).$$

Si existe solución, entonces tenemos infinitos valores con las condiciones que queremos (se obtiene una expresión con congruencias). Si no existe solución, entonces A_G sería diofantino por Lema 1.1.3.

El resto de casos es similar, pues se llega a una ecuación en congruencias de segundo grado (o como mucho un sistema de una ecuación de este tipo con otra en congruencia lineal) que si tiene solución nos da no diofantino y sin solución sería diofantino. En cada caso las condiciones de divisibilidad nos permiten cambiar los valores concretos de A, B, C .

Si q_c es compuesto tenemos que hacer el mismo proceso de plantear una fracción única (teniendo cuidado de desgranar las cantidades para que el denominador sea lo más cercano posible al mínimo común múltiplo) y usar propiedades de divisibilidad para llegar a ecuaciones en congruencias que, según si tiene o no soluciones, nos permitirán determinar si A_G es diofantino o no diofantino.

Veamos un par de ejemplos.

2. Sea $G(x, y) = \frac{1}{20}x^2 + \frac{5}{26}x + \frac{3}{10} - y$. Luego, si suponemos que $(m, n) \in \mathbb{N}$ cumple que $G(m, n) = 0$ tenemos que

$$n = \frac{13m^2 + 50m + 78}{260}.$$

Aplicando la fórmula para la ecuación cuadrática se verifica que no se puede tener $G(m, 0) = 0$ para $m \in \mathbb{N}$. Por divisibilidad, denotando $NUM = 13m^2 + 50m + 78$,

- $2 | NUM \Rightarrow 2 | 13m^2 \Rightarrow 2 | m$.
- $5 | NUM \Rightarrow 5 | 13m^2 + 78$. Luego,

$$13m^2 + 78 \equiv 0 \pmod{5} \quad (5)$$

$$3m^2 + 3 \equiv 0 \pmod{5} \quad (5)$$

$$m^2 \equiv -1 \pmod{5} \quad (5)$$

$$m^2 \equiv 4 \pmod{5} \quad (5)$$

$$m \equiv 2 \pmod{5} \vee m \equiv 3 \pmod{5}.$$

- $13 \mid NUM \Rightarrow 13 \mid 50m \Rightarrow 13 \mid m$.

Notemos que con las condiciones $2 \mid m, 13 \mid m$ se deduce que $26 \mid m$ y podemos escribir $m = 26k$, de donde deducimos

$$\frac{13 \cdot 676k^2 + 50 \cdot 26k + 78}{260} = \frac{13 \cdot 26k^2 + 50k + 3}{10}.$$

Así, $2 \mid 13 \cdot 26k^2 + 50k + 3 \Rightarrow 2 \mid 3$ lo cual no es posible. Por ende, no existen $(m, n) \in \mathbb{N}^2$ tales que $G(m, n) = 0$.

Otro modo de llegar a la misma conclusión es observando que, como $4 \mid 260$, tenemos que $4 \mid NUM$. Usando que $2 \mid m$, se deduce que $4 \mid 50m + 78$ y de ahí que $2 \mid 25m + 39$ lo cual no es posible dado que m es par.

Por lo tanto A_G es diofantino.

3. Sea $G(x, y) = \frac{1}{6}x^2 + \frac{3}{5}x + \frac{2}{15} - y$ y queremos soluciones $(m, n) \in \mathbb{N}^2$. Si consideramos $m \equiv 22 \pmod{30}$, escribiendo $m = 30k + 22$ se tiene que

$$n := \frac{4500k^2 + 7140k + 2820}{30} = 150k^2 + 238k + 94.$$

Con esto se verifica que existen infinitas soluciones cumpliendo $G(m, n) = 0$ y que m tiene una condición de congruencia. Así, usando Lema 2.2.5 se llega a una contradicción asumiendo que A_G es diofantino. Por lo tanto, A_G es no diofantino.

Ahora bien, para llegar a esta condición aplicamos el mismo proceso que en el ejemplo anterior:

$$n = \frac{5m^2 + 18m + 4}{30}.$$

Sea $NUM = 5m^2 + 18m + 4$. Luego,

- $2 \mid NUM \Rightarrow 2 \mid 5m^2 \Rightarrow 2 \mid m$.
- $3 \mid NUM \Rightarrow 3 \mid 5m^2 + 4$.
- $5 \mid NUM \Rightarrow 5 \mid 18m + 4$.

De donde obtenemos los siguientes sistemas

$$\left(\begin{array}{l} m \equiv 0 \pmod{2} \\ m \equiv 1 \pmod{3} \\ m \equiv 2 \pmod{5} \end{array} \right) \vee \left(\begin{array}{l} m \equiv 0 \pmod{2} \\ m \equiv 2 \pmod{3} \\ m \equiv 2 \pmod{5} \end{array} \right).$$

La solución del primero es $m \equiv 22 \pmod{30}$.

4. Queremos $(m, n) \in \mathbb{N}^2$ solución natural. Sea $(q_a, q_c) \neq 1, (q_b, q_c) = 1$ y consideremos $q_c = \lambda$ primo. Luego, $q_a = \lambda q'_a$ y tendríamos

$$n = \frac{p_a q_b m^2 + p_b q_a m + p_c q'_a q_b}{\lambda q'_a q_b},$$

de donde se deduce (por divisibilidad) que

- $q_b \mid q'_a m$.
- $q'_a \mid q_b m^2$.
- $\lambda \mid p_a q_b m^2 + p_c q'_a q_b$, y usando que $(\lambda, q_b) = 1$ tenemos que $\lambda \mid p_a m^2 + p_c q'_a$.

Del mismo modo que antes se forman diversos subcasos en el que cada uno nos entrega distintas condiciones de congruencias y según los coeficientes se tendrán o no soluciones. Por ejemplo, si tenemos $q'_a \mid m$, $q_b \mid m$ y $(q'_a, q_b) = 1$, podemos escribir $m = q'_a q_b k$ y obtenemos

$$n = \frac{p_a q'_a q_b^2 k^2 + p_c}{\lambda} + p_b q'_a k.$$

Deducimos que $p_a q'_a q_b^2 k^2 + p_c \equiv 0 \pmod{\lambda}$. Si esta ecuación no tiene soluciones tendremos A_G diofantino; y si tiene solución (solución en congruencia nos da infinitas parejas (m, n)) tendremos A_G no diofantino.

5. Sea $(q_a, q_c) = 1$, $(q_b, q_c) \neq 1$ y sea $q_c = \lambda$ primo. Luego,

$$n = \frac{p_a}{q_a} m^2 + \frac{p_b}{\lambda q'_b} m + \frac{p_c}{\lambda} = \frac{p_a \lambda q'_b m^2 + p_b q_a m + p_c q_a q'_b}{\lambda q_a q'_b}.$$

Por divisibilidad, denotando $NUM = p_a \lambda q'_b m^2 + p_b q_a m + p_c q_a q'_b$, tenemos que

- $q_a \mid NUM \Rightarrow q_a \mid p_a \lambda q'_b m^2 \Rightarrow q_a \mid \lambda q'_b m^2$.
- $q'_b \mid NUM \Rightarrow q'_b \mid p_b q_a m \Rightarrow q'_b \mid q_a m$.
- $\lambda \mid NUM \Rightarrow \lambda \mid p_b q_a m + p_c q_a q'_b \Rightarrow \lambda \mid p_b m + p_c q'_b$.

Nuevamente se pueden tener diversos casos.

Si tenemos que $q_a \mid m$, $q'_b \mid m$, se obtiene el sistema

$$\left(\begin{array}{l} m \equiv 0 \pmod{q_a} \\ m \equiv 0 \pmod{q'_b} \\ p_b m + p_c q'_b \equiv 0 \pmod{\lambda} \end{array} \right).$$

Si q_a, q'_b, λ son coprimos de a pares, por el teorema chino del resto tenemos solución para este sistema del tipo $m \equiv a \pmod{q_a q'_b \lambda}$, es decir, A_G sería no diofantino.

Ahora bien, si $(q'_b, \lambda) \neq 1$ como $(q'_b, p_b) = 1$ se deduce que $\lambda \nmid p_b$, y así, $\lambda \nmid m$ por la tercera ecuación. Luego, tenemos que $q_a \lambda \mid m$ por lo que, escribiendo $m = q_a \lambda k$ y $q'_b = \lambda q''_b$,

$$n = p_a q_a \lambda^2 k^2 + \frac{p_b q_a \lambda k + p_c q'_b}{q'_b \lambda} = p_a q_a \lambda^2 k^2 + \frac{p_b q_a k + p_c q''_b}{q'_b}.$$

De ahí que para tener una solución natural queremos que $q'_b \mid p_b q_a k + p_c q''_b$. Luego, sabemos que $p_b q_a k + p_c q''_b \equiv 0 \pmod{q'_b}$ si y solo si $d := (p_b q_a, q'_b) \mid p_c q''_b$. Recordemos que $(p_b, q'_b) = 1$, $(q_a, \lambda) = 1$, por lo que $d = (q_a, q'_b)$, $d \neq \lambda$ y $d \mid q''_b$. Así, tenemos una solución en congruencia, lo que nos permite concluir que es no diofantino.

Con estos ejemplos se ilustra el método aplicable a todos los casos no escritos aquí.

5.2. Hipérbola

Sea $G(x, y) = a_5x^2 + a_4xy + a_3y^2 + a_2x + a_1y + a_0$.

Primero veamos las condiciones que debemos pedir a los coeficientes para que la expresión anterior sea una hipérbola.

1. Si $a_0 = a_1 = a_2 = 0$ y (m, n) es solución natural tenemos lo siguiente para $\mu \in \mathbb{N} - \{0\}$

$$a_5\mu^2m^2 + a_4\mu m\mu n + a_3\mu^2n^2 = 0 \Leftrightarrow a_5m^2 + a_4mn + a_3n^2 = 0.$$

Así (m, n) es solución natural si y solo si $(\mu m, \mu n)$ es solución natural. Por ende, con estos coeficientes tenemos dos rectas, una recta o vacío.

2. Si $a_5 \cdot a_3 > 0$ por argumento de crecimiento podemos deducir que las soluciones están acotadas, es decir, que el polinomio representa una elipse. Por ende, para que sea hipérbola pedimos $a_5 \cdot a_3 \leq 0$.

Luego, vamos a justificar (para el Lema 4.0.7) que se tienen infinitas soluciones solo cuando al menos uno de los coeficientes a_3 y a_5 es no nulo. En otras palabras, nos centramos en el caso $a_4xy + a_2x + a_1y + a_0$ y veremos que se obtienen a lo más finitas soluciones naturales o que no es hipérbola.

1. Sea $a_4xy + a_0 = 0$. Así, $xy = -\frac{a_0}{a_4}$. Si (m, n) es solución natural tenemos dos posibilidades
 - Si $-\frac{a_0}{a_4} \notin \mathbb{N}$ llegamos a una contradicción, pues multiplicación de naturales da natural.
 - Si $d := -\frac{a_0}{a_4} \in \mathbb{N}$, como d tiene finitos divisores, tenemos que solo finitas parejas (m, n) cumplen que $mn = d$. Así, tenemos a lo más finitas soluciones.

Así, en este caso tenemos a lo más finitas soluciones.

2. Si $a_4xy + a_2x = 0$ ó $a_4xy + a_1y = 0$ entonces $G(x, y) = 0$ representa dos rectas. Esto pues se pueden factorizar obteniendo $x(a_4y + a_2) = 0$ ó $y(a_4x + a_1) = 0$ en cada caso.
3. Si $a_5 = a_3 = 0$ y a_2, a_1, a_0 con al menos dos no nulos y tomamos (m, n) solución natural tenemos que

$$a_4mn + a_2m + a_1n + a_0 = 0 \Rightarrow n = -\frac{a_2m + a_0}{a_4m + a_1}.$$

Para tener infinitas soluciones es necesario que $a_4m + a_1 \mid a_2m + a_0$ para infinitos valores de m , pero si esto ocurre tenemos que $a_2m + a_0 = k(a_4m + a_1)$ de donde se deduce que

$$a_4mn + a_2m + a_1n + a_0 = 0 \Rightarrow (a_4m + a_1)y + k(a_4m + a_1) = 0 \Rightarrow (a_4m + a_1)(y + k) = 0.$$

Así, tendríamos dos rectas.

Finalmente, veamos un par de casos explícitos.

1. Sea $G(x, y) = xy + x + 2y + 5 = 0$ y notemos que $y = -\frac{x+5}{x+2}$. Luego, si queremos evaluar x por naturales tenemos que $y < 0$, por lo que no tenemos soluciones naturales.
2. Sea $G(x, y) = x^2 - y^2 + x + y + 1 = 0$. Si (a, b) es solución para $G = 0$ tenemos que

$$a^2 - b^2 + a + b + 1 = 0 \Leftrightarrow (a + b)(a - b) + a + b = -1 \Leftrightarrow (a + b)(a - b + 1) = -1.$$

Si queremos tener una solución natural, en particular por ser enteros, tenemos que $a + b = \pm 1$ y $a - b + 1 = \mp 1$.

- Si $a + b = 1$ tenemos que $(a = 0 \wedge b = 1) \vee (a = 1 \wedge b = 0)$. En el primer caso, $a - b + 1 = 0$ y en el segundo $a - b + 1 = 2$, es decir, se llega a una contradicción.
- Si $a + b = -1$ entonces alguno de los dos no es natural.

Por ende, no existen soluciones naturales para $G = 0$.

3. Sea $G(x, y) = x^2 - 2y^2 - 1$. Tenemos que $G(x, y) = 0$ nos da la siguiente ecuación de Pell, $x^2 - 2y^2 = 1$. Luego, sabemos que esta ecuación tiene infinitas soluciones naturales (x_n, y_n) dadas por la siguiente expresión $x_n + \sqrt{2}y_n = (3 + 2\sqrt{2})^n$. Se puede ver en detalle en [11].

5.3. Conjetura

Explicuemos la siguiente conjetura.

Conjetura 5.1. *Dado $G(x, y) \in \mathbb{C}[x, y]$ se tiene que*

- a) *Si $G(x, y) = 0$ tiene a lo más finitas soluciones o si las infinitas soluciones están dadas por una coordenada fija y la otra libre, entonces A_G es diofantino.*
- b) *En otro caso, A_G es no diofantino.*

Dado un $G(x, y) \in \mathbb{C}[x, y]$, por lo comentado en el capítulo 2 sección 1 a partir de la Definición 2.1.5, podemos quedarnos con los $G_{q_i}(x, y) \in \mathbb{Q}[x, y]$ como en la Definición 2.1.5. Luego, en los casos de $G(x, y) \in \mathbb{Q}[x, y]$ de grado 1 ó 2 tenemos lo conversado en los capítulos 3 y 4. Así, esta conjetura afecta los casos donde $\deg G \geq 3$ y $G(x, y) = 0$ tiene infinitas soluciones naturales.

Como los grados son números naturales y estamos analizando la situación $G(\deg f, \deg g) = 0$ los crecimientos de estos grados están relacionados, excepto en el caso que las soluciones sean como en el Lema 3.0.2.

Por ejemplo, si tenemos $G(x, y) = x^5 + 3x^4 - x$ las soluciones para $G(x, y) = 0$ son del tipo (x_i, \star) , donde x_i es solución de $x^5 + 3x^4 - x = 0$ y la segunda coordenada es libre. Así, estas infinitas soluciones son como las del Lema 3.0.2 y se pueden describir de forma diofantina.

En cambio, si tenemos $G(x, y) = x^4 - y^3$, existe una relación entre el crecimiento de las posibles soluciones naturales (m, n) dado por $m \sim n^{\frac{3}{4}}$.

Así, si no se cumple la condición del Lema 3.0.2, entonces el siguiente esquema; que generaliza lo realizado en los capítulos anteriores; nos permitiría probar que es no diofantino:

- a) Suponer por contradicción que A_G es diofantino.
- b) Identificar en la relación de crecimiento cuál de las dos coordenadas crece más lento.
- c) Describir de forma diofantina los infinitos valores de la coordenada que crece lento exigiendo un crecimiento cuadrático (o mayor que lineal).
- d) Definir el valor de la otra coordenada con lo anterior (será diofantina).
- e) Por ser infinitas soluciones tenemos $\text{ddim} = \infty$. Por crecimiento al menos cuadrático tenemos $\text{ddim} < \infty$.

El punto *c* es la parte delicada. En esta tesis se utilizaron tres conjuntos diofantinos de este tipo: el dado en [5] que está aquí en el Lema 1.6.4, el D^a para D como en el Lema 1.6.4 y el dado en el Lema 2.2.5. Desconozco si puede aparecer un nuevo tipo necesario en grados superiores, pero si con estos tres es suficiente, entonces la conjetura es cierta.

Bibliografía

- [1] David Cox, John Little y Donal O’Shea. *Ideals, Varieties and Algorithms*. Springer, 2007.
- [2] Martin Davis. “Hilbert’s Tenth Problem is Unsolvable”. En: *American Mathematical Monthly* 80 3 (1973), págs. 233-269.
- [3] Jeroen Demeyer. “Diophantine sets of polynomials over number fields”. En: *Proc. Amer. Math. Soc.* 138 8 (2010), págs. 2715-2728.
- [4] Jan Denef. “The Diophantine Problem for Polynomial Rings and Fields of Rational Functions”. En: *Trans. Amer. Math. Soc.* 242 (1978), págs. 391-399.
- [5] Natalia Garcia-Fritz, Hector Pasten y Thanases Pheidas. “Non-Diophantine Sets in Rings of Functions”. En: *Preprint* (2022). URL: <https://arxiv.org/abs/2210.10556>.
- [6] David Hilbert. “Mathematische Probleme”. En: *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* (1900). English translation: *Bull. Amer. Math. Soc.*, 8 (1901-1902) 437-479, págs. 253-297.
- [7] Marc Hindry y Joseph Silverman. *Diophantine Geometry an Introduction*. Springer, 2000.
- [8] Jochen Koenigsmann. “Defining Transcendentals in Function Fields”. En: *Journal of Symbolic Logic* 67 3 (2002), págs. 947-956.
- [9] János Kollár. “Diophantine subsets of function fields of curves”. En: *Algebra Number Theory* 2 3 (2008), págs. 299-311.
- [10] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, 1983.
- [11] Ram Murty y Brandon Fodden. *Hilbert’s Tenth Problem: An Introduction to Logic, Number Theory and Computability*. American Mathematical Society, 2019.
- [12] *The LMFDB Collaboration, The L-functions and modular forms database*. 2024. URL: <https://www.lmfdb.org>.