UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Conjuntos mal distribuidos sobre cuerpos globales y conjuntos excepcionales en geometría diofántica

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Marcelo Exequiel Paredes

Director de tesis y consejero de estudios: Dr. Román Sasyk

Buenos Aires, 2019

Fecha de defensa: 4 de Abril, 2019

Ill-distributed sets on Global Fields and Exceptional Sets in Diophantine Geometry

Abstract

This thesis concerns the study of the density of rational points on algebraic varieties and definable sets in o-minimal structures. The strategy consist in showing that the rational points of these sets are badly distributed in residual classes for many prime moduli.

First, we prove that a set of affine or projective points with coordinates lying in a global field, with bounded height, that occupies few residual classes for many prime moduli must be essentially contained in the zero locus of a polynomial of small degree and height. This generalizes results of Walsh. Then, we apply this result to study a conjecture of Wilkie about the distribution of rational points on certain o-minimal structures, and we prove that this conjecture is equivalent to the fact that certain sets of rational points of bounded height are badly distributed at the level of residual classes for many prime moduli.

Keywords: O-minimal structures, ill-distributed sets at the level of residue classes, global fields, height, Wilkie conjecture.

Conjuntos mal distribuidos sobre Cuerpos Globales y Conjuntos Excepcionales en Geometría Diofántica

Resumen

Esta tesis concierne el estudio de la densidad de puntos racionales en variades algebraicas y conjuntos definibles en estructuras o-minimales. La estrategia consiste en probar que los puntos racionales de estos conjuntos están mal distribuidos en clases residuales para muchos módulos primos.

Primero, probamos que un conjunto de puntos afines o proyectivos con coordenadas en un cuerpo global, de altura acotada que ocupa pocas clases residuales para muchos módulos primos debe estar esencialmente contenido en el conjunto de ceros de un polinomio de grado y coeficientes de altura pequeños. Esto generaliza resultados de Walsh. Luego, aplicamos para estudiar una conjetura de Wilkie acerca de la distribución de los puntos racionales en ciertas estructuras o-minimales, y probamos que esta conjetura es equivalente a que ciertos conjuntos de puntos racionales de altura acotada estén mal distribuidos a nivel de clases residuales para muchos primos.

Palabras claves: Estructuras o-minimales, conjuntos mal distribuidos en clases residuales, cuerpos globales, altura, conjetura de Wilkie.

Introducción

La presente tesis tiene por objetivo estudiar la densidad de los puntos racionales en ciertos conjuntos de naturaleza trascendente. Las técnicas que vamos a utilizar provienen de la Combinatoria Aritmética.

1. Una conjetura en Geometría Diofántica

Para entender los resultados y técnicas que obtenemos en la tesis, empezamos introduciendo el problema que vamos a estudiar. Sea $X \subseteq \mathbb{R}^n$ un conjunto no vacío. Sea K un cuerpo de números. Por $X(K)$ notaremos al subconjunto de puntos de X con coordenadas K-racionales. Dado $x \in K$ sea $H(x)$ la altura afín de un número algebraico. Para $T \geq 1$, definimos

$$X(K,T) := \{\mathbf{x} = (x_1, \ldots, x_n) \in X(K) : H(x_i) \leq T \ \forall i\}. \tag{0.1}$$

Si X es una variedad algebraica, el problema de entender el comportamiento asintótico de $|X(K,T)|$ cuando T tiende a infinito es un problema central en Teoría de Números. Sin embargo, también es importante considerar otro tipo de variedades para X. En efecto, varios problemas de trascendencia se traducen en entender cómo están distribuidos los puntos racionales de ciertas curvas, por ejemplo el gráfico de la exponencial, la curva $\{(2^x, 3^x) : x \in \mathbb{R}\}$, o el conjunto de ceros racionales de un polinomio logarítmico $P(\log(x_1), \ldots, \log(x_n)) = 0$, con $P \in \mathbb{Q}[X_1, \ldots, X_n]$. Nosotros estaremos principalmente interesados en obtener estimaciones para la densidad de puntos racionales de este tipo de variedades "trascendentes". En otras palabras, el problema central para esta tesis es:

Problema 0.1. Sea $X \subseteq \mathbb{R}^n$ una variedad de "naturaleza trascendente". Obtener estimaciones para $|X(K,T)|$.

La instancia más sencilla del Problema 0.1 entonces va a ser el caso que X sea el gráfico de una función f. En este caso, si $f : I \to \mathbb{R}$ es una función analítica real trascendente, con I un intervalo cerrado acotado, Bombieri y Pila obtienen la siguiente estimación:

Teorema 0.1 (Bombieri-Pila, [**BP89**, Theorem 1]). *Sea f una función analítica real en un intervalo acotado cerrado I y supongamos que f es trascendente. Sea Γ el gráfico de f. Sea $\varepsilon > 0$. Entonces existe una constant $c(f,\varepsilon)$ tal que*

$$|t\Gamma \cap \mathbb{Z}^2| \leq c(f,\varepsilon)t^{\varepsilon} \tag{0.2}$$

para todo $t \geq 1$.

La demostración del Teorema 0.1 se basa en el método del determinante de Bombieri-Pila, introducido en el mismo artículo [**BP89**]. A grandes rasgos, el esquema de demostración es el siguiente. Primero, cubrimos los puntos de $t\Gamma \cap \mathbb{Z}^2$ por pocas curvas algebraicas de grado pequeño. Para ello, consideramos un determinante que detecta cuándo un punto pertenece a una curva algebraica, y controlamos el tamaño de este determinante utilizando que Γ no tiene "oscilaciones",

más precisamente, que se puede parametrizar de manera que la derivada de Γ esté acotada. Luego, estimamos la cantidad de puntos en la intersección de una curva algebraica de grado fijo d y la curva Γ. Dado que Γ es el gráfico de una función analítica trascendente, esta intersección está controlada uniformemente: existe una constante $c(d)$ tal que toda curva algebraica de grado a lo sumo d interseca a Γ en a lo sumo $c(d)$ puntos (una forma de pensar este hecho es que se trata de una versión muy débil del teorema de Bezout). Como tenemos pocas curvas cubriendo $t\Gamma \cap \mathbb{Z}^2$ y de grado chico, deducimos el Teorema 0.1.

Cuando t es un número entero positivo, el Teorema 0.1 da una estimación para la cantidad de puntos racionales de la forma $(\frac{x}{N}, \frac{y}{N})$ con $1 \leq |x|, |y| \leq N$ que se hallan en Γ. No obstante, es más natural contar puntos racionales (x, y) con altura afín de x e y acotada por N. En [**Pil07**], Pila extiende el Teorema 0.1 en este contexto, obteniendo

Teorema 0.2. *Sea f una función analtítica real en un intervalo acotado cerrado I y supongamos que f es trascendente. Sea Γ el gráfico de f, y $\Gamma(\mathbb{Q}, T)$ el conjunto de puntos $(x, y) \in \Gamma \cap \mathbb{Q}^2$ tal que la altura afín de x e y es a lo sumo T. Entonces para todo $\varepsilon > 0$, tenemos*

$$|\Gamma(\mathbb{Q}, T)| \leq cT^{\varepsilon}. \tag{0.3}$$

Una primera intuición en el estudio de densidad de puntos racionales en curvas trascendentes es que una tal curva debe tener muy pocos puntos algebraicos. No obstante, la curva trascendente definida por $f(x) = 2^x$ tiene infinitos puntos racionales. Más aún, siguiendo [**VdP68**], es posible construir funciones analíticas trascendentes que aplican números algebraicos en números algebraicos. Por lo tanto, el Teorema 0.1 da información no trivial, y de hecho, Bombieri y Pila en [**BP89**] construyen ejemplos que muestran que en general no se pueden esperar mejores cotas.

La siguiente instancia al Problema 0.1 es considerar conjuntos de dimensión 2. Supongamos entonces que X es el gráfico de una función analítica trascendente $f : [0, 1]^2 \to \mathbb{R}$. Si uno trata de utilizar el método del determinante de Bombieri-Pila como en la prueba del Teorema 0.1, tenemos que considerar intersecciones de X con hipersuperficies de grado grande. La primera dificultad técnica que aparece es que tales intersecciones pueden ser sumamente singulares, y ya no son finitas, pero pertenecen a la familia de conjuntos semi-analíticos. Uno entonces quisiera argumentar de manera inductiva, considerando la imagen de tales conjuntos bajo proyecciones, pero la clase de conjuntos semi-analíticos no es estable por proyecciones. No obstante, la observación fundamental en [**Pil04**] es que las proyecciones mencionadas pertenecen a la clase de conjuntos sub-analíticos acotados. Por lo tanto, una clase de conjuntos adecuada para generalizar el Teorema 0.1 sería la clase de subconjuntos analíticos acotados.

Sin embargo, en dimensiones superiores, obtenemos una obstrucción nueva. Por ejemplo, sea X el gráfico de $f : [0, 1]^2 \to \mathbb{R}$, $f(x) = e^{x+y}$. Se trata de una función analítica trascendente. Sin embargo, $X(\mathbb{Q}, T)$ tiene muchos puntos "triviales": todo punto en la recta $x = -y$ contribuye a $X(\mathbb{Q}, T)$, con lo que $|X(\mathbb{Q}, T)| \gg T^2$. Aún peor, sea $X = \{(x, y, z) : z = x^y, x, y \in [1, 2]\}$. De nuevo X es el gráfico de una función analítica trascendente, pero si $y \in \mathbb{Q}$, la fibra X_y es la curva semi-algebraica $z = x^y$, que de nuevo aporta muchos puntos racionales a $|X(\mathbb{Q}, T)|$. Por lo tanto, si queremos tener alguna esperanza de tener un control para $|X(\mathbb{Q}, T)|$, tenemos que extraer de X todos los puntos de naturaleza "algebraica". Esto conduce a la siguiente noción

Definición 0.2. Sea $X \subseteq \mathbb{R}^n$. La parte algebraica de X, denotada X^{alg}, es la unión de todos los subconjuntos conexos semi-algebraicos de X de dimensión positiva. La parte trascendente de X, denotada X^{trans}, es el complemento $X \backslash X^{\text{alg}}$.

Notemos que la parte algebraica de un conjunto X es en general muy complicada; para $X = \{(x, y, z) : z = x^y, x, y \in [1, 2]\}$ es una unión de infinitas componentes conexas, dadas por las curvas semi-algebraicas $X_y = \{(x, z) : z = x^y, x \in [1, 2]\}$, para $y \in \mathbb{Q} \cap [1, 2]$. No obstante, una vez excluida la parte algebraica de un conjunto sub-analítico, tenemos un resultado análogo al Teorema 0.2, que se sigue de una adaptación adecuada del método del determinante de Bombieri-Pila.

Teorema 0.3 ([**Pil05**, Theorem 1.1]). *Sea $X \subseteq \mathbb{R}^n$ un conjunto sub-analítico compacto de dimensión 2, y sea $\varepsilon > 0$. Entonces existe una constante $c(X, \varepsilon)$ tal que*

$$|X^{trans}(\mathbb{Q}, T)| \leq c(X, \varepsilon) T^{\varepsilon}. \tag{0.4}$$

La generalización del Teorema 0.3 a conjuntos sub-analíticos compactos arbitrarios en $\mathbb{R}^n$ fue conjeturada en [**Pil05**]. Tales conjuntos son globalmente sub-analíticos (es decir son sub-analíticos como subconjuntos de $\mathbb{P}^n(\mathbb{R})$). La observación fundamental de Pila y Wilkie en [**PW06**] es que tales conjuntos determinan una estructura o-minimal. Entonces Pila y Wilkie dan una respuesta al Problema 0.1 en el contexto de conjuntos definibles en estructuras o-minimales:

Teorema 0.4 ([**PW06**, Theorem 1.8]). *Sea $X \subseteq \mathbb{R}^n$ un conjunto definible en una estructura o-minimal, y sea $\varepsilon > 0$. Existe una constante positiva $c = (X, \varepsilon)$ tal que*

$$|X^{trans}(\mathbb{Q}, T)| \leq c(X, \varepsilon) T^{\varepsilon}. \tag{0.5}$$

Notemos que la exclusión de la parte algebraica X^{alg} en el Teorema 4.1, donde los puntos racionales podrían acumularse, es débilmente análoga a la noción de conjuntos excepcionales en Geometría Diofántica. Más específicamente, la conjetura de Lang (ver [**HS00**, § F.5]) afirma que una variedad algebraica V es mordélica (i.e. tiene sólo finitos puntos racionales) fuera de un conjunto excepcional. Cuando V es una curva, esta es la conjetura de Mordell, probada por Faltings. En dimensiones superiores, esta conjetura está sumamente abierta. El conjunto excepcional es la clausura Zariski de la unión de todas las imágenes de morfismos no constantes racionales de espacios proyectivos y variedades abelianas. La parte algebraica de un conjunto X es en algún sentido un conjunto mucho más grande, pero parece ser la manera apropiada de extraer la parte esencialmente trascendente del Problema 0.1.

La idea de la demostración del Teorema 4.1 sigue el esquema del método del determinante de Bombieri-Pila. Primero se prueba que los puntos a estimar residen en pocas hipersuperficies de grado pequeño. Luego se procede por inducción. Esta inducción, no obstante, tiene dificultades técnicas que hacen que sea mejor trabajar con una versión más general del Teorema 4.1. Veremos esto con más detalle en el Capítulo 4. Por el momento, sólo notaremos que, para poder emplear el método del determinante en esta situación, Pila y Wilkie prueban que todo conjunto X definible en una estructura o-minimal admite una parametrización en la cuál las derivadas de todos los órdenes hasta un parámetro prefijado r permanecen acotadas. Este resultado es una generalización del hecho (sencillo) que aparecía en la demostración del Teorema 0.1: el gráfico de una función real analítica en un intervalo acotado cerrado, trascendente, admite una parametrización con derivada acotada.

Notemos que la demostración del Teorema 4.1 no usa propiedades de $\mathbb{Q}$, y por lo tanto se extiende sin dificultad a todo cuerpo de números $K \subseteq \mathbb{R}$, con la constante del teorema ahora dependiendo también de K (de hecho, sólo en el grado de K). También es importante notar que la prueba del Teorema 4.1 admite una mejora importante. Esto fue notado por Pila en [**Pil09**], y el resultado que obtiene es el siguiente.

Teorema 0.5 ([**Pil09**, Theorem 1.6.]). *Sea $X \subseteq \mathbb{R}^n$ definible, sea k un entero positivo, y sea $\varepsilon > 0$. Entonces existe una constante $c(X, k, \varepsilon)$ tal que*

$$|X(k,T)| := |\{\boldsymbol{x} = (x_1, \ldots, x_n) \in X : \max_i [\mathbb{Q}(x_i) : \mathbb{Q}] \leq k, \max_i H(x_i) \leq T\}| \leq c(X,k,\varepsilon)T^{\varepsilon}. \tag{0.6}$$

Las consecuencias que tuvieron los resultados de Pila y Wilkie en la literatura son destacables. Además de establecer estimaciones no triviales para la densidad de los puntos racionales en variedades de naturaleza trascendente como en el Problema 0.1, el Teorema 4.1 y su generalización el Teorema 4.5 han tenido notables impactos en la Geometría Diofántica, por ejemplo en las conjeturas de Manin-Mumford, André-Oort y Zilber-Pink (ver los surveys [**Sca12, Pil15, Daw15**]). La razón principal de este hecho reside en que en estos problemas, uno está interesado en estudiar los puntos "especiales" de ciertas variedades (toros multiplicativos, variedades abelianas, variedades de Shimura), que poseen uniformizaciones sumamente trascendentes. Los puntos especiales que son de interés para el problema en cuestión son aplicados a puntos racionales vía estas uniformaciones, con lo que uno se ve conducido a estudiar la distribución de puntos racionales en una variedad de naturaleza trascendente, digamos X. Luego, para estudiar la densidad de puntos racionales en X, se estudian por separado la parte algebraica y la parte trascendente de X. El Teorema 4.5 permite estudiar el subconjunto X^{trans}, mientras que para estudiar la parte algebraica X^{alg} uno requiere establecer análogos funcionales de la conjetura de Schanuel para las funciones que definen la uniformización.

Volvamos ahora al Problema 0.1. El Teorema 4.1 da una respuesta muy general a este problema, y en general es sabido que no se pueden esperar mejores estimaciones que las que da el teorema. No obstante, para varios conjuntos de interés, por ejemplo el conjunto de ceros de un polinomio logarítmico $P(\log(x), \log(y), \log(z)) = 0$ con $P \in \overline{\mathbb{Q}}[X, Y, Z]$, el Teorema 4.1 provee una cota que se espera esté muy lejos de ser la óptima. Es esperable que para ciertas estructuras o-minimales la estimación del Teorema 4.1 sea mejorable. Esta problemática motivó a Wilkie a formular la siguiente conjetura.

Conjetura 0.3 (Conjetura de Wilkie, [**PW06**, Conjecture 1.11]). Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en la estructura o-minimal $\mathbb{R}_{\exp}$ (ver Capítulo 1,Ejemplo 1.5). Para todo cuerpo de números $K \subseteq \mathbb{R}$, existen constantes positivas $c_1 = c_1(X, K)$, $c_2 = c_2(X)$ tales que

$$|X^{\text{trans}}(K, N)| \leq c_1(\log(N))^{c_2} \tag{0.7}$$

para todo $N > e$.

La Conjetura 0.3 puede interpretarse como una versión (quizás más débil) cuantitativa de la conjetura de Schanuel. El motivo de esto es que varios conjuntos definibles en $\mathbb{R}_{\exp}$ están relacionados con problemas de formas logarítmicas. Por ejemplo, si $P \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$, entonces consideremos X, el conjunto de ceros reales de $P(\log(x_1), \ldots, \log(x_n))$. La conjetura de Schanuel implica que, si $x_1, \ldots, x_n$ son números algebraicos tales que las formas logarítmicas $\log(x_1), \ldots \log(x_n)$ son

linealmente independientes sobre $\mathbb{Q}$, entonces $1, \log(x_1), \ldots, \log(x_n)$ son algebraicamente independientes sobre $\overline{\mathbb{Q}}$. En particular, si $P(x, y, z, w) = xy - zw$, tenemos como consecuencia la conjetura de cuatro exponenciales. Mientras tanto, la Conjetura 4.2 nos dice que los puntos algebraicos que no satisfacen "relaciones algebraicas no triviales" y para los cuáles

$$P(\log(x_1), \ldots, \log(x_n)) = 0$$

deben estar distribuidos de manera muy rala. Más aún, debido a que la constante c_2 no depende del cuerpo K, la cota de la Conjetura 4.2 para ciertas curvas y superficies definibles en $\mathbb{R}_{\exp}$ implica instancias de la conjetura de cuatro exponenciales. Específicamente, sean $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{R}$ con la propiedad que e^{λ_i} es algebraica para todo i. Supongamos que λ_1 y λ_3 son $\mathbb{Q}$-linealmente independientes, y que λ_1 y λ_4 son $\mathbb{Q}$-linealmente independientes. Entonces $\lambda_1\lambda_2 \neq \lambda_3\lambda_4$. Para más detalles, ver [**Pil10, But17**].

Notemos que tenemos una generalización bastante natural de la Conjetura 0.3.

Conjetura 0.4. Sea $f_1, \ldots, f_r$ una cadena Pfaffiana (ver Capítulo 4, § 3) y supongamos que $\tilde{\mathbb{R}} = (\mathbb{R}, <, +, \cdot, f_1, \ldots, f_r)$. Asumamos adicionalmente que $\tilde{\mathbb{R}}$ es "model complete", es decir toda fórmula de primer orden $\phi(\overline{v})$ en $\tilde{\mathbb{R}}$ es equivalente a una fórmula de la forma $\exists\ \overline{w}\ \psi(\overline{v}, \overline{w})$, donde $\psi(\overline{v}, \overline{w})$ es libre de cuantificadores. Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en $\tilde{\mathbb{R}}$. Para todo cuerpo de números $K \subseteq \mathbb{R}$, existen constantes positivas $c_1 = c_1(X, K)$, $c_2 = c_2(X)$ tales que

$$|X^{\text{trans}}(K, N)| \leq c_1(\log(N))^{c_2} \tag{0.8}$$

para todo $N > e$.

Expliquemos ahora qué resultados se saben acerca de la Conjetura 0.3, y su generalización la conjetura 0.4. Si la dimensión de X es igual a 1, entonces la Conjetura 4.2 se sabe que vale debido a los trabajos de Butler [**But12**] y Jones y Thomas [**JT12**]. Si X tiene dimensión más grande que 1, la Conjetura 4.2 sólo se sabe que vale para la familia de superficies

$$\{(x, y, z) \in (0, \infty)^3 : (\log(x))^a(\log(y))^b(\log(z))^c = 1\},\ (a, b, c) \in \mathbb{Q}^3, \tag{0.9}$$

debido a trabajos por Pila [**Pil10**] cuando $(a, b, c) = (1, 1, -1)$ y Butler [**But12**] en el caso general. Si $X \subseteq \mathbb{R}^3$ es definible en una estructura o-minimal como en la Conjetura 0.4, entonces, bajo la hipótesis que X posee una mild parametrization (ver Capítulo 4), en [**JT12**] Jones y Thomas prueban que X satisface la Conjetura 0.4. Este resultado puede generalizarse para un conjunto $X \subseteq \mathbb{R}^n$ de dimensión 2, como se ha probado en [**Sch18**].

Las demostraciones de los casos conocidos de la Conjetura 0.3 y Conjetura 0.4 siguen el esquema de demostración de la prueba del Teorema 4.1, cubriendo primero los puntos a estudiar por hipersuperficies de grado pequeño, y luego estimando la intersección entre una hipersuperficie de grado fijo y el conjunto definible estudiado. Sin embargo, dado que se espera obtener una cota mejor, hay diferencias substanciales. Más precisamente, si queremos estimar $|X^{\text{trans}}(K, T)|$:

(1) Es necesario tener un mayor control en el número y grado de las hipersuperficies que cubren a $X(K, T)$. Esto fuerza a que la cantidad de hipersuperficies y su grado dependa como un polinomio en $\log(T)$.
(2) Debido a (1), no alcanza con tener parametrizaciones regulares como las empleadas en [**PW06**], sino parametrizaciones suaves, con una cota uniforme para todas las derivadas.
(3) Es necesario tener estimaciones fuertes para la intersección de un conjunto definible en $\mathbb{R}_{\exp}$ con una hipersuperficie de grado fijo.

El mayor obstáculo en el esquema de la demostración es (2). Cuando X es de dimensión 1, es posible evitar pasar por considerar parametrizaciones muy regulares, pero en dimensiones superiores, todos los resultados conocidos pasan por probar que X tiene parametrizaciones muy regulares.

Debido a la fuerte conexión entre la Conjetura 0.3 y la conjetura de Schanuel, es esperable que la estimación en esta conjetura valga para otras estructuras o-minimales, como $\mathbb{R}_{\wp}$, la expansión o-minimal del cuerpo real ordenado generada por la función $\wp$ de Weierstrass (para un lattice fijo), o $\mathbb{R}_j$, la expansión o-minimal del cuerpo real ordenado generada por la función j-invariante. En ambos casos, como la función $\wp$ de Weierstrass y la función j-invariante son periódicas, necesitamos restringirnos a un dominio fundamental para garantizar la o-minimalidad de las estructuras mencionadas (ver [**PS13**]). Relacionada con estas estructuras o-minimales, también tenemos la estructura o-minimal de funciones elementales restringidas $\mathbb{R}^{RE} := (\mathbb{R}, <, +, \cdot, \exp|_{[0,1]}, \sin|_{[0,\pi]})$. Para esta última estructura, es un resultado reciente de Binyamini y Novikov [**BN17**, Theorem 2] que los conjuntos definibles en $\mathbb{R}^{RE}$ verifican la cota en la Conjetura 0.3.

El objetivo de esta tesis es estudiar la validez de la Conjetura 0.3 para más conjuntos. Para evitar el obstáculo que aparece en los trabajos [**Pil10, But12, JT12**], vamos a proponer una estrategia que proviene de los problemas inversos de Combinatoria Aritmética.

2. Un problema inverso para conjuntos definibles

Para entender cómo aparece la Combinatoria Aritmética, consideremos $X \subseteq \mathbb{R}^n$ un conjunto definible en $\mathbb{R}_{\exp}$. Dado un primo $p \in \mathbb{Z}$, definimos

$$X_p := \{(x_1, \dots, x_n) \mod (p) : (x_1, \dots, x_n) \in X\}. \tag{0.10}$$

Es fácil ver (ver el Capítulo 4) que la Conjetura 4.2 implica

$$|X^{\text{trans}}(\mathbb{Z}, N)| \leq p^{\kappa} \tag{0.11}$$

para todos los primos $p \geq c_1(\log(N))^{\frac{n}{n-\kappa}}$, con $0 \leq \kappa < n$. Por lo tanto, el conjunto X está mal distribuido a nivel de clases residuales módulo p. Entender cómo son los conjuntos mal distribuidos es un problema de interés general en Teoría de Números, y constituye lo que se conoce como un problema inverso. En el caso en cuestión, $X^{\text{trans}}(\mathbb{Z}, N)$ está mal distribuido, porque es un conjunto muy pequeño.

Planteamos entonces el siguiente problema.

Problema 0.5. Sea $X \subseteq \mathbb{R}^n$ definible en $\mathbb{R}_{\exp}$. Supongamos que para todo $N > e$ existen constantes $c_1 := c_1(X)$, $\kappa = \kappa(X)$ tales que el conjunto X satisface (0.11), para todo primo $p \geq c_1(\log(N))^{\frac{n}{n-\kappa}}$. ¿Qué podemos decir de $X^{\text{trans}}(\mathbb{Z}, T)$?

Sin la hipótesis de que X sea definible en $\mathbb{R}_{\exp}$, no podemos decir mucho. En efecto, una razón para que un conjunto esté mal distribuido a nivel de clases residuales es que tenga estructura algebraica. Por ejemplo, consideremos una variedad algebraica $V \subseteq \mathbb{A}^n$ definida por polinomios con coeficientes en $\mathbb{Z}$. Podemos considerar la variedad V_p sobre $\mathbb{Z}/p\mathbb{Z}$ que se obtiene de reducir módulo p a V. Un hecho remarcable es que si V era una variedad geométricamente irreducible, de dimensión d y grado $\deg(V)$, entonces, salvo finitos primos p, la reducción V_p es una variedad sobre $\mathbb{Z}/p\mathbb{Z}$ geométricamente irreducible, de dimensión d y grado $\deg(V)$. Por lo tanto, la estimación de Lang-Weil nos dice que la cantidad de puntos $\mathbb{F}_p$-racionales de V_p es exactamente $p^d + O(p^{d-1/2})$. Por lo tanto, una variedad algebraica cumple que, para todos salvo finitos primos p, las reducciones V_p son conjuntos pequeños en $\mathbb{A}^n(\mathbb{F}_p)$, y en consecuencia se trata de un conjuntos mal distribuido en clases residuales.

En resumen, un conjunto como en el Problema 0.5, podría, entre otras cosas, o bien ser pequeño, o bien tener algún tipo de estructura algebraica. Esto nos lleva a considerar el siguiente problema inverso en Combinatoria Aritmética, observado por Croot y Elsholtz [**CL07**] y por Helfgott y Venkatesh [**HV09**].

Problema 0.6 (Problema inverso de criba). Sea $S \subseteq [N]^d$ un conjunto que ocupa muy pocas clases residuales módulo p para muchos primos p. Entonces, o bien S es pequeño, o posee alguna estructura algebraica.

El Problema 0.6 fue resuelto por Helfgott y Venkatesh en [**HV09**] para el caso que $d = 2$, y para $d > 2$ por Walsh en [**Wal12**]. Específicamente, el resultado probado en [**Wal12**] es el siguiente.

Teorema 0.6 (Walsh, [**Wal12**, Theorem 1.1]). *Sean $0 \leq k < d$ enteros y sean $\varepsilon, \alpha, \eta > 0$ números reales positivos. Entonces, existe una constante C dependiendo sólo en los parámetros anteriores, tal que para todo conjunto $S \subseteq [N]^d$ ocupando a lo sumo αp^κ clases residuales módulo p para todo primo p al menos una de las siguientes afirmaciones vale:*

(1) (S es pequeño) $|S| \ll_{d,k,\varepsilon,\alpha} N^{k-1+\varepsilon}$,
(2) (S es fuertemente algebraico) Existe un polinomio $f \in \mathbb{Z}[X_1, \ldots, X_d]$ de grado a lo sumo C y coeficientes acotados por N^C anulándose en al menos $(1-\eta)|S|$ puntos de S.

Volvamos ahora al Problema 0.5. El Teorema 3.2 nos sugiere que las hipótesis sobre X implican, o bien una estimación como en (1), o bien según (2), que $X^{\text{trans}}(\mathbb{Z}, N)$ está esencialmente contenido en una hipersuperficie de grado acotado. Ahora, $X^{\text{trans}}(\mathbb{Z}, N)$ es, por definición, altamente no algebraico, por lo tanto si este conjunto verificara (2), debería tener estructura fuertemente algebraica, y nuestra intuición nos dice que un conjunto simuláneamente "algebraico" y "no algebraico" debe ser pequeño.

La heurística del párrafo anterior, sin embargo, no se traduce a una demostración. Para empezar, el Teorema 3.2 da una dicotomía, con lo que podría darnos que $|X^{\text{trans}}(\mathbb{Z}, T)|$ sea pequeño, pero no lo suficientemente pequeño como deducir una cota como la de la Conjetura 0.3. Esta obstrucción en un principio podría solucionarse: en [**Wal12**, Theorem 6.1], Walsh prueba, que si un conjunto mal distribuido es suficientemente regular, entonces está esencialmente contenido en una hipersuperficie de grado acotado (es decir, en el Teorema 3.2 siempre vale (2)). No obstante, una de las hipótesis de regularidad es que, a grandes rasgos, $X^{\text{trans}}(\mathbb{Z}, T)$ tenga al menos T^ε puntos para algún ε, y por el Teorema 4.1 sabemos que esto no es posible para T suficientemente grande.

En conclusión, nuestro Problema 0.5 es un problema inverso, como en el sentido del Problema 0.6, pero como ya sabemos que nuestros conjuntos son pequeños, no podemos emplear el Teorema 3.2. Lo que necesitaríamos es entonces un resultado que afirme que todo conjunto mal distribuido posee algún tipo de estructura algebraica. En esta dirección, en [**Wal14**], se prueba un resultado de este tipo.

Teorema 0.7 ([**Wal14**, Theorem 1.3]). *Para todo entero posiitvo d, y todo número real $0 \leq \kappa < d$, existe $\tau = \tau(d, \kappa) > 0$ tal que lo siguiente vale. Escribamos $\mathcal{P}_I$ para los primos en el intervalo*

$$I = \left[\tau(\log(N))^{\frac{d}{d-\kappa}}, 2\tau(\log(N))^{\frac{d}{d-\kappa}}\right]. \tag{0.12}$$

Entonces, para todo $S \subseteq \{1, \ldots, N\}^d$ ocupando $\ll p^\kappa$ clases residuales módulo p para todo $p \in \mathcal{P}_I$, y para todo $\varepsilon > 0$, existe un polinomio no nulo $P \in \mathbb{Z}[X_1, \ldots, X_d]$ de complejidad $\ll_{\kappa,d,\varepsilon} (\log(N))^{\frac{\kappa}{d-\kappa}}$ anulándose en al menos $(1-\varepsilon)|S|$ puntos de S.

Aquí, por un polinomio P de complejidad a lo sumo C nos referimos a que P tiene grado a lo sumo C y sus coeficientes están acotados por N^C.

Observemos ahora cómo la heurística de demostración que planteamos anteriormente puede efectuarse a cabo con el Teorema 0.7, aplicado al caso que $X \subseteq \mathbb{R}^2$ sea el gráfico de una función trascendente analítica definible en $\mathbb{R}_{\exp}$. En este caso, $X^{\text{trans}} = X$. Supongamos que X está en las condiciones del Problema 0.5, por lo tanto $X(\mathbb{Z}, T)$ ocupa a lo sumo p^κ clases residuales módulo p para muchos primos p. Por el Teorema 0.7, concluimos que existe una curva algebraica $V(P)$ de grado $O((\log(T))^{c(X)})$ que se anula en una proporción positiva de $X(\mathbb{Z}, T)$. Para concluir que el conjunto $(X \cap V(P))(\mathbb{Z}, T)$ es pequeño, usamos que el conjunto X puede describirse implícitamente por funciones Pfaffianas, luego $X \cap V(P)$ puede estimarse a partir de las cotas de complejidad de Khovanskii para funciones Pfaffianas (ver el Capítulo 4). Luego deducimos que $(X \cap V(P))(\mathbb{Z}, T) \ll_X (\log(T))^{c(X)}$, lo que prueba un caso muy particular de la estimación de la Conjetura 4.2.

En esta tesis, lo que realizamos es adaptar la demostración explicada en el párrafo anterior para proponer una estrategia para demostrar la Conjetura 0.3 para conjuntos de dimensión 2.

3. Generalizaciones al contexto de cuerpos globales

Para poder generalizar la estrategia explicada en el contexto de cuerpos de números y para los puntos racionales $X^{\text{trans}}(K, N)$, primero extendemos en este contexto al Teorema 0.7. De hecho, nosotros probamos que el Teorema 0.7 puede generalizarse en el contexto de cuerpos globales, reemplazando $\mathbb{Z}$ por el anillo de enteros O_K de un cuerpo global K. El análogo diofántico de $\{0, \dots, N\}$ en K que consideramos es el conjunto de elementos de O_K de altura afín $H(x)$ a lo sumo N. Denotamos a este conjunto por $[N]_{O_K}$. Entonces tenemos la siguiente definición de complejidad.

Definición 0.7 (Complejidad). Decimos que un polinomio no nulo $P \in O_K[X_1, \dots, X_n]$ tiene complejidad a lo sumo C en $[N]^n_{O_K}$ si tiene grado a lo sumo C y sus coeficientes tienen altura acotada por N^C.

Para un ideal no nulo $I \subseteq O_K$, sea $\mathcal{N}(I)$ la norma absoluta de I, definida como el cardinal (finito) del conjunto O_K/I. Para un ideal primo no nulo $\mathfrak{p} \subseteq O_K$, y un conjunto $X \subseteq O_K^n$, denotamos para el conjunto de clases residuales de X módulo $\mathfrak{p}$:

$$X_{\mathfrak{p}} = \{(x_1, \dots, x_n) \mod (\mathfrak{p}) : (x_1, \dots, x_n) \in X)\}. \tag{0.13}$$

Siguiendo la misma estrategia de Walsh, probamos la siguiente generalización del Teorema 0.7.

Teorema 0.8. *Para todo $n > 0$, todo número real $0 \leq \kappa < n$ y todo cuerpo global K, existe $\tau = \tau(n, \kappa, K) \geq 1$ tal que lo siguiente vale. Denotemos por $\mathcal{P}_{I,K}$ el conjunto de ideales primos no nulos $\mathfrak{p} \subseteq O_K$ definido como*

(0.14)

$$\mathcal{P}_{I,K} := \begin{cases} \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) \in I = [\tau(\log(N))^{\frac{n}{n-\kappa}}, 2\tau(\log(N))^{\frac{n}{n-\kappa}}]\} \text{ si } K \text{ es un cuerpo de números} \\ \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) = \tau(\log(N))^{\frac{n}{n-\kappa}}\} \text{ si } K \text{ es un cuerpo funcional} \end{cases}.$$

Entonces, para todo $X \subseteq [N]^n_{O_K}$ con $|X_{\mathfrak{p}}| \ll \mathcal{N}(\mathfrak{p})^\kappa$ para todo primo $\mathfrak{p} \in \mathcal{P}_{I,K}$, y todo $\varepsilon > 0$, existe algún $P \in O_K[X_1, \dots, X_n]$ no nulo de complejidad $\ll_{\kappa,n,\varepsilon,K} (\log(N))^{\frac{\kappa}{n-\kappa}}$ anulándose en al menos $(1-\varepsilon)|X|$ puntos de X.

Notemos que el Teorema 0.7 es el caso $K = \mathbb{Q}$ del Teorema 0.8. No obstante, este resultado concierne el estudio de puntos enteros, mientras que la Conjetura 0.3 afirma una cota en los puntos racionales de un conjunto definible. Por este motivo, damos una prueba de un resultado más general que el Teorema 0.8, que concierne el estudio de subconjuntos de $\mathbb{P}^n(K)$ mal distribuido al nivel de clases residuales. Usamos la notación $[N]_{\mathbb{P}^n(K)}$ para referirnos a los puntos de $\mathbb{P}^n(K)$ de altura proyectiva a lo sumo N.

Teorema 0.9. *Para todo $n > 0$, todo número real $0 \leq \kappa < n$ y todo cuerpo global K, existe $\tau = \tau(n, \kappa, K) \geq 1$ tal que lo siguiente vale. Denotemos por $\mathcal{P}_{I,K}$ el conjunto de ideales primos no nulos $\mathfrak{p} \subseteq O_K$ definido como*
(0.15)
$$\mathcal{P}_{I,K} := \begin{cases} \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) \in I = [\tau(\log(N))^{\frac{n}{n-\kappa}}, 2\tau(\log(N))^{\frac{n}{n-\kappa}}]\} \text{ si } K \text{ es un cuerpo de números} \\ \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) = \tau(\log(N))^{\frac{n}{n-\kappa}}\} \text{ si } K \text{ es un cuerpo funcional} \end{cases}.$$
Entonces, para todo $X \subseteq [N]_{\mathbb{P}^n(K)}$ con $|X_{\mathfrak{p}}| \ll \mathcal{N}(\mathfrak{p})^{\kappa}$ para todo primo $\mathfrak{p} \in \mathcal{P}_{I,K}$, y todo $\varepsilon > 0$, existe algún $P \in O_K[X_0, \ldots, X_n]$ no nulo, homogéneo, de complejidad $\ll_{\kappa,n,\varepsilon,K} (\log(N))^{\frac{\kappa}{n-\kappa}}$ anulándose en al menos $(1-\varepsilon)|X|$ puntos de X.

No es muy difícil de ver que el Teorema 0.9 implica el Teorema 0.8 (ver Capítulo 3). Notemos que, desde el punto de vista de Geometría Diofántica, resulta de interés tener un resultado como el Teorema 0.9, pero considerando al conjunto X contenido en una variedad proyectiva arbitraria Z. En este caso, esperaríamos que un conjunto mal distribuido esté esencialmente contenido en una hipersuperficie proyectiva, que no se anule en Z. En el Capítulo 2 damos una demostración de un resultado de este estilo, que generaliza al Teorema 0.9.

Teorema 0.10 ([**Par19**, Theorem 3.2]). *Sea $Z \subseteq \mathbb{P}^m(\overline{K})$ una variedad proyectiva definida sobre un cuerpo global K. Supongamos que Z es geométricamente irreducible de dimensión n. Para todo $n > 0$, todo número real $0 \leq \kappa < n$ existe una constante $\tau = \tau(n, \kappa, K, Z) \geq 1$ tal que lo siguiente vale. Escribamos $\mathcal{P}_{I,K}$ para el conjunto de ideales primos no nulos $\mathfrak{p} \subseteq O_K$ definido como*
(0.16)
$$\mathcal{P}_{I,K} := \begin{cases} \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) \in I = [\tau(\log(N))^{\frac{n}{n-\kappa}}, 2\tau(\log(N))^{\frac{n}{n-\kappa}}]\} \text{ si } K \text{ es un cuerpo de números} \\ \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) = \tau(\log(N))^{\frac{n}{n-\kappa}}\} \text{ si } K \text{ es un cuerpo funcional} \end{cases}.$$
Entonces, para todo $X \subseteq Z \cap [N]_{\mathbb{P}^n(K)}$ con $|X_{\mathfrak{p}}| \ll \mathcal{N}(\mathfrak{p})^{\kappa}$ para todo primo $\mathfrak{p} \in \mathcal{P}_{I,K}$, y para todo $\varepsilon > 0$, existe un polinomio homogéneo no nulo $P \in O_K[T_0, \ldots, T_m]$ que no es cero en en el anillo coordenado $\overline{K}[Z]$, de complejidad $\ll_{\kappa,n,m,\varepsilon,K,Z} (\log(N))^{\frac{n}{n-\kappa}}$ anulándose en al menos $(1-\varepsilon)|X|$ puntos de X.

Como mencionamos, la idea de la demostración del Teorema 0.10 sigue la demostración de [**Wal14**]. Dado X como en el Teorema 0.10, primero construimos un subconjunto característico $C \subseteq X$ de complejidad pequeña, es decir, si un polinomio de complejidad pequeña se anula en C, entonces se anula en una proporción positiva de X. Luego, construimos un polinomio homogéneo de complejidad pequeña que se anule en C. En la demostración, surgen algunas dificultades. Entre estas, que al considerar subconjuntos en una variedad Z, tenemos que tener un cuidado adicional para que el polinomio que construyamos no se anule en Z. Para evitar esta dificultad, utilizamos el lema de normalización de Noether para realizar un cambio de variables adecuado.

En el capítulo 3 estudiamos la efectividad del Teorema 0.10. Por este motivo, damos una prueba efectiva del lema de normalización de Noether, que consideramos puede ser de utilidad:

Teorema 0.11. *Sea V una variedad proyectiva irreducible definida sobre un cuerpo global K. Entonces existe un morfismo finito $\varphi : V \to \mathbb{P}^{\dim(V)}$, definido sobre K, tal que $\varphi(\boldsymbol{x}) = (L_0(\boldsymbol{x}) : \ldots : L_{\dim(V)}(\boldsymbol{x}))$ con L_i formas lineales con coeficientes en $\mathbb{Z}$ o $\mathbb{F}_q[T]$ según K, de altura acotada por $\ll_{m,k} \deg(V)^{\dim(V)}$, donde la constante implícita es efectivamente computable.*

Lo nuevo del Teorema 0.11 es la estimación de la altura en los coeficientes del cambio de variables lineal.

Una vez probado el Teorema 0.10, lo aplicamos a la Conjetura 0.3, y probamos el siguiente resultado.

Teorema 0.12 ([**Par19**, Theorem 4.3]). *Sea X un conjunto definible en $\mathbb{R}_{\exp}$, de dimensión a lo sumo 2. Entonces X cumple la Conjetura 4.3 para el cuerpo K si y sólo si $X^{trans}(K, T)$ ocupa pocas clases residuales modulo $\mathfrak{p}$ para muchos primos $\mathfrak{p}$ de K.*

Agradecimientos

- A mis padres y a mi hermana, por su constante apoyo y calidez. Sin ellos no habría llegado tan lejos;
- A Román, por las numerosas reuniones, discusiones matemáticas, charlas de seminario y referencias, y en general por la gran cantidad de horas que le dedica a hacer matemática conmigo;
- A los jurados, por haber leído detenidamente la tesis y haberme señalado algunas referencias útiles.
- A Fernando Cukierman, Alicia Dickenstein, Harald Helfgott, Marc Hindry, Roberto Miatello, Ariel Pacetti y Miguel Walsh, por responder a varias de mis preguntas y contagiar un poco su entusiasmo matemático;
- A Eli, Jaz, y Yami, con quienes suelo compartir muchos momentos (entre estos los distintos juegos de mesa que propone Eli, siempre con la energía que la caracteriza);
- A Facu, Juan y Mora, mis amigos y compañeros de investigación, de quienes suelo aprender algo todo los días, tanto matemático como de la vida. Gracias por el tiempo que compartimos y por su amistad.

Índice

CAPÍTULO 1

Estructuras o-minimales

El objetivo principal de este capítulo es introducir la noción de estructuras o-minimales y sus propiedades básicas que usaremos en el Capítulo 4. La exposición sigue el libro [**vdD98**] y el artículo [**JW08**].

1. Nociones básicas y ejemplos

Sea A un conjunto no vacío y supongamos que tenemos dados, para todo $n \geq 1$, una colección $\mathcal{S}_n$ de subconjuntos de A^n. Escribimos $\mathcal{S}$ para la unión disjunta $\bigcup_{n\in\mathbb{N}} \mathcal{S}_n$. Llamamos a $\mathcal{S}$ una pre-estructura (en A).

Definición 1.1 (Estructura). Una estructura en A es una pre-estructura $\mathcal{S} = \bigcup_{n\in\mathbb{N}} \mathcal{S}_n$ tal que las siguientes condiciones valen:

(S1) Para cada $n \in \mathbb{N}$, $\mathcal{S}_n$ es un álgebra booleana de subconjuntos de A^n, i.e. es cerrada bajo uniones y complementos (y por lo tanto bajo intersecciones);
(S2) Si $X \in \mathcal{S}_n$ entonces $A \times X$ y $X \times A$ están en $\mathcal{S}_{n+1}$;
(S3) Si $X \in \mathcal{S}_{n+1}$ y $\pi : A^{n+1} \to A^n$ es la función de proyección en las primeras n coordenadas entonces $\pi(A) \in \mathcal{S}_n$.

En vez de decir que $\mathcal{S}$ es una estructura en A también decimos que $(A, \mathcal{S})$ es una estructura. Los conjuntos que están en $\mathcal{S}$ se llaman definibles, y las funciones cuyos gráficos están en $\mathcal{S}$ se llaman funciones definibles.

Un ejemplo básico e importante de una estructura son los conjuntos constructibles. Sea Ω un cuerpo algebraicamente cerrado y sea $K \subseteq \Omega$ un subcuerpo. Los subconjuntos K-constructibles de Ω^n son las uniones finitas de conjuntos de la forma $\{\mathbf{x} \in \Omega^n : f_1(\mathbf{x}) = \cdots = f_k(\mathbf{x}) = 0, g(\mathbf{x}) \neq 0\}$, donde $f_1(X), \ldots, f_k(X), g(X) \in K[X]$ y $X = (X_1, \ldots, X_n)$. El hecho que los conjuntos K-constructibles conforman una estructura en Ω es esencialmente el teorema de constructibilidad de Chevalley, el cuál en términos de teoría de modelos equivale a la eliminación de cuantificadores para cuerpos algebraicamente cerrados.

Ahora, sea A un conjunto no vacío. Dadas dos estructuras $\mathcal{S}(1) = \bigcup_{n\in\mathbb{N}} \mathcal{S}(1)_n$ y $\mathcal{S}(2) = \bigcup_{n\in\mathbb{N}} \mathcal{S}(2)_n$ en A escribimos $\mathcal{S}(1) \subseteq \mathcal{S}(2)$ si $\mathcal{S}(1)_n \subseteq \mathcal{S}(2)_n$ para todo n; esto define un orden parcial en la colección de estructuras en A. Toda familia $(\mathcal{S}(i))_{i\in I}$ de estructuras en A tiene una cota inferior más grande $\mathcal{S}$ en la colección de estructuras de A, concretamente

$$\mathcal{S} = \bigcap_i \mathcal{S}(i) \text{ con } \mathcal{S}_m := \bigcap_i \mathcal{S}(i)_m \text{ para cada } m. \tag{1.1}$$

Es sumamente conveniente interpretar la noción de una estructura en un conjunto no vacío A en términos de teoría de modelos.

Definición 1.2 (Estructura de teoría de modelos). Una estructura de teoría de modelos $\mathcal{A} = (A, (S_i)_{i\in I}, (f_j)_{j\in J})$ consiste de un conjunto no vacío A, relaciones $S_i \subseteq A^{m(i)}$ ($i \in I$, $m(i) \in \mathbb{N}_0$), y

funciones $f_j : A^{n(j)} \to A$ ($j \in J, n(j) \in \mathbb{N}_0$). Si $n(j) = 0$, identificamos f_j con su único valor en A, y llamamos f_j una constante. También notamos A al conjunto subyacente de $\mathcal{A}$, y llamamos a los S_i y f_j las relaciones y funciones básicas (o primitivas) de $\mathcal{A}$. Si los conjuntos de índices I y J son finitos usualmente listamos las relaciones y funciones.

Dada una estructura de teoría de modelos $\mathcal{A} = (A, (S_i)_{i\in I}, (f_j)_{j\in J})$, y un conjunto $C \subseteq A$ definimos la estructura de teoría de modelos $\mathcal{A}_C := (A, (S_i)_{i\in I}, (f_j)_{j\in J}, (c)_{c\in C})$ la cual tiene el mismo conjunto subyacente y las mismas relaciones básicas de $\mathcal{A}$, pero le agregamos a las funciones básicas f_j una constante c para cada elemento $c \in C$, donde formalmente identificamos c con la correspondiente función $A^0 \to A$.

Dada una estructura de teoría de modelos $\mathcal{A} = (A, (S_i), (f_j))$, notamos $\mathrm{Def}(\mathcal{A})$ a la estructura más pequeña en el conjunto A (en el sentido de la Definición 1.1) que contiene cada relación S_i y cada función f_j. Notemos que para cada $C \subseteq A$ la estructura $\mathrm{Def}(\mathcal{A}_C)$ en A es igual o más grande que $\mathrm{Def}(\mathcal{A})$. Los conjuntos $S \subseteq A^m$ y las funciones $f : S \to A^n$ que pertenecen a $\mathrm{Def}(\mathcal{A})$ también se dicen definibles en $\mathcal{A}$ (o sólo definibles, cuando $\mathcal{A}$ es claro en el contexto). Un punto $\mathbf{a} = (a_1, \ldots, a_m) \in A^m$ se dice definible en $\mathcal{A}$ si el conjunto $\{\mathbf{a}\} \subseteq A^m$ es definible en $\mathcal{A}$.

Usualmente escribimos "definible en $\mathcal{A}$ usando constantes de C", o "definible en $\mathcal{A}$ con parámetros de C" en lugar de "definible en $\mathcal{A}_C$". Para $C = A$ escribimos "definible en $\mathcal{A}$ usando constantes" o "definible en $\mathcal{A}$ usando parámetros" en vez de "definible en $\mathcal{A}_A$".

De ahora en más nos vamos a focalizar en el caso $A = \mathbb{R}$. Una estructura o-minimal $\mathcal{S} = \bigcup_{n\in\mathbb{N}} \mathcal{S}_n$ en $\mathbb{R}$ será una estructura tal que, si empezamos con conjuntos relativamente simples en el espacio euclideano y realizamos operaciones elementales usuales en ellos, sólo podemos obtener conjuntos con el mismo nivel de complejidad. Resulta que esto ocurrirá si los conjuntos de $\mathcal{S}_1$ son simples.

Definición 1.3 (Estructura o-minimal). Una estructura o-minimal (en $\mathbb{R}$) es una estructura $\mathcal{S}$ en $\mathbb{R}$ tal que

(O1) $\{(x, y) \in \mathbb{R}^2 : x < y\} \in \mathcal{S}_2$,
(O2) los conjuntos en $\mathcal{S}_1$ son exactamente las uniones finites de intervalos y puntos.

En otras palabras, una estructura o-minimal es una estructura $(\mathbb{R}, \mathcal{S})$ que contiene la estructura definida por $(\mathbb{R}, <)$ y cumple que $\mathcal{S}_1$ consiste sólo de uniones finitas de intervalos y puntos. Si tenemos dada una estructura de teoría de modelos $\mathcal{A} = (\mathbb{R}, (S_i)_{i\in I}, (f_j)_{j\in J})$, entonces vamos a decir que $\mathcal{A}$ es una estructura o-minimal si la estructura obtenida por los conjuntos definibles con parámetros es o-minimal.

Observación 1.4. Si $\mathcal{S}$ es una estructura satisfaciendo $(O1)$ pero no la condición $(O2)$, entonces los conjuntos definibles en $\mathcal{S}$ pueden ser muy complejos, ver [**vdD98**, Chapter 1, § 2.6].

Ejemplo 1.5. Mencionemos los siguientes ejemplos importantes de estructuras o-minimales.

(I) Un conjunto $X \subseteq \mathbb{R}^n$ se dice básico semi-algebraico si es de la forma $\{\mathbf{a} \in \mathbb{R}^n : P(\mathbf{a}) > 0\}$ para algún polinomio $P(\mathbf{X}) \in \mathbb{R}[X_1, \ldots, X_n]$. Un conjunto semi-algebraico en $\mathbb{R}^n$ es una unión finita de conjuntos semi-algebraicos básicos. Si $\mathcal{S}_n$ denota la familia de conjuntos semi-algebraicos en $\mathbb{R}^n$, entonces $\mathcal{S} = \bigcup_{n\in\mathbb{N}} \mathcal{S}_n$ es una estructura o-minimal (ver [**vdD98**, Chapter 2]). Aquí, la única afirmación no trivial es que la proyección de un conjunto semi-algebraico sigue siendo un conjunto semi-algebraico (esto es el el contenido del teorema de Tarski-Seidenberg). Equivalentemente, los conjuntos definibles con constantes en $\overline{\mathbb{R}} =$

$(\mathbb{R}, <, 0, 1, +, -, \cdot)$ son exactamente los conjuntos semi-algebraicos, y ellos conforman una estructura o-minimal. Llamamos a $\overline{\mathbb{R}}$ el cuerpo ordenado de números reales.

(II) Sea $M \subseteq \mathbb{R}^n$ una variedad analítica real. Un conjunto $X \subseteq M$ se dice semi-analítico si para cada $\mathbf{x} \in M$ existe un entorno U tal que $X \cap U$ es una unión finita de conjuntos de la forma $\{\mathbf{x} \in \mathbb{R}^n : f_1(\mathbf{x}) = \ldots = f_r(\mathbf{x}) = 0, g_1(\mathbf{x}) > 0, \ldots, g_h(\mathbf{x}) > 0\}$ con $f_1, \ldots, f_r, g_1, \ldots, g_h$ funciones anaílitcas reales en U. Más en general, S se dice sub-analítica si cada punto de M admite un entorno U tal que $X \cap U$ es una proyección de un conjunto semi-analítico relativamente compacto (i.e. existe una variedad analítica real N y un subconjunto compacto semi-analítico A de $M \times N$ tal que $X \cap U = \pi(A)$, donde $\pi : M \times N \to M$ es una proyección). Un subconjunto globalmente sub-analítico de $\mathbb{R}^n$ es un subconjunto sub-analítico de $\mathbb{R}^n$ que también es sub-analítico cuando se lo consider como subconjunto de $\mathbb{P}^n(\mathbb{R})$, bajo la identificación $(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$. Más aún, todos los conjuntos semi-algebraicos son subconjuntos globalmente sub-analíticos de $\mathbb{R}^n$. Definimos $\mathcal{S}^{\text{an}} = \bigcup_{n\in\mathbb{N}} \mathcal{S}_n^{\text{an}}$. Entonces $\mathcal{S}^{\text{an}}$ es una estructura o-minimal (esto es una consecuencia de un resultado de Gabrielov, el cuál afirma que el complemento de un conjunto sub-analítico es sub-analítico, ver [**DvdD88, Gab68**]). Equivalentemente, podemos definir esta estructura o-minimal de la siguiente manera. Llamemos $\mathcal{F}_n$ para la familia de funciones analíticas reales $f : U \subseteq \mathbb{R}^n \to \mathbb{R}$ donde U es un conjunto abierto conteniendo el cubo $[-1, 1]^n$. Para toda $f \in \mathcal{F}_n$, definimos

$$\tilde{f}(\mathbf{x}) := \begin{cases} f(x) \text{ si } \mathbf{x} \in [-1, 1]^n \\ 0 \text{ en otro caso} \end{cases} . \tag{1.2}$$

Llamamos $\tilde{\mathcal{F}}_n$ a la nueva familia de funciones obtenida. Denotamos $\tilde{\mathcal{F}} = \bigcup_{n\in\mathbb{N}} \tilde{\mathcal{F}}_n$. Entonces los conjuntos globalmente sub-analíticos de $\mathbb{R}^n$ son exactamente los conjuntos definibles con constantes en la estructura $\mathbb{R}_{\text{an}} = (\mathbb{R}, <, 0, 1, +, -, \cdot, (\tilde{f})_{\tilde{f}\in\tilde{\mathcal{F}}})$, y conforman una estructura o-minimal. La estructura $\mathbb{R}_{\text{an}}$ se llama la expansión analítica restringida de los reales.

(III) Dado $\mathbf{x} = (x_1, \ldots, x_n)$, denotemos $e^{\mathbf{x}} = (e^{x_1}, \ldots, e^{x_n})$. Para cada $n \in \mathbb{N}$, definimos

$$\mathcal{S}_n^{\exp} := \{V(F) : F(\mathbf{x}) = P(\mathbf{x}, e^{\mathbf{x}})\} \text{ para algún } P(\mathbf{x}, \mathbf{y}) \in \mathbb{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]. \tag{1.3}$$

Sea $\mathcal{S}^{\exp}$ la menor estructura conteniendo $\bigcup_{n\in\mathbb{N}} \mathcal{S}_n^{\exp}$. Por el resultado de Wilkie [**Wil96**, Second Main Theorem] los conjuntos definibles en $\mathcal{S}^{\exp}$ son precisamente las proyecciones de conjuntos en $\bigcup_{n\in\mathbb{N}} \mathcal{S}_n^{\exp}$. Equivalentemente, los conjuntos definibles de $\mathcal{S}^{\exp}$ son conjuntos definibles con constantes en la estructura $\mathbb{R}_{\exp} = (\mathbb{R}, <, 0, 1, +, -, \cdot, \exp)$.

(IV) Sean $f_1, \ldots, f_r$ una cadena Pfaffiana en $\mathbb{R}^n$ (ver el Capítulo 4, § 3). Entonces resulta que si consideramos $(\mathbb{R}, <, 0, 1, +, -, \cdot, \tilde{f}_1, \ldots, \tilde{f}_r)$ es una estructura o-minimal, donde $\tilde{f}_i$ denota la función restringida asociada a f_i, como en el ejemplo (II). Este resultado es [**Wil96**, First Main Theorem].

(V) Si en el ejemplo (IV) consideramos la estructura no restringida $(\mathbb{R}, <, 0, 1, +, -, \cdot, f_1, \ldots, f_r)$ entonces esta estructura es o-minimal. Más aún, si consideramos $\mathcal{F}$ la familia de funciones Pfaffianas (ver el Capítulo 4, § 3), entonces $\mathbb{R}_{\text{Pfaff}} := (\mathbb{R}, <, 0, 1, +, -, \cdot, \mathcal{F})$ es una estructura o-minimal. Ambos resultados se siguen de [**Wil99**, Theorem 1.9] y el teorema de Khovanskii (ver el Capítulo 4).

Observación 1.6. No hay una estructura o-minimal más grande; esto es un resultado de [**RSW03**].

2. Propiedades básicas de estructuras o-minimales

De ahora en más, vamos a trabajar con estructuras o-minimales que son expansiones del cuerpo real ordenado, i.e. contienen los conjuntos definibles de $\overline{\mathbb{R}} = (\mathbb{R}, <, 0, 1, +, -, \cdot)$. Fijtemos una tal estructura o-minimal, digamos $(\mathbb{R}, \mathcal{S})$.

La primera manifestación de "domabilidad" en una estructura o-minimal es el hecho que las funciones 1-dimensionales que son definibles en $\mathcal{S}$ son monótonas a trozos y poseen derivadas continuas.

Teorema 1.7 (Teorema de monotonía, [**vdD98**, Chapter 3, §1.2], [**vdD98**, Chapter 7, § 2.5]). *Sea $f : (a, b) \to \mathbb{R}$ una función definible en el intervalo (a, b). Fijemos un entero no negativo r. Entonces existen puntos $a_1 < \cdots < a_k$ en (a, b) tales que en cada subintervalo (a_j, a_{j+1}) con $a_0 = a$, $a_{k+1} = b$, la función es constante o estrictamente monótona y $f|_{(a_j, a_{j+1})} \in C^r(\mathbb{R})$ para todo j.*

El hecho remarcable de las estructuras o-minimales es que los "teoremas de finitud" valen de manera uniforme. Una primera instancia de este hecho es la siguiente "propiedad de finitud uniforme". Dado $Y \subseteq \mathbb{R}^{m+1}$, decimos que Y es finito sobre $\mathbb{R}^m$ si para todo $\mathbf{x} \in \mathbb{R}^m$ la fibra $Y_{\mathbf{x}} := \{y \in \mathbb{R} : (\mathbf{x}, y) \in Y\}$ es finito; llamamos a Y uniformemente finito sobre $\mathbb{R}^m$ si existe $N \in \mathbb{N}$ tal que $|Y_{\mathbf{x}}| \leq N$ para todo $\mathbf{x} \in \mathbb{R}^m$.

Lema 1.8 ([**vdD98**, Chapter 3, § 2.13]). *Supongamos que $Y \subseteq \mathbb{R}^{m+1}$ es finito sobre $\mathbb{R}^m$. Entonces Y es uniformemente finito sobre $\mathbb{R}^m$.*

Ahora, volvamos al Teorema 1.7. Este teorema es una consecuencia del hecho que $\mathcal{S}_1$ sea unión finita de puntos e intervalos. Resulta que para los conjuntos definibles de dimensiones más grandes una caracterización similar se tiene, reemplazando los puntos e intervalos por objetos más generales, llamados celdas. En lo que sigue, si r es un entero no negativo, C^0 denotará la clase de funciones continuas, mientras que si $r > 0$ C^r denotará la clase de funciones con derivadas continuas de orden a lo sumo r. Por C^∞ denotaremos la clase de funciones suaves, y por C^ω la clase de funciones analíticas.

Definición 1.9 (Celdas). Sea r un entero no negativo, $r = \infty$ o $r = \omega$. Para $n \geq 1$ y $n \geq m \geq 0$ definimos la noción de una C^r celda m-dimensional en $\mathbb{R}^n$ inductivamente como sigue:

(1) (i) Una C^r-celda 0-dimensional en $\mathbb{R}$ es un conjunto de un elemento $\{a\}$ (para $a \in \mathbb{R}$).
    (ii) Una C^r-celda 1-dimensional en $\mathbb{R}$ es un intervalo abierto (a, b) (para $a, b \in \mathbb{R}, a < b$).
(2) Para $n \geq 2$, una C^r-celda $(m + 1)$-dimensional en $\mathbb{R}^n$ tiene las siguientes formas:
    (i) $\text{graph}(f)$, donde $f : C \to \mathbb{R}$ es una función definible de clase C^r y C es una C^r celda $(m + 1)$-dimensional en $\mathbb{R}^{n-1}$, o
    (ii) $(f, g)_C := \{(\mathbf{x}, y) \in \mathbb{R}^n : \mathbf{x} \in C \text{ y } f(\mathbf{x} < y < g(\mathbf{x}))\}$, donde $f, g : C \to \mathbb{R}$ son funciones definibles de clase C^r con $f(\mathbf{x}) < g(\mathbf{x})$ (para todo $\mathbf{x} \in C$) y C es una C^r-celda m-dimensional en $\mathbb{R}^{n-1}$.

Una C^∞-celda se dice una celda suave, y una C^ω-celda se dice una celda analítica.

Notemos que todo $X \in \mathcal{S}_1$ es una unión finita de C^r-celdas.

Definición 1.10 (Partición de celdas). Sea r un entero no negativo, $r = \infty$ o $r = \omega$. Una C^r-descomposición de $\mathbb{R}^m$ es una clase especial de partición de $\mathbb{R}^m$ en C^r-celdas. La definición es por inducción en m:

(1) Una C^r-descomposición de $\mathbb{R}$ es una colección

$$\{(-\infty, a_1), (a_1, a_2), \ldots, (a_k, +\infty), \{a_1\}, \ldots, \{a_k\}\} \tag{1.4}$$

donde $a_1 < \cdots < a_k$ son puntos en $\mathbb{R}$;

(2) Una C^r-descomposición de $\mathbb{R}^{m+1}$ es una partición finita de $\mathbb{R}^{m+1}$ en C^r-celdas A tales que el conjunto de proyecciones $\pi(A)$ es una descomposición de $\mathbb{R}^m$. (Aquí $\pi : \mathbb{R}^{m+1} \to \mathbb{R}^m$ es la proyección usual.)

Una C^r-descomposición $\mathcal{D}$ se dice una partición de un conjunto $S \subseteq \mathbb{R}^m$ si cada celda en $\mathcal{D}$ es o bien parte de S o es disjunta de S, en otras palabras, si S es una unión de celdas en $\mathcal{D}$.

Una C^∞-descomposición se dice una descomposición suave, y una C^ω se dice una descomposición analítica.

Ahora podemos enunciar la generalización del Theorem 1.7.

Teorema 1.11 (C^r-descomposición en celdas). *Sea $r \geq 0$ un entero no negativo.*

(I_m) Dados conjuntos definibles $A_1, \ldots, A_k \subseteq \mathbb{R}^m$ existe una descomposición de $\mathbb{R}^m$ en C^1-celdas particionando $A_1, \ldots, A_k$.

(II_m) Dada una función definible $f : A \to \mathbb{R}$, $A \subseteq \mathbb{R}^m$, existe una C^r-descomposición de $\mathbb{R}^m$ en C^r-celdas, particionando A, tal que cada restricción $f|_C : C \to \mathbb{R}$ es C^r para cada celda $C \subseteq A$ de la descomposición.

La prueba del Teorema 1.11 está dada en [**vdD98**, Chapter 3, § 2] para el caso $r = 0$ y en [**vdD98**, Chapter 7, § 3.2] para el caso $r = 1$, pero el argumento se generaliza para el caso C^r para todo $r \geq 1$ (ver los ejercicios en [**vdD98**, Chapter 7, § 3.3]).

Con el Teorema 1.11, podemos dar una definición natural para la dimensión de un conjunto definible $X \subseteq \mathbb{R}^n$.

Definición 1.12 (Dimension). La dimensión der un conjunto no vacío $X \subseteq \mathbb{R}^n$, que denotaremos por $\dim(X)$, se define como el mayor m tal que X contiene una C^0-celda[1] m-dimensional en $\mathbb{R}^n$

En particular, si $X \subseteq \mathbb{R}^n$ es un conjunto no vacío, $\dim(X) = 0$ si y sólo si X es finito, y $\dim(X) = n$ si y sólo si X contiene una C^0-celda abierta. Más aún, por el Teorema 1.11, para una función definible $f : A \subseteq \mathbb{R}^m \to \mathbb{R}$, existe un subconjunto definible $B_r \subseteq A$ tal que $f|_{B_r}$ es de clase C^r y dimensión $\dim(A \backslash B_r) = 0$. Notemos que esta noción de dimensión se comporta bien, ver [**vdD98**, Chapter 4].

Es importante notar que la prueba del Teorema 1.11 no implica que podemos tomar una partición en celdas suaves de un conjunto X. En efecto, en [**LGR09**] se construye una función $H : \mathbb{R} \to \mathbb{R}$ tal que la estructura $\mathbb{R}_H := (\mathbb{R}, <, 0, 1, +, -, \cdot, H)$ es o-minimal, y no admite una descomposición en celdas suaves de $\mathbb{R}^2$ que particione el gráfico de H. Sin embargo, muchas estructuras o-minimales admiten descomposiciones en celdas suaves, e incluso celdas analíticas. Ejemplos de estas últimas estructuras o-minimales son:

(I) El cuerpo real ordenado $\overline{\mathbb{R}}$.

(II) La expansión del cuerpo real ordenado por funciones analíticas restringidas $\mathbb{R}_{\text{an}}$.

(III) La expansión del cuerpo real ordenado por la exponencial $\mathbb{R}_{\exp}$.

(IV) La expansión del cuerpo real ordenado $(\mathbb{R}, <, 0, 1, +, -, \cdot, f_1, \ldots, f_r)$ y el análogo restringido $(\mathbb{R}, <, 0, 1, +, -, \cdot, \tilde{f}_1, \ldots, \tilde{f}_r)$, donde $f_1, \ldots, f_r : U \subseteq \mathbb{R} \to \mathbb{R}$ son una cadena Pfaffiana.

[1] La dimensión permanece igual si consideramos C^r-celdas para todo entero $r \geq 0$.

La descomposición en celdas analíticas de $\overline{\mathbb{R}}$ y $\mathbb{R}_{\text{an}}$ se sigue del teorema de Hironaka sobre la existencia de estratificaciones de Whitney con estratos analíticos para conjuntos sub-analíticos (para una prueba con teoría de modelos, ver [**DvdD88**, § 4]). La descomposición en celdas analíticas para $\mathbb{R}_{\text{exp}}$ se sigue también de un resultado análgo sobre estratificaciones (ver [**vdDM94, Loi94**]), o también del siguiente teorema.

Teorema 1.13 ([**Tho11**, Corollary 5.6]). *Sea* $(\mathbb{R}, <, 0, 1, +, -, \mathcal{F})$ *una estructura localmente polinomialmente acotada tal que* $\mathcal{F}$ *consiste de funciones en una variable suaves, que son analíticas salvo quizás en el* 0*. Entonces* $(\mathbb{R}, <, 0, 1, +, -, \mathcal{F})$ *tiene descomposición en celdas analíticas.*

Notemos que la descomposición en celdas analíticas en el ejemplo (IV) también se sigue del teorema anterior.

Antes de concluir esta sección, volvamos al hecho que en las estructuras o-minimales, los teoremas de finitud valen en una manera uniforme. Sea $S \subseteq \mathbb{R}^{m+n} = \mathbb{R}^m \times \mathbb{R}^n$ definible. Para cada $\mathbf{a} \in \mathbb{R}^m$ ponemos

$$S_{\mathbf{a}} := \{\mathbf{x} \in \mathbb{R}^n : (\mathbf{a}, \mathbf{x}) \in S\} \subseteq \mathbb{R}^n. \tag{1.5}$$

Vemos a. S como describiendo una familia de conjuntos $(S_{\mathbf{a}})_{\mathbf{a}\in\mathbb{R}^m}$. Una tal familia se llama una familia definible (de subconjuntos de $\mathbb{R}^n$, con espacio de parámetros $\mathbb{R}^m$). Los conjuntos $S_{\mathbf{a}}$ se llaman fibras de la familia. Resulta que cada fibra de una familia definible tiene su "complejidad" acotada.

Proposición 1.14. *Sea* $r \geq 0$ *un entero no negativo. Sea* $S \subseteq \mathbb{R}^m \times \mathbb{R}^n$ *definible. Entonces existe un número* $M_S \in \mathbb{N}$ *tal que para todo* $\boldsymbol{a} \in \mathbb{R}^m$ *el conjunto* $S_{\boldsymbol{a}} \subseteq \mathbb{R}^n$ *tiene una partición en a lo sumo* M_S C^r*-celdas.*

La prueba de la Proposición 1.14 está dada en [**vdD98**, Chapter 3, § 3.6] para el caso $r = 0$, pero la prueba se generaliza de manera directa.

CAPÍTULO 2

Alturas en cuerpos globales

1. Introducción y notaciones

El objetivo de este capítulo es recordar las propiedades de las alturas en cuerpos globales que vamos a requerir en los próximos capítulos. La mayor parte de la presentación es estándar, y puede encontrarse en [**BG06, HS00, Lan83**]. Sin embargo, también probamos algunos resultados que no encontramos en la literatura, principalmente cuando consideramos cuerpos funcionales.

En la sección 2, recordamos la teoría básica de valores absolutos, y entonces definimos normalizaciones para el conjunto de lugares de un cuerpo global para poder tener una fórmula del producto. Aquí, adoptamos la exposición en [**HS00, Lan83**], mostrando que los valores absolutos de un cuerpo funcional K de grado de trascendencia 1 sobre $\mathbb{F}_q$ definidos en términos de la curva propia íntegra asociada a K admiten una interpretación aritmética, análoga al caso de cuerpo de números.

Habiendo construido las normalizaciones de los lugares en un cuerpo global, definimos la altura de un punto afín o proyectivo con coordenadas en un cuerpo global. Como nuestras aplicaciones son de naturaleza aritmética, resulta natural considerar la altura multiplicativa absoluta en vez de la altura multiplicativa relativa, que usualmente se usa en el caso de cuerpos funcionales. Luego damos las propiedades básicas de la altura, proveyendo pruebas para los resultados que no pudimos encontrar en la literatura.

Finalmente, en la últimas sección proveemos variantes del lema de Siegel que usaremos en el próximo capítulo.

2. Cuerpos globales

Sea K un cuerpo. Diremos que K es un cuerpo global si:

- K es un cuerpo de números, i.e. una extensión finita de $\mathbb{Q}$, o
- K es un cuerpo funcional de una variable sobre un cuerpo finito, i.e. una extensión de cuerpos finita separable[1] de $\mathbb{F}_q(T)$ para algún q. Más aún, siempre vamos a asumir que el cuerpo de constantes de K es $\mathbb{F}_q$, i.e. $K \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$.

Vamos a usar la letra k para referirnos a cualquiera de los cuerpos $\mathbb{Q}, \mathbb{F}_q(T)$. Fijamos una clausura algebraica $\overline{k}$ de k y sea k^{sep} la respectiva clausura algebraica separable. Denotamos O_k para $\mathbb{Z}$ si $k = \mathbb{Q}$, o $\mathbb{F}_q[T]$ si $k = \mathbb{F}_q(T)$. El anillo de enteros[2] de K se define como la clausura entera de O_k en K. Como es usual, un primo en K será un ideal primo no nulo $\mathfrak{p} \subseteq O_K$. Si p es un primo debajo de $\mathfrak{p}$, entonces $e_{\mathfrak{p}|p}$ y $f_{\mathfrak{p}|p}$ denotarán el índice de ramificación y el índice de inercia

[1] Como es usual, si K es una extensión finita de $\mathbb{F}_q(T)$, existe $s(T) \in K$ tal que K es una extensión finita separable de $\mathbb{F}_q(s(T))$. Con lo que la hipótesis de separabilidad no es necesaria.

[2] Notemos que si K es un cuerpo funcional, entonces O_K depende del parámetro T. Por ejemplo, si tomamos $O_k = \mathbb{F}_q 1/T]$, las clausuras íntegras de O_k y $\mathbb{F}_q[T]$ en K serán diferentes

respectivamente. El anillo local de O_K en un primo $\mathfrak{p}$ es un anillo de valuación, que denotaremos $O_{(\mathfrak{p})}$. Denotamos su cuerpo residual $O_K/\mathfrak{p}$ por $\kappa(\mathfrak{p})$. El cuerpo residual $\kappa(\mathfrak{p})$ es finito; llamamos su cardinal la norma absoluta de $\mathfrak{p}$, y la denotamos por $N(\mathfrak{p})$. Más generalmente, si $I \subseteq O_K$ es un ideal no nulo, definimos la norma absoluta de I como O_K/I y la denotamos por $N(I)$. Si $x \in O_K \backslash \{0\}$, la denotamos $N(x) := N((x))$.

Cuando K es un cuerpo funcional, notemos que para todo primo $\mathfrak{p}$ en K tenemos $N(\mathfrak{p}) = q^{[O_K/\mathfrak{p}:\mathbb{F}_q]}$. El grado de $\mathfrak{p}$ es el número $\deg(\mathfrak{p}) := [O_K/\mathfrak{p} : \mathbb{F}_q]$.

Denotemos M_K para el conjunto de lugares v de K. Para cada $v \in M_K$ sea K_v la completación de K con respecto a v. Si O_v es el anillo de valuación de v en K_v, denotamos $\mathfrak{m}_v$ a su ideal maximal y k_v para el cuerpo residual $O_v/\mathfrak{m}_v$. En este caso pensamos a v como la correspondiente valuación discreta normalizada $v : K^\times \to \mathbb{Z}$.

Para cada $v \in M_K$ vamos a elegir un representante adecuado $|\cdot|_v$. Primero, supongamos que $K = k = \mathbb{Q}$.

- Si $v = \infty$, entonces $|\cdot|_\infty$ es el valor absoluto arquimediano usual de k.
- Si v se corresponde con un primo p, entonces $|\cdot|_p$ es el valor absoluto p-ádico. Para todo $x \in \mathbb{Q}^\times$, sea $v_p(x)$ la valuación p-ádica normalizada de x. Entonces $|x|_p = p^{-v_p(x)}$.

Ahora, supongamos que $K = k = \mathbb{F}_q(T)$.

- Si v se corresponde con un polinomio irreducible $p \in \mathbb{F}_q[T]$, entonces $|\cdot|_p$ es el valor p-ádico absoluto. Para todo $x \in \mathbb{F}_q(T)^\times$, sea $v_p(x)$ la valuación normalizada p-ádica en x. Entonces $|x|_p = q^{-v_p(x)\deg(p)}$.
- Si $v = \infty$ es el valor absoluto con $1/T \in \mathfrak{m}_v$, entonces $|\cdot|_\infty$ es el valor absoluto no arquimediano correspondiente a la valuación discreta normalizada en $1/T$. Para todo $x = \frac{f}{g} \in \mathbb{F}_q(T)$, definimos $|x|_\infty = q^{\deg(f)-\deg(g)}$.

Una consecuencia inmediata de la factorización única es que (k, M_k) es un cuerpo con fórmula del producto, concretamente:

(1) Todo $v \in M_k$, salvo finitas excepciones, es no arquimediano.
(2) Para todo $x \in k^\times$, tenemos que $|x|_v = 1$ para todos salvo finitos v.
(3) Para todo $x \in k^\times$, tenemos la fórmula del producto

$$\prod_{v \in M_K} |x|_v = 1. \tag{2.1}$$

Ahora vamos a extender los valores absolutos representando los lugares de M_k. Para esto, necesitamos recordar algunos resultados sobre la teoría de cuerpos completos. Comenzamos con el siguiente teorema fundamental.

Teorema 2.1 ([**Jac74**, Theorem 9.8, Theorem 9.9, Theorem 9.12]). *Sea $|\cdot|_v$ un valor absoluto no trivial en un cuerpo F tal que F es completo relativo a $|\cdot|_v$ y sea E/F una extensión finita. Entonces $|\cdot|_v$ puede extenderse de manera única a un valor absoluto $|\cdot|_w$ en E, y esta extensión está dada por la fórmula*

$$|a|_w := \left|N_{E/F}(a)\right|_v^{1/[E:F]}. \tag{2.2}$$

Más aún, E es completo relativo a $|\cdot|_w$.

Otro resultado fundamental es que hay finitas extensiones de un valor absoluto $|\cdot|$ en k a un valor absoluto en un cuerpo global K:

Teorema 2.2 ([**Jac74**, Theorem 9.14, Corollary in Page 568]). *Sea $|\cdot|$ un valor absoluto en F, $\widehat{F}$ la correspondiente completación de F, y sea E/F una extensión finita separable, digamos $E = F(u)$. Sean $f_1(X), \dots, f_h(X)$ los factores mónicos irreducibles de $f(x)$ en $\widehat{F}[X]$. Entonces hay exactamente h extensiones de $|\cdot|$ a valores absolutos en E. Las correspondientes completaciones son isomorfas a $E_j := \widehat{F}[X]/(f_j(X))$, $1 \le j \le h$, y $[E_j : \widehat{F}] = \deg(f_j(x))$. Además, $\sum_{j=1}^{h} [E_j : \widehat{F}] = [E : F]$.*

Ahora volvemos al contexto de cuerpos globales. Sea K un cuerpo global. Dado un lugar $v \in M_k$ representado por el valor absoluto normalizado $|\cdot|_v$ y un lugar $w \in M_K$ con $w|v$, para todo $x \in K$ definimos

$$\|x\|_w := \left|N_{K_w/k_v}(x)\right|_v^{1/[K:k]}, \tag{2.3}$$

Por el Teorema 2.1 sabemos que la restricción de $|N_{K_w/k_v}(x)|_v^{1/[K:k]}$ a K es un representante de w extendiendo $|\cdot|_v$. Del Teorema 2.2, deducimos $[K_w : k_v] \le [K : k]$, que implica que $\|\cdot\|_w$ es un valor absoluto representando w. De esta manera construimos representantes normalizados de los elementos en M_K, que satisfacen la fórmula del producto.

Proposición 2.3 ([**BG06**, Lemma 1.3.7., Proposition 1.4.2.]). *Sea K un cuerpo global y M_K el conjunto de lugares de K, con los representantes* (2.3)*.*

(a) Para todo $x \in k^\times$ e $y \in K^\times$, se tiene que

$$\sum_{w|v} \log \|x\|_w = \log \|x\|_v, \ \frac{1}{[K:k]} \sum_{w|v} \log \|y\|_w = \log \|N_{K/k}(x)\|_v. \tag{2.4}$$

(b) El cuerpo (K, M_K) satisface la fórmula del producto.

El conjunto de lugares $w \in M_K$ que se encuentran arriba del lugar $v = \infty \in M_k$ se llaman los lugares del infinito de K, y los denotamos por $M_{K,\infty}$. Llamamos al complemento $M_K \backslash M_{K,\infty}$ los lugares finitos de K, y los denotamos $M_{K,\text{fin}}$. Del Teorema 2.2 deducimos

Hecho 2.4. $|M_{K,\infty}| \le [K : k]$.

Si K es un cuerpo funcional, $M_{K,\infty}$ consiste de lugares no arquimedianos. Dado $w \in M_{K,\infty}$, definimos el grado de w, y lo denotamos $\deg(w)$, como el grado $[\mathcal{O}_w/\mathfrak{w} : \mathbb{F}_q]$.

Notemos que los valores absolutos normalizados (2.3) en los lugares $w \in M_K$ pueden computarse de otra manera. Sea K un cuerpo global, y sea $v \in M_{k,\text{fin}}$. Ya sabemos que v se corresponde con un ideal primo no nulo de $\mathcal{O}_k$. Sea $\mathfrak{p} \subseteq \mathcal{O}_K$ un primo sobre p, y para todo $x \in K^\times$ denotemos $v_\mathfrak{p}(x)$ para la valuación $\mathfrak{p}$-ádica en x. Entonces definimos

$$|x|_\mathfrak{p} := \begin{cases} p^{-v_\mathfrak{p}(x)/e_{\mathfrak{p}|p}} \text{ si } K \text{ es un cuerpo de números} \\ q^{-v_\mathfrak{p}(x)\deg(\mathfrak{p})/e_{\mathfrak{p}|p} f_{\mathfrak{p}|p}} \text{ si } K \text{ es un cuerpo funcional} \end{cases}. \tag{2.5}$$

Es fácil ver que $|\cdot|_\mathfrak{p}$ extiende el valor absoluto $|\cdot|_p$ a todo K. Concluimos que $|\cdot|_\mathfrak{p}$ se extiende a un valor absoluto en la completación $\mathfrak{p}$-ádica $K_\mathfrak{p}$, que extiende a $|\cdot|_p$ en la completación p-ádica k_p. Por el Teorema 2.1, concluimos que

$$|x|_\mathfrak{p} = \left|N_{K_\mathfrak{p}/k_p}(x)\right|_p^{1/[K_\mathfrak{p}:k_p]}. \tag{2.6}$$

Ahora, recordemos la siguiente propiedad de los índices de ramificación e inercia.

Teorema 2.5 ([**Jac74**, Proposition 9.3, Theorem 10.10]). *Sea K un cuerpo global, y sean $\mathfrak{p}, p$ y los valores absolutos $|\cdot|_{\mathfrak{p}}, |\cdot|_p$ como arriba. Sean $O_{(\mathfrak{p})}, O_{(p)}$ los anillos valuación de las completaciones $K_{\mathfrak{p}}$, k_p respectivamente. Entonces el índice de ramificación $e_{\mathfrak{p}|p}$ coincide con el índice $(|K^\times|_{\mathfrak{p}} : |k^\times|_p)$, y el índice de inercia $f_{\mathfrak{p}|p}$ coincide con el grado de extensión $[O_{(\mathfrak{p})/\mathfrak{p}} : O_{(p)}/p]$. Además, $e_{\mathfrak{p}|p} \cdot f_{\mathfrak{p}|p} = [K_{\mathfrak{p}:k_p}]$.*

Ahora, definamos

$$\|x\|_{\mathfrak{p}} := \mathcal{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)/[K:k]}. \tag{2.7}$$

Usando el Teorema 2.5, vemos que

$$|x|_{\mathfrak{p}}^{[K_{\mathfrak{p}}:k_p]/[K:k]} = \|x\|_{\mathfrak{p}}. \tag{2.8}$$

Resulta que los valores absolutos (2.5) se corresponden a todos los lugares en M_K que extienden el lugar asociado a $|\cdot|_p$:

Teorema 2.6 ([**Jac74**, Theorem 10.9]). *Sea K un cuerpo global. Sea p un primo en k, y supongamos que p se factoriza en K como $p = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$ con los $\mathfrak{p}_i$'s primos en K. Entonces los valores absolutos $|\cdot|_{\mathfrak{p}_i}$ son no equivalentes si $i \neq j$ y son las únicas extensiones de $|\cdot|_p$ a valores absolutos en K.*

El Teorema 2.6 nos permite asociar, para cada lugar $w \in M_K$ que no está encima de $\infty \in M_k$, un primo $\mathfrak{p}_w$ en K. Entonces, para todo $w \in M_K$ que está encima de $v \in M_k \backslash \{\infty\}$,(2.6) y (2.8) dan la expresión

$$\|x\|_w = |x|_{\mathfrak{p}_w}^{[K_{\mathfrak{p}_w}:k_{p_v}]/[K:k]} = \|x\|_{\mathfrak{p}_w} = \mathcal{N}(\mathfrak{p}_w)^{-v_{\mathfrak{p}_w}(x)/[K:k]}. \tag{2.9}$$

Ahora, sea $k = \mathbb{Q}$. Como $|\cdot|_\infty$ es un valor absoluto arquimediano, todo $w \in M_{K,\infty}$ debe ser un lugar arquimediano. Pero tales lugares son bien conocidos:

Teorema 2.7 ([**Jac74**, Teorema de Ostrowski, Page 552]). *Los únicos cuerpos que son completos relativos a un valor absoluto arquimediano son $\mathbb{R}$ o $\mathbb{C}$.*

Entonces $K_w \cong \mathbb{R}$ o $K_w \cong \mathbb{C}$, y

$$\|x\|_w = \begin{cases} |x|_\infty^{1/[K:k]} \text{ si } w \text{ es real} \\ |x|_\infty^{2/[K:k]} \text{ si } w \text{ es complejo} \end{cases}. \tag{2.10}$$

Más aún, de (2.10) obtenemos una correspondencia entre los lugares arquimedianos y las inmersiones de K:

- Los lugares reales de K están en biyección con los embeddings $\sigma : K \hookrightarrow \mathbb{R}$.
- Los lugares complejos de K están en biyección con el par de inmersiones complejas conjugadas $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$.

Finalmente, supongamos que $k = \mathbb{F}_q(T)$ y $w \in M_{K,\infty}$. Para poder computar $\|\cdot\|_w$, consideremos el anillo $O'_k = \mathbb{F}_q[1/T]$. Notemos que $1/T$ es un elemento primo en O'_k. Entonces podemos considerar la valuación $1/T$-ádica y el respectivo valor absoluto $|\cdot|_{1/T}$, dado por $|x|_{1/T} := q^{-v_{1/T}(x)}$. Notemos que si $x = \frac{f}{g}$ con $f, g \in \mathbb{F}_q[T]$, entonces $v_{1/T}(x) = \deg(g) - \deg(f)$, con lo que $|\cdot|_{1/T} = |\cdot|_\infty$. Concluimos que todo lugar $w \in M_K$ extendiendo a ∞ verificará la igualdad (2.9) para algún primo no nulo $\mathfrak{p}$ adecuado en la clausura íntegra de $\mathbb{F}_q[1/T]$ en K.

Concluimos esta sección con el resultado muy importante que dice que el anillo de enteros de un cuerpo global se realiza como la intersección de todos sus anillos de valuación.

Teorema 2.8 ([**Jac74**, Theorem 10.8, Page 615]). *Sea K un cuerpo global. Entonces*

$$\mathcal{O}_K = \bigcap_{v\in M_{K,fin}} \mathcal{O}_{(\mathfrak{p}_v)} = \bigcap_{v\in M_{K,fin}} \{x \in K : \|x\|_v \leq 1\} = \bigcap_{v\in M_{K,fin}} \{x \in K : \|x\|_{\mathfrak{p}_v} \leq 1\}. \tag{2.11}$$

Más aún, si $R \subsetneq K$ es un anillo de valuación conteniendo $\mathcal{O}_K$, entonces $R = \mathcal{O}_{(\mathfrak{p}_v)}$ para algún $v \in M_{K,fin}$.

Observación 2.9. Notemos que en la literatura hay otra definición para un primo (o lugar) en un cuerpo funcional K sobre $\mathbb{F}_q$ (ver [**Ros02, Sti09**]): un primo $\mathfrak{P}$ de K es el ideal maximal de algún anillo de valuación discreta $\mathcal{O}_{\mathfrak{P}}$ de K conteniendo $\mathbb{F}_q$, y el grado de $\mathfrak{p}$ se define como el grado de la extensión $[\mathcal{O}_K/\mathfrak{P} : \mathbb{F}_q]$. No es difícil de ver que un tal primo se corresponde, salvo finitas excepciones, con un ideal primo no nulo $\mathfrak{p} \subseteq \mathcal{O}_K$ de grado $[\mathcal{O}_{\mathfrak{p}} : \mathbb{F}_q]$, los primos excepcionales estando en correspondencia con los ideales primos arriba de $1/T$ en la clausura íntegra de $\mathbb{F}_q[1/T]$ en K.

Remark 2.10 (Cuerpos funcionales y curvas). Es importante notar que los cuerpos funcionales admiten una interpretación geométrica, que es útil. Sea k un cuerpo, no necesariamente $\mathbb{Q}$ o $\mathbb{F}_q(T)$. Existe una correspondencia entre cuerpos funcionales sobre k y curvas sobre k

Teorema 2.11 ([**GW10**, Theorem 15.22]). *Existe una equivalencia contravariante entre la categoría de curvas normales propias sobre k (con morfismos no constantes) y la categoría de cuerpos funcionales de grado de trascendencia* 1 *sobre k (con k-morfismos) dada por la asignación que aplica a una curva C a su cuerpo funcional $k(C)$.*

Bajo la correspondencia del Teorema 2.11, el cuerpo racional $k(T)$ se corresponde con la recta proyectiva $\mathbb{P}^1_k$. Más en general, sea K un cuerpo funcional de grado de trascendencia 1 sobre k. Existe T, trascendente sobre k, tal que la extensión $K/k(T)$ es finita. Definimos C como la normalización de la recta proyectiva $\mathbb{P}^1_k$, cuyo cuerpo funcional identificamos con $k(T)$, en K. Más explícitamente, sea $K_{\mathbb{P}^1_k}$ el haz constante con valor K en $\mathbb{P}^1_k$. Es una $\mathcal{O}_{\mathbb{P}^1_k}$-álgebra cuasi-coherente. Para todo abierto U de $\mathbb{P}^1_k$, definimos el haz $\mathcal{A}$ de $\mathcal{O}_{\mathbb{P}^1_k}$-subálgebras de $K_{\mathbb{P}^1_k}$ mediante

$$\Gamma(U, \mathcal{A}) := \{f \in \Gamma(U, K_{\mathbb{P}^1_k}) : f \text{ es íntegro sobre } \Gamma(U, \mathcal{O}_{\mathbb{P}^1_k})\}. \tag{2.12}$$

Ahora construimos un esquema mediante pegado. Para cualquier abierto afín $U \subseteq \mathbb{P}^1_k$, sea $f_U : \mathrm{Spec}(\Gamma(U, \mathcal{A})) \to U$ el morfismo inducido por la inclusión $\Gamma(U, \mathcal{O}_{\mathbb{P}^1_k}) \hookrightarrow \Gamma(U, \mathcal{A})$. Más aún, si $V \subseteq U$ es otro abierto afín de $\mathbb{P}^1_k$, definimos $\rho^U_V : \mathrm{Spec}(\Gamma(V, \mathcal{A})) \to \mathrm{Spec}(\Gamma(U, \mathcal{A}))$ como el morfismo inducido por la restricción $\Gamma(U, \mathcal{A}) \to \Gamma(V, \mathcal{A})$. Por [**GW10**, Proposition 3.10] podemos pegar los U-esquemas $f_U : \mathrm{Spec}(\Gamma(U, \mathcal{A})) \to U$ para obtener un $\mathbb{P}^1_k$-esquema $\pi : \mathrm{Spec}(\mathcal{A}) \to \mathbb{P}^1_k$ que satisface:

- para todo abierto afín $U \subseteq \mathbb{P}^1_k$ existe un isomorfismo $i_U : \pi^{-1}(U) \to \mathrm{Spec}(\Gamma(U, \mathcal{A}))$, y
- para toda elección $V \subseteq U \subseteq \mathbb{P}^1_k$ de abiertos afines la composición

$$\mathrm{Spec}(\Gamma(V, \mathcal{A})) \xrightarrow{i_V^{-1}} \pi^{-1}(V) \xrightarrow{inclusion} \pi^{-1}(U) \xrightarrow{i_U^{-1}} \mathrm{Spec}(\Gamma)(U, \mathcal{A})$$

  es el morfismo $\rho^U_V : \mathrm{Spec}(\Gamma(V, \mathcal{A})) \to \mathrm{Spec}(\Gamma(U, \mathcal{A}))$.

Sea $C = \mathrm{Spec}(\mathcal{A})$. Entonces se tiene:

Proposición 2.12 ([**GW10**, Proposition 12.43, Corollary 12.52, Corollary 13.82]). *La normalización $\pi : C \to \mathbb{P}^1_k$ satisface:*

(i) C es íntegra y normal, con cuerpo funcional $k(C) = K$.
(ii) El morfismo π es íntegro y suryectivo y $\dim(C) = 1$.
(iii) Sea $U \subseteq \mathbb{P}^1_k$ un subesquema abierto no vacío. Entonces la restricción $\pi^{-1}(U) \to U$ es la normalización de U en K.
(iv) C es finito sobre $\mathbb{P}^1_k$. En particular, C es propia.

Si tomamos $U_0 = D_+(X_0)$, $U_1 = D_+(X_1)$ y hacemos las identificaciones $\Gamma(U_0, \mathbb{P}^1_k) = k[T]$ y $\Gamma(U_1, \mathbb{P}^1_k) = k[1/T]$ entonces (2.12) toma la forma

$$\Gamma(U_0, \mathcal{A}) = \{f \in K : f \text{ es íntegra sobre } k[T]\} = \mathcal{O}_K, \tag{2.13}$$

$$\Gamma(U_1, \mathcal{A}) = \{f \in K : \text{ es íntegra sobre } k[1/T]\} = \tilde{\mathcal{O}}_K, \tag{2.14}$$

luego, tenemos las restricciones

$$\pi|^{U_0} : \operatorname{Spec}(\mathcal{O}_K) \to \operatorname{Spec}(k[T]),\ \pi|^{U_1} : \operatorname{Spec}(\tilde{\mathcal{O}}_K) \to \operatorname{Spec}(k[1/T]). \tag{2.15}$$

Habiendo construido una curva normal propia $C \to \mathbb{P}^1_k$ con $k(C) = K$, vamos a construir valores absolutos en K en una manera geométrica. Denotamos por C^1 el subconjunto de puntos cerrados de C. Recordamos que el grado de un punto cerrado $p \in C^1$ es el grado de la extensión de cuerpos $\deg(p) := [\kappa(p) : k]$, donde $\kappa(p)$ es el cuerpo residual en p. Vamos a usar:

Proposición 2.13 ([**GW10**, Proposition 5.4]). *Sea C una curva sobre k. Entonces existe una biyección entre los puntos cerrados de C y las órbitas de Galois de $X(\bar{k})$.*

Dado cualquier punto cerrado $p \in C^1$, para todo $f \in K^\times$, definimos la valuación $v_p(f)$ como el orden de f en cualquier punto en la órbita de Galois asociada. Es usual denotar $\operatorname{ord}_p(f) := v_p(f)$. Tenemos el valor absoluto asociado

$$|f|_p := c^{-\operatorname{ord}_p(f)\deg(p)},\ f \in K^\times, \tag{2.16}$$

donde c es un número fijo, $0 < c < 1$. Resulta que estos valores absolutos definen representantes de los lugares de K.

Teorema 2.14 ([**BG06**, Proposition 1.4.7]). *Los valores absolutos $|\cdot|_{p \in C^1}$ son no triviales y no equivalentes. Si M_C denota el conjunto de lugares con estos representantes, entonces (K, M_C) satisface la fórmula del producto.*

En este contexto la fórmula del producto significa que para toda función racional $f \in k(T)^\times$ tiene el mismo número de ceros y polos:

$$\sum_p \operatorname{ord}_p(f)\deg(p) = 0 \text{ for all } f \in k(T)^\times. \tag{2.17}$$

Ahora, veamos cómo estos valores absolutos están conectados a los que definimos al principio de esta sección, cuando $k = \mathbb{F}_q$. Elijamos $c = q^{-1}$ en (2.16). Supongamos que $C = \mathbb{P}^1_k$. Dado cualquier punto cerrado $p \in \mathbb{P}^1_k$, para todo $f \in k(T)$ definimos la valuación $v_p(f)$ como el orden de f en cualquier punto en la órbita asociada de Galois. Un punto en $\mathbb{P}^1(\bar{k})$ tiene coordenadas $(x_0 : x_1) \mapsto \frac{x_1}{x_0}$. Si $x_0 = 0$, ponemos $\infty = (0 : 1)$. Sea $x \in \mathbb{A}^1(\bar{k})$. Entonces existe un polinomio mónico, irreducible $p \in \mathbb{F}_q[T]$ el cuál tiene a x como una raíz. La órbita de Galois de x consiste

exactamente de las raíces de p, con lo que los puntos cerrados que no se encuentran en el infinito de $\mathbb{P}^1_k$ corresponden con polinomios mónicos irreducibles en $\mathbb{F}_q[T]$. Más aún, para todo conjugado z de x y para todo $f \in k(T)^\times$, $\mathrm{ord}_z(f)$ coincide con $v_p(f)$. Como $\kappa(x) = \mathrm{Frac}(\mathcal{O}_{\mathbb{P}^1_k,x}) = k[T]/p$, tenemos que $\deg(x) = \deg(p)$, el grado del polinomio p. Esto quiere decir que el valor absoluto (2.16) coincide con $|\cdot|_p$.

Ahora consideremos el punto ∞. Como este punto está definido en k, su órbita de Galois consiste de un sólo punto. Entonces $\deg(\infty) = 1$, y para todo $f \in k(T)^\times$ tenemos que $\mathrm{ord}_\infty(f) = \mathrm{ord}_{1/T} f(1/T)$ y $|\cdot|_\infty$ es el valor absoluto en el infinito que definimos al principio de esta sección.

En conclusión, los valores absolutos que definimos en una manera aritmética para $\mathbb{F}_q(T)$ coinciden con los valores absolutos (2.16) definidos en una manera geométrica, asociados a $\mathbb{P}^1_{\mathbb{F}_q}$.

Ahora, consideremos el caso general de una curva normal propia $\pi : C \to \mathbb{P}^1_k$. Sea U_0, U_1 el cubrimiento afín de $\mathbb{P}^1_k$ que definimos antes. Si $x \in C^1$, entonces $x \in \pi^{-1}(U_0)$ o $x \in \pi^{-1}(U_1)$. Supongamos que $x \in \pi^{-1}(U_0)$. Por (2.15), tenemos que x se corresponde con un primo no nulo $\mathfrak{p}$ de $\mathcal{O}_K$, lo cual implica que $\mathcal{O}_{C,x} = \mathcal{O}_{K_{(\mathfrak{p})}}$. En consecuencia, para todo $f \in K^\times$ la valuación $\mathrm{ord}_x(f)$ coincide con la valuación $\mathfrak{p}$-ádica $v_\mathfrak{p}(f)$, $\kappa(x) = \mathrm{Frac}(\mathcal{O}_{C,x}) = \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$ y entonces $\deg(x) = \deg(\mathfrak{p})$.

De la discusión anterior, podemos deducir que hay una correspondencia uno-uno entre puntos cerrados $x \in \pi^{-1}(U_0)$ y primos no nulos $\mathfrak{p}_x \subseteq \mathcal{O}_K$, tale que

$$|f|_x^{1/[K:k]} = \|f\|_{\mathfrak{p}_x} \text{ for all } f \in K^\times, \tag{2.18}$$

donde$\|\cdot\|_\mathfrak{p}$ es el valor absoluto (2.7). Una razonamiento similar se aplica a un punto $x \in U_1$ que se encuentra en la fibra $\pi^{-1}(p)$ con p el ideal primo $(1/T)k[1/T]$.

En conclusión, un cuerpo funcional separable K sobre $\mathbb{F}_q(T)$ se corresponde con una curva normal propia C sobre $\mathbb{F}_q$, y los valores absolutos (2.7) están relacionados con los valores absolutos (2.16) vía (2.18).

3. Alturas

3.1. Definición y propiedades básicas. De ahora en más, para todo cuerpo global K, elegimos representantes de M_K como en (2.3). Sea $\overline{k}$ una clausura algebraica separable de k, y sea $\mathbf{x} \in \mathbb{P}^n(\overline{k})$ con coordenadas proyectivas $(x_0 : \ldots : x_n)$ que se encuentran en una extensión finita separable K sobre k. La altura multiplicativa absoluta de $\mathbf{x}$ se define como

$$H(\mathbf{x}) := \prod_{v \in M_L} \max_{0 \le i \le n} \|x_i\|_v. \tag{2.19}$$

No es difícil de ver [**BG06**, Lemma 1.5.2, Lemma 1.5.3] que la altura de $\mathbf{x}$ es independiente del cuerpo de definición L y de la elección de las coordenadas, y es siempre al menos 1.

Dado un punto $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n(K)$, definimos su altura como

$$H(\mathbf{x}) := H(1 : \mathbf{x}) = H(1 : x_1 : \ldots : x_n) = \prod_{v \in M_K} \max_{1 \le i \le n} \{1, \|x_i\|_v\}. \tag{2.20}$$

En particular, para todo $1 \le i \le n$ y para todo $v \in M_K$ se tiene

$$\|x_i\|_v \le \prod_{\substack{v \in M_K \\ \|x_i\|_v \ge 1}} \|x_i\|_v \le \prod_{v \in M_K} \max\{1, \|x_i\|\} = H(x_i) \le \prod_{v \in M_K} \max_j \{1, \|x_j\|_v\} = H(1 : \mathbf{x}). \tag{2.21}$$

Algunas de las propiedades básicas de la altura multiplicativa son las siguientes.

Proposición 2.15. *Tenemos:*

(a) *Para todo* $x \in \overline{k}$, $H(x^m) = |m|H(x)$ *para todo* $m \in \mathbb{Z}$.

(b) *Para todo* $\boldsymbol{x} \in \mathbb{P}^n(\overline{k})$ *y para todo* $\boldsymbol{y} \in \mathbb{P}^m(\overline{k})$ *con coordenadas* $(x_i)_i$ *e* $(y_j)_j$ *respectivamente, consideremos el punto* $\boldsymbol{x} \otimes \boldsymbol{y} \in \mathbb{P}^{(n+1)(m+1)-1}(\overline{k})$ *con coordenadas* $(x_i y_j)_{i,j}$. *Entonces* $H(\boldsymbol{x} \otimes \boldsymbol{y}) = H(\boldsymbol{x})H(\boldsymbol{y})$.

(c) *Para todo* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r \in \mathbb{A}^n(\overline{k})$, *tenemos*

$$H\left(\sum_{i=1}^{r} \boldsymbol{x}_i\right) \leq r \prod_{i=1}^{r} H(\boldsymbol{x}_i). \tag{2.22}$$

Más aún, si M_K *no tiene lugares arquimedianos, la cota anterior vale sin el factor r.*

(d) *Sea* $\boldsymbol{x}$ *un punto en* $\mathbb{A}^n(\overline{k})$ *o* $\mathbb{P}^n(\overline{K})$ *con coordenadas* $(x_j)_j$. *Si* $\sigma \in Gal(\overline{k}/K)$ *y si* $\sigma(\boldsymbol{x})$ *está dado por las coordenadas* $(\sigma(x_j))_j$, *entonces* $H(\boldsymbol{x}) = H(\sigma(\boldsymbol{x}))$.

(e) *Sea* $S \subseteq M_K$ *un conjunto finito de lugares. Para todo* $x \in \overline{k}$ *se tiene. que vale la desigualdad fundamental:*

$$H(x)^{-1} \leq \prod_{v \in S} \|x\|_v \leq H(x). \tag{2.23}$$

Las demostraciones de las propiedades anteriores pueden encontrarse en [**BG06**, § 1.5] para $K = \mathbb{Q}$, pero las pruebas se extienden fácilmente al caso general.

Observación 2.16. Definimos la altura H en una clausura algebraica separable de k, porque estamos trabajando con cuerpos globales, pero esto no es necesario, ver [**BG06**, § 1.3.10, 1.4.6-1.4.13, 1.5.22].

Observación 2.17. Mientras que la altura multiplicativa se usa usualmente pues está definida sobre todo $\overline{\mathbb{Q}}$ y es independiente del cuerpo de definición de las coordenadas, en la literatura también es usada la noción de altura multiplicativa relativa de un punto. Si K es un cuerpo de números, para un lugar $v \in M_K$, definimos

$$|x|_v := \begin{cases} |x|_\infty \text{ if } v \text{ is real} \\ |x|_\infty^2 \text{ if } v \text{ is complex} \\ \mathcal{N}(\mathfrak{p}_v)^{-v_{\mathfrak{p}_v}(x)} \text{ if } v \text{ is non-archimedean} \end{cases}. \tag{2.24}$$

Si K es un cuerpo funcional, consideramos la curva normal propia asociada C y consideramos los valores absolutes (2.16) con $c = q^{-1}$. Para todo punto $\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$ la altura multiplicativa relativa de $\mathbf{x}$ es la cantidad

$$H_K(\mathbf{x}) = \prod_{v \in M_K} \max_i \{|x_i|_v\}. \tag{2.25}$$

De la definición de la altura multiplicativa absoluta y la Observación 2.10 concluimos que

$$H(\mathbf{x}) = H_K(\mathbf{x})^{1/[K:k]}. \tag{2.26}$$

Notemos que (2.17), luego de tomar logaritmos, toma la siguiente forma "geométrica" cuando K es un cuerpo funcional y $\mathbf{x} = (f_0 : \ldots f_n)$ con $f_i \in K = k(C)$:

$$h_K(\mathbf{x}) := \log_q(H_K(\mathbf{x})) = -\sum_{x \in C^1} \deg(x) \min_i \{\mathrm{ord}_x(f_i)\}. \tag{2.27}$$

En particular, si $f \in K^\times = k(C)^\times$, tenemos

$$h_K(f) := h_K(1 : f) = -\sum_{x \in C^1} \deg(x) \min\{0, \mathrm{ord}_x(f)\}. \tag{2.28}$$

Observación 2.18. Notemos que la altura de un cuerpo de números tiene una diferencia muy importante con la altura de un cuerpo funcional. Si K es un cuerpo global que es un cuerpo funcional, entonces la función altura H es muy esparsa. Más precisamente, la altura proyectiva de un punto $\mathbf{x} \in \mathbb{P}^n(K)$ es de la forma $q^{m/[K:k]}$, donde m es un entero positivo.

Sea $K = k$. De la definición de la altura, se sigue inmediatamente que $\mathcal{N}(x) = H(x)$ para todo $x \in O_k$. En el caso general, no tenemos una igualdad: si $K = \mathbb{Q}(\sqrt{3})$, entonces

$$\mathcal{N}(1 + \sqrt{3}) = N_{K/\mathbb{Q}}(1 + \sqrt{3}) = 2 > \sqrt{1 + \sqrt{3}} = H(1 + \sqrt{3}).$$

Sin embargo, tenemos una cota que se sigue de la desigualdad fundamental (Proposición 2.15 (e)).

Lema 2.19. *Sea $x \in O_K \backslash \{0\}$. Entonces*

$$\mathcal{N}(x) \leq H(x)^{[K:k]}. \tag{2.29}$$

Demostración. Sea $x = \prod_{i=1}^r \mathfrak{p}_i^{v_{\mathfrak{p}_i}(x)}$ la factorización por ideales primos en O_K y sea p_i el primo debajo de $\mathfrak{p}_i$. Entonces por (2.9)

$$\mathcal{N}(x)^{1/[K:k]} = \prod_{i=1}^r \mathcal{N}(\mathfrak{p}_i)^{v_{\mathfrak{p}_i}(x)/[K:k]} = \prod_{i=1}^r \|x^{-1}\|_{w_{\mathfrak{p}_i}}. \tag{2.30}$$

Por la Proposición 2.15 (e), de la desigualdad anterior concluimos

$$\mathcal{N}(x) \leq H(x)^{[K:k]}. \tag{2.31}$$

□

3.2. Cota para coordenadas afines. Para uso próximo, notemos que la altura afín y proyectiva de un punto puede acotarse en términos de las alturas afines de sus coordenadas; concretamente, si $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{k})$ con los x_i's contenidos en una extensión separable de k, entonces es fácil ver que

$$H(x_1 : \ldots : x_n) \leq H(1 : x_1 : \ldots : x_n) \leq \max_i\{H(x_i)\}^n. \tag{2.32}$$

Más aún, supongamos que $\mathbf{x}$ tiene sus coordenadas $x_i \in O_K$ para algún cuerpo global K. Por el Teorema 2.8, $\|x_i\|_v \leq 1$ para todo $v \in M_{K,\mathrm{fin}}$ y para todo i. Entonces (2.21), el Hecho (2.4) y el hecho que la altura es siempre al menos 1, deducimos que

$$H(1 : x_1 : \ldots : x_n) = \prod_{v \in M_{K,\infty}} \max_i\{1, \|x_i\|_v\} \leq \prod_{v \in M_{K,\infty}} \max_i\{H(x_i)\} \leq \max_i\{H(x_i)\}^{[K:k]}. \tag{2.33}$$

Notemos que la desigualdad (2.33) es más fuerte que (2.32) cuando n es más grande que $[K : k]$.

De (2.32) y (2.33), vemos que si un punto $\mathbf{x} \in \mathbb{P}^n(K)$ admite coordenadas con altura pequeña, entonces la altura proyectiva de $\mathbf{x}$ es pequeña. Para nuestros propósitos, necesitamos un recíproco de este resultado, que probamos en el siguiente lema.

Lema 2.20. *Sea K un cuerpo global de grado $d = [K : k]$. Entonces, todo $\boldsymbol{x} \in \mathbb{P}^n(K)$ de altura proyectiva a lo sumo N admite coordenadas $(y_0 : \ldots : y_n)$ con $y_i \in \mathcal{O}_K$ para todo $1 \leq i \leq n$ e $\|y_i\|_w \leq N^{dn+1}$ para todo $w \in M_K$. En particular,*

$$H(1 : y_0 : \ldots : y_n) \leq N^{(dn+1)d}. \tag{2.34}$$

Si bien el Lema 2.20 es estándar, no pudimos encontrar una referencia en la literatura. En el caso de cuerpos de números, el Lema 2.20 se sigue fácilmente de la interpretación de la altura en términos de la medida de Mahler de un polinomio; ver la Observación 2.21. Esto sin embargo no funciona para cuerpos funcionales. Por este motivo, incluimos una prueba que contempla tanto el caso de cuerpos de números como el de cuerpos funcionales.

Demostración. Sea $\mathbf{x} \in \mathbb{P}^n(K)$ con $H(\mathbf{x}) \leq N$. Existen coordenadas $(x_0 : \ldots : x_n)$ con $x_i \in K$ para todo $0 \leq i \leq n$ y $x_{i_0} = 1$ para algún $0 \leq i_0 \leq n$. Podemos suponer que $i_0 = 0$ y $\mathbf{x} = (1 : x_1 : \ldots : x_n)$. Para algún j tal que $x_j \neq 0$, sea S_j el conjunto de $w \in M_K$ con $\|x_j\|_w > 1$. Para cualquier tal lugar la cota (2.21) implica

$$\|x_j\|_w \leq H(\mathbf{x}) \leq N \text{ para todo } j = 1, \ldots, n, \text{ y todo } w \in S_j. \tag{2.35}$$

Ahora, sea $w \in M_{K,\mathrm{fin}} \cap S_j$ y $\mathfrak{p}_w$ el correspondiente primo en $\mathcal{O}_K$. Sea $v_w \in M_k$ el lugar debajo de w y p_w el correspondiente primo en $\mathcal{O}_k$. Definimos $a_{j,w} := -v_{\mathfrak{p}_w}(x_j) f_{\mathfrak{p}_w|p_w}$, $z_{j,w} := p_w^{a_{j,w}}$ y $z_j = \prod_{w \in S_j} z_{j,w}$. Por lo tanto (2.9) implica que para todo $w \in M_{K,\mathrm{fin}}$ se tiene

$$\|z_j \cdot x_j\|_w \leq \|z_{j,w}\|_w \cdot \|x_j\|_w \leq 1. \tag{2.36}$$

Como $\|x_j\|_w \leq 1$ para todo $w \notin S_j$ y por construcción, $z_j \in \mathcal{O}_k$, deducimos $\|z_j \cdot x_j\|_w \leq 1$ para todo $w \in M_{K,\mathrm{fin}}$, lo cuál significa que $z_j \cdot x_j \in \mathcal{O}_K$.

Ahora, sea $w \in M_{K,\infty}$. Como $z \in \mathcal{O}_k$, tenemos

$$\|z_j\|_w = \|z_j\|_\infty^{\frac{[K_w:k_\infty]}{d}} = \left(\prod_{w' \in S_j} \|z_{j,w'}\|_\infty^{\frac{1}{d}} \right)^{[K_w:k_\infty]} = \left(\prod_{w' \in S_j} \|p_{w'}\|_\infty^{\frac{a_{j,w'}}{d}} \right)^{[K_w:k_\infty]}. \tag{2.37}$$

Si $k = \mathbb{Q}$, entonces $\|p_{w'}\|_\infty = |p_{w'}|$ y $\mathcal{N}(\mathfrak{p}_{w'}) = |p_{w'}|^{[\mathcal{O}_K/\mathfrak{p}_{w'} : \mathcal{O}_k/p_{w'}]} = \|p_{w'}\|_\infty^{f_{\mathfrak{p}_{w'}|p_{w'}}}$. Si $k = \mathbb{F}_q(T)$, entonces $\|p_{w'}\|_\infty = q^{\deg(p_{w'})} = q^{[\mathcal{O}_k/p_{w'} : \mathbb{F}_q]}$ y

$$\mathcal{N}(\mathfrak{p}_{w'}) = q^{[\mathcal{O}_K/\mathfrak{p}_{w'} : \mathbb{F}_q]} = q^{[\mathcal{O}_K/\mathfrak{p}_{w'} : \mathcal{O}_k/p_{w'}][\mathcal{O}_k/p_{w'} : \mathbb{F}_q]} = \|p_{w'}\|_\infty^{f_{\mathfrak{p}_{w'}|p_{w'}}}.$$

Reemplazando $a_{j,w'} = -v_{\mathfrak{p}'_w}(x_j) f_{\mathfrak{p}_{w'}|p_{w'}}$ en (2.37), usando la cota $[K_w : k_\infty] \leq d$, la identidad (2.9) y el Teorema 2.15 (e), concluimos

$$\|z_j\|_w \leq \left(\prod_{w' \in S_j} \mathcal{N}(\mathfrak{p}_{w'})^{-\frac{v_{\mathfrak{p}_{w'}}(x_j)}{d}} \right)^{[K_w:k_\infty]} \leq \prod_{w' \in S_j} \|x_j\|_{w'}^d \leq H(x_j)^d. \tag{2.38}$$

Como $\|x_j\| \leq H(x_j) \leq N$, de (2.38) concluimos $\|z_j\|_w \leq N^d$. Ahora, definamos $z = \prod_{j=1}^n z_j$. Tenemos $\|z \cdot x_j\|_w \leq 1$ para todo $w \in M_{K,\mathrm{fin}}$ y $\|z \cdot x_j\|_w \leq N^{dn+1}$ para todo $w \in M_{K,\infty}$. Si $y_0 = z$ e $y_j = z \cdot x_j$, concluimos que $(y_0 : \ldots : y_n)$ es un conjunto de coordenadas de $\mathbf{x}$ que satisfacen el Lema 2.20. Más aún,

$$H(1 : y_0 : \ldots : y_n) = \prod_{w \in M_{K,\infty}} \max\{1, |y_i|_w\} \leq N^{(dn+1)d}. \tag{2.39}$$

□

Observación 2.21. La idea de la prueba del Lema 2.20 es limpiar los denominadores de cada coordenada de $\mathbf{x}$. Podemos conseguir esto de una manera "más sencilla" si K es un cuerpo de números de grado d. En efecto, sea $x \in K$ y $f = \sum_{i=0}^{d} a_i T^i = a_d(T-\alpha_1)\cdots(T-\alpha_d)$ el polinomio minimal de x sobre $\mathbb{Z}$. Por [**BG06**, Proposition 1.6.5], sabemos que

$$H(x)^d = |a_d| \prod_{j:|\alpha_j|\geq 1} |\alpha_j|, \tag{2.40}$$

donde $|\cdot|$ es el valor absoluto euclideano de $\mathbb{C}$. Notemos que $a_d x \in O_K$, y $H(x)^d \geq |a_d|$. Si $\mathbf{x} = (1 : x_1 : \ldots : x_n)$ con $x_i \in K$ para todo i, y verifica $H(\mathbf{x}) \leq N$, entonces $H(x_i) \leq N$, y para cualquier i tal que $x_i \neq 0$, existe $a_i \in \mathbb{Z}\backslash\{0\}$ tal que $|a_i| \leq H(x_i)^d \leq N^d$ y $a_i \cdot x_i \in O_K$. Tomando $a = \prod_{i=1}^{n} a_i$, $y_0 = a$, $y_i = a x_i$ para todo i, obtenemos coordenadas proyectivas $(y_0 : \ldots : y_n)$ para $\mathbf{x}$ que satisfacen el Lema 2.20.

3.3. Comportamiento de la altura bajo polinomios. Vamos a necesitar entender el comportamiento de la altura proyectiva bajo funciones polinomiales. Si bien esto podríamos hacerlo usando la teoría de alturas de Weil, para nuestros propósitos la siguiente proposición sencilla será suficiente.

Proposición 2.22. *Sea $\phi : \mathbb{P}^n \to \mathbb{P}^m$ una función racional de grado d definida sobre $\bar{k}$, $\phi = (f_0, \ldots, f_m)$ con f_i polinomios homogéneos de grado d, y sea $Z \subseteq \mathbb{P}^n$ el subconjunto de ceros comunes de los f_i's. Notemos que ϕ está definida en $\mathbb{P}^n\backslash Z$. Entonces*

$$H(\phi(\boldsymbol{x})) \leq RH(\boldsymbol{a})H(\boldsymbol{x})^d \text{ para todo } \boldsymbol{x} \in \mathbb{P}^n(\bar{k})\backslash Z, \tag{2.41}$$

donde R es el máximo número de monomios apareciendo en los f_i, y $\boldsymbol{a}$ es el punto proyectivo con coordenadas los coeficientes de todos los f_i.

Se puede encontrar una prueba de esta proposición en [**HS00**, Proposition B.2.5 (a)] para cuerpos de números, pero la misma prueba sirve para cuerpos funcionales.

Como corolario de esta proposición, obtenemos una cota superior para altura afín de la imagen de una función polinomial.

Corolario 2.23. *Sea $P(T_1, \ldots, T_n) = \sum_{(i_1,\ldots,i_n)} c_{i_1,\ldots,i_n} T_1^{i_1} \cdots T_n^{i_n} \in K[T_1, \ldots, T_n]\backslash\{0\}$, $\boldsymbol{c} = (c_{i_1,\ldots,i_n})_{(i_1\ldots,i_n)}$. Sea R el número de $(i_1, \ldots, i_n)$ con $c_{i_1,\ldots,i_n} \neq 0$. Entonces para todo $\boldsymbol{x} \in \mathbb{A}^n(K)$ tenemos*

$$H(P(\boldsymbol{x})) \leq RH(1 : \boldsymbol{c})H(1 : \boldsymbol{x})^{\deg(P)}. \tag{2.42}$$

Demostración. Sea $Q(T_0, \ldots, T_n) = T^{\deg(P)} P(\frac{T_1}{T_0}, \ldots, \frac{T_n}{T_0})$ la homogenicación de P. Aplicando la Proposicioń 2.22 a $\phi(x_0, \ldots, x_n) = (x_0^{\deg(P)} : Q(x_0, \ldots, x_n))$ concluimos que

$$H(x_0^{\deg(P)} : Q(x_0, \ldots, x_n)) \leq RH(1 : \mathbf{c})H(x_0 : \ldots : x_n)^{\deg(P)}. \tag{2.43}$$

Luego, arribamos a la conclusión deseada evaluando en $(1 : x_1 : \ldots : x_n)$. □

3.4. Teorema de Northcott. Es trivial que el conjunto de números racionales de altura acotada es acotado. Cuando K es un cuerpo global, el mismo resultado vale, y es un teorema de Northcott; ver [**HS00**, Theorem B.2.3] para una prueba para cuerpos de números que también funciona para cuerpos globales que son cuerpos funcionales. Sin embargo, para nuestros propósitos, requrimos una versión cuantitativa del teorema de Northcott, que enunciamos en el próximo teorema.

Teorema 2.24 (K cuerpo de números: [**Sch79**]; K cuerpo funcional: [**Wan92**]). *Sea K un cuerpo global de grado d, sea $n \geq 1$ un entero, y sea*

$$N_K(\mathbb{P}^n(K), T) = \begin{cases} |\{\boldsymbol{x} \in \mathbb{P}^n(K) : H_K(\boldsymbol{x}) \leq T\}| \text{ if } K \text{ is a number field} \\ |\{\boldsymbol{x} \in \mathbb{P}^n(K) : H_K(\boldsymbol{x}) = T\}| \text{ if } K \text{ is a function field} \end{cases}.$$

Entonces, existe una constante explícita $a(K, n) > 0$ tal que

$$N(\mathbb{P}^n(K), T) = a(K, n)T^{(n+1)} + O(T^{(n+1)-\frac{1}{d}}). \tag{2.44}$$

En particular, si

$$N(\mathbb{P}^n(K), T) = \begin{cases} |\{\boldsymbol{x} \in \mathbb{P}^n(K) : H(\boldsymbol{x}) \leq T\}| \text{ if } K \text{ is a number field} \\ |\{\boldsymbol{x} \in \mathbb{P}^n(K) : H(\boldsymbol{x}) \leq T\}| \text{ if } K \text{ is a function field} \end{cases},$$

entonces, existe una constante explícita $a'(K, n) > 0$ tal que

$$N(\mathbb{P}^n(K), T) = a'(K, n)T^{d(n+1)} + O(T^{d(n+1)-1}). \tag{2.45}$$

4. Construcción de polinomios auxiliares

4.1. Una variante del lema de Siegel para cuerpos globales. Uno de los pasos importantes del método polinomial es construir polinomios de baja complejidad que se anulen en un conjunto de puntos. Vamos a hacer esto construyendo un tal polinomio de la misma manera que en [**Wal14, Wal12**], probando una variación del lema de Siegel, que incluye tanto el caso de cuerpo de números como el de cuerpo funcional. Notemos que para cuerpos de números, podemos usar el resultado de Bombieri-Vaaler [**BV83**, Corollary 11] (ver también § 4.2), o incluso un resultado más elemental como [**BG06**, Corollary 2.9.2]. Debido a la falta de una referencia para el cuerpo funcional, damos una prueba válida para ambos casos.

Lema 2.25. *Sea K un cuerpo global con $[K : k] = d$. Sean $(a_{ij})_{i,j}$, $1 \leq i \leq s$, $1 \leq j \leq t$ elementos de O_K con $H(a_{ij}) \leq C$ para todo i, j. Supongamos que $t > 2d^2 s$. Entonces, existe $\boldsymbol{x} = (c_1, \ldots, c_t) \in O_K^t \backslash \{0\}$, tal que*

$$H(1 : \boldsymbol{c}) \ll_K (tC^d)^{\frac{2d^2 s}{t-2d^2 s}} \tag{2.46}$$

y

$$\sum_{j=1}^{t} c_j a_{ij} = 0 \text{ for all } 1 \leq i \leq s. \tag{2.47}$$

Demostración. Sea $h \geq 1$ un parámetro a elegir más adelante. Sean $N(\mathcal{O}_K, h)$ y $N(K, h)$ respectivamente el número de puntos en $\mathcal{O}_K$ y K de altura a lo sumo h. Hay $N(\mathcal{O}_K, h)^t$-tuplas $(c_1, \ldots, c_t)$ con $H(c_i) \leq h$ par atodo $1 \leq i \leq t$. Para cualquier tal elección, (2.33) y el Corolario 2.23 implican

$$H\left(\sum_{j=1}^{t} c_j a_{ij}\right) \leq tH(1 : \mathbf{c})H(1 : a_{i1} : \ldots : a_{it}) \leq t(hC)^d. \tag{2.48}$$

Entonces, hay $N(\mathcal{O}_K, t(hC)^d)^s$ posibles configuraciones para todas las sumas $\sum_{j=1}^{t} c_j a_{ij}$. Si

$$N(\mathcal{O}_K, h)^t \gg_K (N(\mathcal{O}_K, (t(hC)^d)))^s, \tag{2.49}$$

entonces existen dos tuplas $\mathbf{c}_1, \mathbf{c}_2 \in [h]^t_{\mathcal{O}_K} \backslash \{0\}$, $\mathbf{c}_1 = (c_1^{(1)}, \ldots, c_t^{(1)})$, $\mathbf{c}_2 = (c_1^{(2)}, \ldots, c_t^{(2)})$, $\mathbf{c}_1 \neq \mathbf{c}_2$ tales que

$$\sum_{j=1}^{t} c_j^{(1)} a_{ij} = \sum_{j=1}^{t} c_j^{(2)} a_{ij} \text{ for all } 1 \leq i \leq s, \tag{2.50}$$

y $\mathbf{c} = \mathbf{c}_1 - \mathbf{c}_2$ satisface (2.47). Como $H(x+y) \leq 2H(x)H(y)$ para todo $x, y \in \overline{k}$, tenemos $H(c_j^{(1)} - c_j^{(2)}) \leq 2h^2$ para todo $1 \leq j \leq t$. Entonces la desigualdad (2.33) da la cota $H(1 : \mathbf{c}) \leq (2h^2)^d$. Veremos que existe un h adecuado tal que se cumple (2.49), y que para esta elección de h, $\mathbf{c}$ satisface (2.46) . Notemos que

$$N(\mathcal{O}_K, h)^t \geq (N_{\mathcal{O}_k}, h)^t \text{ and } N(K, (t(hC)^d))^s > N(\mathcal{O}_K, (t(hC)^d))^s. \tag{2.51}$$

Es fácil ver que $N(\mathcal{O}_k, h) \sim_k h$. Ahora, por el Teorema 2.24, $N(K, h) \sim_K h^{2d}$. Por lo tanto, eligiendo h tal que

$$h^t \gg_K (t(hC)^d)^{2ds}, \tag{2.52}$$

concretamente,

$$h \sim_K (tC^d)^{\frac{2ds}{t-2d^2 s}}, \tag{2.53}$$

entonces $N(\mathcal{O}_k, h)^t \geq N(K, (t(hC)^d))^s$. Esto, junto con (2.51), implican (2.49) y (2.46). □

4.2. Puntos de altura pequeña en subespacios. Para el Capítulo 2 necesitaremos encontrar puntos de altura pequeña en un espacio vectorial fijo. Vamos a hacer esto mediante una generalización del lema de Siegel, siguiendo [**BV83, Thu95, RT96**]. Primero definimos la altura de Arakelov de un punto $\mathbf{x} \in \mathbb{P}^n(\overline{k})$. Dado $w \in M_K$ y $v \in M_k$ el lugar debajo de w, para cualquier $\mathbf{x} = (x_0, \ldots, x_n) \in (K_v)^{n+1}$ definimos

$$H_v(x) = \begin{cases} \max_{0 \leq i \leq n} \{\|x_i\|_v\}^{[K_w : k_v]/[K:k]} \text{si } w \in M_{K,\text{fin}} \\ \left(\sum_{i=0}^{n} \|x_i\|_v^2\right)^{[K_w : k_v]/2[K:k]} \quad \text{si } w \in M_{K,\infty} \end{cases}. \tag{2.54}$$

Entonces la altura de Arakelov de $\mathbf{x} \in \mathbb{P}^n(K)$ es

$$H_{\text{Ar}}(\mathbf{x}) = \prod_{w \in M_K} H_w(\mathbf{x}). \tag{2.55}$$

Debido a la fórmula del producto, la altura de Arakelov está bien definida, y es fácil de ver que no depende de la elección de coordenadas de $\mathbf{x}$. Más aún, la definición de $H_{\text{Ar}}(\mathbf{x})$ no depende en la

extensión. K, i.e. $H_{\mathbf{Ar}}$ es una función bien definida en $\mathbb{P}^n(\overline{k})$. También, es fácil de probar que para todo $\mathbf{x} \in \mathbb{P}^n(\overline{k})$, se tiene

$$H(\mathbf{x}) \leq H_{\mathrm{Ar}}(\mathbf{x}) \leq \sqrt{n+1}H(\mathbf{x}). \tag{2.56}$$

Sea r un entero positivo. Dado un anillo conmutativo R escribimos $\bigwedge^r(R^n)$ para la potencia exterior r-ésima de R^n. Sea $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ la base canónica de R^n. Si $r \leq n$, ponemos $M = \binom{n}{r}$ e identificamos $\bigwedge^r(R^n)$ con R^M vía el morfismo de R-módulos que aplica los productos $\mathbf{e}_{i_1} \wedge \cdots \wedge \mathbf{e}_{i_r}$ con $1 \leq i_1 < \cdots < i_r \leq n$ a la base canónica de R^M, de acuerdo al orden lexicográfico. Entonces podemos definir las funciones (2.54) en $\bigwedge^r((K_v)^n)$ para todo $v \in M_K$.

Sea $V \subseteq \overline{k}^n$ un k-subespacio vectorial. Si V es de dimensión 1, definimos la altura de Arakelov de V, y la denotamos $H_{\mathrm{Ar}}(V)$, como la altura de Arakelov $H_{\mathrm{Ar}}(\mathbf{x})$, donde $\mathbf{x}$ es cualquier elemento no nulo de V. En general, si $V \subseteq \overline{k}^n$ es un subespacio de dimensión $m \geq 1$, entonces $\bigwedge^m V$ es un subespacio de dimensión 1 de $\bigwedge^m \overline{k}^n$ y ponemos

$$H_{\mathrm{Ar}}(V) = H\left(\bigwedge^m V\right). \tag{2.57}$$

Si $V = \{0\}$, definimos $H_{\mathrm{Ar}}(V) = 1$. Notemos que la altura $H_{\mathrm{Ar}}(V)$ posee la siguiente propiedad útil. Sea $\langle\cdot\rangle : K^n \times K^n \to K$ la forma bilineal dada por

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i, \text{ for all } \mathbf{x} := (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n). \tag{2.58}$$

Dado un subespacio $V \subseteq \overline{k}^n$, denotemos $V^\perp$ para el subespacio de $\overline{k}^n$ ortogonal a V, i.e. el subespacio de $\mathbf{x} \in \overline{k}^n$ tal que $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ para todo $\mathbf{y} \in V$. Se tiene:

Teorema 2.26 ([**Thu93**, Duality Theorem]). *Para todo subespacio $V \subseteq \overline{k}^n$, se tiene*

$$H(V^\perp) = H(V). \tag{2.59}$$

Ahora volvemos al problema de hallar puntos de altura pequeña en un espacio vectorial. La generalización del lema de Siegel que usaremos es el siguiente teorema.

Teorema 2.27 ([**BV83**, Corollary 11], [**Fuk10**, Theorem 1.2.]). *Dado un cuerpo global K, existe una constante positiva $C(K)$ tal que vale lo siguiente. Sea $V \subseteq \overline{k}^n$ un subespacio de dimensión $m > 0$ definido sobre K. Entonces existe una base $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$ de V en K^n tal que*

$$\prod_{i=1}^{m} H(\boldsymbol{x}_i) \leq \prod_{i=1}^{m} H(1 : \boldsymbol{x}_i) \leq C(K)^m H_{Ar}(V). \tag{2.60}$$

En particular, existe un vector no nulo $\boldsymbol{x} \in K^n$ tal que

$$H(\boldsymbol{x}) \leq H(1 : \boldsymbol{x}) \leq C(K) H_{Ar}(V)^{1/m}. \tag{2.61}$$

CAPÍTULO 3

Conjuntos mal distribuidos en cuerpos globales

1. Introducción

El propósito de este capítulo es generalizar resultados conocidos sobre las propiedades de los conjuntos de enteros mal distribuidos al nivel de clases residuales para muchos módulos primos. Más precisamente, vamos a probar una versión en cuerpos globales del siguiente principio:

PROBLEM 3.1 (Problema Inverso de Criba). *Supongamos que tenemos un conjunto $S \subseteq \{1, \dots, N\}^d$ ocupando muy pocas clases residuales módulo p para muchos primos p. Entonces, o bien S es pequeño, o posee una estructura algebraica robusta.*

Siguiendo la explicación en [**Wal12**], un tal resultado inverso de criba es de mucho interés en teoría de números. El Problema 3.1 permanece abierto para $d = 1$. En [**HV09**], Helfgott y Venkatesh prueban el caso $d = 2$ del Problema 3.1 usando el método del determinante de Bombieri-Pila para obtener una generalización de dimensión 2 de la criba más grande. Para todo $d \geq 2$, en [**Wal12**] Walsh resuelve el Problema 3.1. Más precisamente, él prueba el siguiente resultado

TEOREMA 3.2 (Walsh, [**Wal12**, Theorem 1.1]). *Seam $0 \leq k < d$ enteros y sean $\varepsilon, \alpha, \eta > 0$ números reales positivos. Entonces, existe una constante C dependiendo sólo de los parámetros anteriores, tal que para todo conjunto $S \subseteq \{1, \dots, N\}^d$ ocupando a lo sumo αp^k clases residuales para todo primo p se tiene al menos una de las siguientes:*

(i) (S es pequeño) $|S| \ll_{d,k,\varepsilon,\alpha} N^{k-1+\varepsilon}$,

(ii) (S es robustamente algebraicos) Existe un polinomio $f \in \mathbb{Z}[X_1, \dots, X_d]$ de grado a lo sumo C y coeficientes acotados por N^C anulándose en más de $(1-\eta)|S|$ puntos de S.

La idea en [**Wal12**] para probar el Teorema 3.2 sigue el esquema del método polinomial: primero, encontramos un "subconjunto característico" X de S, i.e. un conjunto tal que todo polinomio de complejidad pequeña que se anula en X debe también anularse en una proporción positiva de S. Entonces, por argumentos de contar dimensionales, encontramos un polinomio de complejidad pequeña que se anula en X. Como X era un subconjunto característico, esto fuerza a que el polinomio se anule en una proporción positiva de S.

Una pregunta natural es si el Teorema 3.2 puede mejorarse, en el sentido que un conjunto ocupando pocas clases residuales siempre posee algún tipo de estructura algebraica, i.e. si satisface el Teorema 3.2 (ii). En [**Wal12**] está probado que existen conjuntos $S \subseteq \{1, \dots, N\}^d$ de tamaño $|S| \gg N^{k-1}$ ocupando menos de p^k clases residuales para todo primo p pero que no poseen estructura algebraica. Sin embargo, Walsh muestra que todo $S \subseteq \{1, \dots, N\}^d$ de tamaño $|S| \gg N^{\varepsilon}$ ocupando pocas clases residuales para muchos primos p, que verifica ciertas condiciones de regularidad, debe satisface el Teorema 3.2 (ii).

Si bien no se puede esperar que un conjunto mal distribuido sea fuertemente algebraico como en el Teorema 3.2 (ii), Walsh en [**Wal14**] probó que tales conjuntos siempre poseen algún tipo

de estructura algebraica. Para poder enunciar su resultado recordamos la noción de complejidad usada en [**Wal14**]. Un polinomio no nulo tiene complejidad a lo sumo C en $\{1,\dots,N\}^d$ si tiene grado a lo sumo C y sus coeficientes están acotados por N^C.

Teorema 3.3 ([**Wal14**, Theorem 1.2]). *Sea $S \subseteq \{1,\dots,N\}^d$ ocupando $\ll p^\kappa$ clases residuales para todo primo p y algún número real $0 \leq \kappa < d$. Entonces, para todo $\varepsilon > 0$, existe $P \in \mathbb{Z}[X_1,\dots,X_d]$ no nulo de complejidad $\ll_{\kappa,d,\varepsilon} (\log(N))^{\frac{\kappa}{d-\kappa}}$ anulándose en al menos $(1-\varepsilon)|S|$ puntos de S.*

El Teorema 3.3 es ajustado al exponente; en [**Wal14**] se prueba que para toda elección de $0 \leq \kappa < d$, existe algún $c > 0$ y un conjunto $S \subseteq \{1,\dots,N\}^d$ satisfaciendo las hipótesis del resultado, pero tal que no hay ningún polinomio de complejidad a lo sumo $(\log(N))^c$ anulándose en una proporción positiva de este conjunto.

La prueba del Teorema 3.3 también sigue el método polinomial, pero a diferencia del Teorema 3.2, donde la construcción del subconjunto característico es más bien delicada, aquí se usa un argumento de muestreo aleatorio.

El objetivo de esta sección es proveer una generalización del Teorema 3.3 en el contexto de cuerpos globales, reemplazando $\mathbb{Z}$ con el anillo de enteros O_K, con K un cuerpo global. El análogo diofantino correcto de $\{1,\dots,N\}$ deberían ser los elementos de O_K de altura afín $H(x)$ a lo sumo N. Notemos a este conjunto como $[N]_{O_K}$. Ahora tenemos una noción obvia de complejidad de un polinomio definido sobre O_K. Decimos que un polinomio no nulo $P \in O_K[X_1,\dots,X_n]$ tiene complejidad a lo sumo C en $[N]^n_{O_K}$ si tiene grado a lo sumo C y sus coeficientes tienen altura afín acotada por N^C.

Generalizamos en una manera directa la noción de conjuntos mal distribuidos al nivel de clases residuales. Para un ideal primo $\mathfrak{p} \subseteq O_K$, y un conjunto $X \subseteq O_K^n$, notemos $X_\mathfrak{p}$ al conjunto de clases residuales de X módulo $\mathfrak{p}$:

$$X_\mathfrak{p} = \{(x_1,\dots,x_n) \mod (\mathfrak{p}) : (x_1,\dots,x_n) \in X\}. \tag{3.1}$$

Siguiendo la misma estrategia de Walsh, probamos la siguiente generalización del Teorema 3.3.

Teorema 3.4 ([**Par19**, Theorem 1.7]). *Sea $X \subseteq [N]^n_{O_K}$ ocupando $\ll \mathcal{N}(\mathfrak{p})^\kappa$ clases residuales para todo primo $\mathfrak{p}$ y algún número real $0 \leq \kappa < n$. Entonces, para todo $\varepsilon > 0$ existe $P \in O_K[X_1,\dots,X_d]$ no nulo de complejidad $\ll_{K,\kappa,n,\varepsilon} (\log(N))^{\frac{\kappa}{n-\kappa}}$ anulándose en al menos $(1-\varepsilon)|X|$ puntos de X.*

Como en el Teorema 3.3, el Teorema 3.4 es ajustado al exponente; De hecho, nosotros probamos un teorema más general que el Teorema 3.4 donde consideramos puntos racionales de altura acotada que están contenidos en una variedad proyectiva. Vamos a formular este resultado en la próxima sección. En el proceso de la prueba del Teorema 3.4, obtenemos una versión efectiva del teorema de normalización de Noether, la cuál creemos que puede ser de interés.

2. Notación

Antes de probar el resultado principal, que implicará el Teorema 3.4, introduciremos notaciones y definiciones convenientes. Empezamos con la generalización de la caja $[N] = \{1,\dots,N\}$:

Notación 3.5. Dado un cuerpo global K y un entero positivo N, denotamos:

$$[N]^n_{O_K} := \{\mathbf{x} = (x_1,\dots,x_n) \in O_K^n : \max_i\{H(x_i)\} \leq N\},$$

$$[N]_K^n := \{\mathbf{x} = (x_1, \ldots, x_n) \in K^n : \max_i\{H(x_i)\} \leq N\},$$
$$[N]_{\mathbb{A}^n(K)} := \{\mathbf{x} = (x_1, \ldots, x_n) \in K^n : H(1 : x_1 : \ldots : x_n) \leq N\},$$
$$[N]_{\mathbb{P}^n(K)} := \{\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K) : H(x_0 : \ldots : x_n) \leq N\}.$$

2.1. Reducción módulo un primo. Sea $\mathfrak{p} \subseteq O_K$ un primo, y consideremos $\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$. Dado que $O_\mathfrak{p}$ es un anillo de valuación discreta, si $x_i \neq 0$ podemos escribir $x_i = a_i u^{v_\mathfrak{p}(x_i)}$ con $a_i \in O_\mathfrak{p}^\times$ y u un elemento uniformizador de $O_\mathfrak{p}$. Sea $v = \min\{v_p(x_i) : x_i \neq 0\}$ y denotemos por i_0 al índice que alcanza este mínimo. Ahora, para todo $0 \leq i \leq n$, sea $x_i' = 0$ si $x_i = 0$, o $x_i' = u^{-v} x_i$ caso contrario. Entonces $\mathbf{x}$ admite coordenadas $(x_0' : \ldots : x_n')$, las cuáles verifican que son cero o $v_\mathfrak{p}(x_i') \geq 0$ para todo i, y $v_\mathfrak{p}(x_{i_0}') = 0$. Además, si $(y_0 : \ldots : y_n)$ es otro conjunto de coordenadas para $\mathbf{x}$ e $(y_0' : \ldots : y_n')$ son las coordenadas obtenidas mediante el "limpiado de denominadores" como hicimos con $(x_0 : \ldots : x_n)$, es claro que $x_i' = 0$ si y sólo si $y_i' = 0$, y caso contrario, $v_\mathfrak{p}(x_i') = v_\mathfrak{p}(y_i')$. En particular, $(y_0', \ldots, y_n') = (\lambda x_0', \ldots, \lambda x_n')$ con $\lambda \in K$ y $v_\mathfrak{p}(\lambda) = 0$. Podemos escribir esto como:

Hecho 3.6. Dado un primo $\mathfrak{p}$ en K, todo $\mathbf{x} \in \mathbb{P}^n(K)$ admite coordenadas $(x_0 : \ldots : x_n)$ tales que para todo i, $x_i = 0$ o $v_\mathfrak{p}(x_i) \geq 0$, y existe $0 \leq i_0 \leq n$ con $v_\mathfrak{p}(x_{i_0}) = 0$. Más aún, otro sistema de coordenadas que satisface esta condición difiere por un múltiplo $\lambda \in O_\mathfrak{p}^\times$.

Para todo primo $\mathfrak{p} \subseteq O_K$, definimos la función reducción módulo $\mathfrak{p}$ $\pi_\mathfrak{p} : \mathbb{P}^n(K) \to \mathbb{P}^n(O_K/\mathfrak{p})$ como sigue. Dado $\mathbf{x} \in \mathbb{P}^n(K)$, elegimos coordenadas como en le Hecho 3.6. En particular, para cada i, tiene sentido tomar la reducción de x_i módulo $\mathfrak{p}$, i.e. ver la imagen de x_i bajo la reducción $O_\mathfrak{p} \to O_\mathfrak{p}/\mathfrak{p} \cong O_K/\mathfrak{p}$. Entonces definimos $\pi_\mathfrak{p}(\mathbf{x})$ como el punto en $\mathbb{P}^n(O_K/\mathfrak{p})$ con coordenadas $(x_0 \mod (\mathfrak{p}) : \ldots : x_n \mod (\mathfrak{p}))$. Que esta función está bien definida es consecuencia de la "unicidad" del Hecho 3.6.

Será natural usar la siguiente notación.

Notación 3.7. Para todo $\mathbf{x}, \mathbf{x}' \in \mathbb{P}^n(K)$, denotamos $\mathbf{x} \equiv \mathbf{x}' \mod (\mathfrak{p})$ si $\pi_\mathfrak{p}(\mathbf{x}) = \pi_\mathfrak{p}(\mathbf{x}')$.

Notemos que la reducción módulo $\mathfrak{p}$ satisface la siguiente propiedad, análoga al hecho que los polinomios preservan clases residuales.

Hecho 3.8. Sea $P(T_0, \ldots, T_n) \in O_K[T_0, \ldots, T_n]$ un polinomio homogéneo no nulo. Sean $\mathbf{x}, \mathbf{x}' \in \mathbb{P}^n(K)$ con $\mathbf{x} \equiv \mathbf{x}' \mod (\mathfrak{p})$. En particular, si $(x_0, \ldots, x_n)$ y $(x_0' : \ldots : x_n')$ son coordenadas de $\mathbf{x}$ y $\mathbf{x}'$ respectivamente, entonces existe $\lambda \in O_K$ tal que $x_i \equiv \lambda x_i' \mod (\mathfrak{p})$ para todo i. Entonces $P(\mathbf{x}) \equiv \lambda^{\deg(P)} P(\mathbf{x}') \mod (\mathfrak{p})$. En consecuencia, si $\mathbf{x}'$ verifica $P(\mathbf{x}) \equiv 0 \mod (\mathfrak{p})$, tenemos $P(\mathbf{x}') \equiv 0 \mod (\mathfrak{p})$.

Observación 3.9 (Manera alternativa de definir la reducción módulo un primo). Sea K un cuerpo global y O_K su anillo de enteros. Existe un conjunto de lugares finito $S \subseteq M_K$ tal que el anillo de S-unidades $O_{K,S}$ es un dominio de ideales principales. Luego, todo elemento $\mathbf{x} \in \mathbb{P}^n(K)$ admite coordenadas $(x_0 : \ldots : x_n)$ tal que su máximo común divisor es trivial. Más aún, esta elección de coordenadas es único salvo un escalar $\lambda \in O_{K,S}^\times$. Por lo tanto, para todo primo $\mathfrak{p} \notin S$ se tiene que $(x_0 \mod (\mathfrak{p}) : \ldots : x_n \mod (\mathfrak{p}))$ define un elemento en $\mathbb{P}^n(O_{K,S}/\mathfrak{p})$. Usando la identificación $O_{K,S}/\mathfrak{p} \cong O_K/\mathfrak{p}$, arribamos a la reducción módulo $\mathfrak{p}$ $\pi_\mathfrak{p} : \mathbb{P}^n(K) \to \mathbb{P}^n(O_K/\mathfrak{p})$, que coincide con la función que definimos anteriormente. El único inconveniente con esta definición es que funciona para todo primo $\mathfrak{p}$ salvo finitas excepciones.

Habiendo definido las funciones reducción, es natural definir un "conjunto mal distribuido" de $\mathbb{P}^n(K)$ como un conjunto tal que su imagen bajo la reducción $\pi_\mathfrak{p}$ es pequeña, para muchos primos $\mathfrak{p}$. Por este motivo, será conveniente usar la siguiente notación.

Notación 3.10. Para todo ideal primo no nulo $\mathfrak{p} \subseteq O_K$, y todo conjunto $X \subseteq \mathbb{P}^n(K)$, denotamos $X_\mathfrak{p} := \pi_\mathfrak{p}(X)$.

Notemos que si $X \subseteq \mathbb{P}^n(K)$, entonce spara todo primo $\mathfrak{p}$ in K, $|X_\mathfrak{p}| \ll_n \mathcal{N}(\mathfrak{p})^n$.

2.2. Complejidad y conjuntos mal distribuidos. Consideremos $Z \subseteq \mathbb{P}^n(\bar{k})$ una variedad proyectiva definida sobre un cuerpo global K, con ideal homogéneo $I(Z)$ generado por polinomios homogéneos $f_1, \dots, f_l \in O_K[T_0, \dots, T_m]$, con lo que $Z = V(f_1, \dots, fl)$. Llamemos $\dim(Z)$ a la dimensión de Z como variedad. Sea $M > 0$ un número real tal que $l < M$, $\dim(Z) < M$ y $\deg(f_i) < M$ para todo i. Supongamos que Z es geométricamente irreducible. Entonces, el teorema de Bertini-Noether [**FJ08**, Proposition 10.4.2, Corollary 10.4.3(a)] nos dice que para todos salvo finitos primos $\mathfrak{p}$ de K la reducción $Z_\mathfrak{p} := V(\tilde{f}_1, \dots, \tilde{f}_l)$, donde $\tilde{f}_i$ denota la reducción módulo $\mathfrak{p}$ de f_i, permanece geométricamente irreducible y $\dim(Z_\mathfrak{p}) = \dim(Z) < M$.

Debido a la estimación de Lang-Weil, la reducción $Z_\mathfrak{p}$ tiene $(1+O_M(\mathcal{N}(\mathfrak{p})^{-1/2}))\mathcal{N}(\mathfrak{p})^{\dim(Z)}$ clases residuales par casi todo primo $\mathfrak{p}$. El resultado principal de este capítulo es un teorema que afirma que un conjunto mal distribuido en Z tiene algún tipo de estructura algebraica, con respecto a la variedad Z. Para poder formular precisamente este resultado, adaptamos la noción de estructura, adaptamos la noción de estructura algebraico para subconjuntos en $Z(K, N) := Z(K) \cap [N]_{\mathbb{P}^n(K)}$. Esto requiere extender la definición de complejidad de un polinomio dada en [**Wal14, Wal12**].

Definición 3.11. Sea $P \in O_K[T_0, \dots, T_m]$ un polinomio no nulo. Decimos que P tiene complejidad a lo sumo C en $[N]^n_{O_K}$ si su grado tiene a lo sumo C y sus coeficientes tienen altura afún a lo sumo N^C. Más en general, sea $Z \subseteq \mathbb{P}^n(\bar{k})$ una variedad proyectiva definida sobre K. Decimos que un polinomio homogéneo $P \in O_K[T_0, \dots, T_m]$ que no se anula en Z, tiene complejidad a lo sumo C si existe un polinomio no nulo homogéneo $Q \in O_K[Y_0, \dots, Y_{\dim(Z)}]$ de complejidad a lo sumo C y un cambio de variables polinomial $Y_i = L_i(T_0, \dots, T_m)$, $1 \le i \le \dim(Z)$, con $P(T_0, \dots, T_m) = Q(L_0(T_0, \dots, T_m), \dots, L_{\dim(Z)}(T_0, \dots, T_m))$.

Cuando $Z = \mathbb{P}^n(\bar{k})$, la noción de complejidad coincide con la complejidad de un polinomio homogéneo no nulo $P \in O_K[T_0, \dots, T_n]$.

Ahora enunciamos el resultado principal de este capítulo, que generaliza [**Wal12**, Theorem 1.3].

Teorema 3.12 ([**Par19**, Theorem 3.2]). *Sea $Z \subseteq \mathbb{P}^m(\bar{k})$ una variedad proyectiva definida sobre un cuerpo global K con ideal de definición homogéneo $I(Z)$ generado por $f_1, \dots, f_l \in O_K[T_0, \dots, T_m]$, y llamemos $n = \dim(Z)$. Supongamos que Z es geométricamente irreducible. Para todo $n > 0$, todo número real $0 \le \kappa < n$, existe $\tau = \tau(n, \kappa, K, Z) \ge 1$ tal que lo siguiente vale. Sea I el intervalo real $[\tau(\log(N))^{\frac{n}{n-\kappa}}, 2\tau(\log(N))^{\frac{n}{n-\kappa}}]$. Escribamos $\mathcal{P}_{I,K}$ para el conjunto de ideales primos $\mathfrak{p} \subseteq O_K$ definido como*

$$\mathcal{P}_{I,K} := \begin{cases} \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) \in I \text{ si } K \text{ es un cuerpo de números} \\ \{\mathfrak{p} \subseteq O_K : \mathcal{N}(\mathfrak{p}) = \tau(\log(N))^{\frac{n}{n-\kappa}}\} \text{ si } K \text{ es un cuerpo funcional} \end{cases}.$$

Entonces, para todo $X \subseteq Z(K, N)$ con $|X_\mathfrak{p}| \ll \mathcal{N}(\mathfrak{p})^\kappa$ para todo primo $\mathfrak{p} \in \mathcal{P}_{I,K}$, y todo $\varepsilon > 0$ existe un polinomio homogéneo no nulo $P \in O_K[T_0, \dots, T_m]$ que no se anula en Z, tiene complejidad $\ll_{\kappa,n,m,\varepsilon,K,Z} (\log(N))^{\frac{n}{n-\kappa}}$ y se anula en al menos $(1-\varepsilon)|X|$ puntos de X.

En la próxima sección, veremos que cuando $K = \mathbb{Q}$ y $Z = \mathbb{P}^m(\overline{\mathbb{Q}})$, el Teorema 3.12 implica [**Wal12**, Theorem 1.5]. También, vamos a ver que el Teorema 3.12 es ajustado al exponente.

Observación 3.13 (Mala distribución luego de extender el cuerpo base). Sea $X \subseteq [N]^n_{O_K}$ un conjunto tal que X ocupa pocas clases residuales para muchos primos. Entonces es fácil de ver que X permanece mal distribuido en cualquier cuerpo global K' extendiendo K, i.e. viendo a X como subconjunto de $[N]^n_{O_K}$, X ocupa pocas clases residuales para muchos primos. En particular, de ser necesario, podemos asumir que la extensión K/k tiene alguna propiedad específica, e.g. es de Galois y tiene grado suficientemente grande.

3. Prueba del Teorema 3.12

Como en el esquema del método polinomial, la prueba del Teorema 3.12 consistirá de dos pasos: construir un conjunto característico, y construir un polinomio que se anula en dicho conjunto. Para poder realizar lo segundo, vamos a requerir realizar un cambio de variables adecuados, siendo una de las maneras posibles de hacerlo mediante el teorema de normalización de Noether.

3.1. Construcción del conjunto característico. Introducimos la cantidad

$$r = \eta(\log(N))^{\frac{n\kappa}{n-\kappa}}, \tag{3.2}$$

donde $\eta \geq 1$ es una constante a ser elegida después. Notemos que para todo $c > 0$,

$$r \leq N^{r^c} \tag{3.3}$$

para N suficientemente grande, dependiente en n, κ pero independente de η.

Proposición 3.14. *Sea $X \subseteq Z(K, N)$ con $|X_{\mathfrak{p}}| \leq \alpha \mathcal{N}(\mathfrak{p})^\kappa$ para todo ideal primo $\mathfrak{p} \in \mathcal{P}_{I,K}$. Entonces existen una constante positiva $C_1 = C_1(\alpha, \kappa)$, conjuntos $C, X' \subseteq X$ de tamaño $|C| \leq r$, $|X'| \gg |X|$, tales que si $\eta \geq C_1 \tau^\kappa$, entonces para todo $\boldsymbol{x} \in X'$ tenemos*

$$\sum_{\mathfrak{p} \in \mathcal{P}_{I,K}} 1_{\exists \boldsymbol{c} \in C : \boldsymbol{x} \equiv \boldsymbol{c} \mod (\mathfrak{p})} \log(\mathcal{N}(\mathfrak{p})) \gg_K |I|, \tag{3.4}$$

donde $|I| = \tau(\log(N))^{\frac{n}{n-\kappa}}$.

Notemos que si K es un cuerpo de números, entonces $|I|$ es la longitud del intervalo I.

Demostración. La prueba es exactamente la misma que en [**Wal12**, Proposition 3.1]. La incluimos por completitud. Llamemos $(x, L) \in X \times X^r$ una tupla buena módulo $\mathfrak{p}$ si existe una coordenada de L tal que su reducción módulo $\mathfrak{p}$ coincide con la reducción módulo $\mathfrak{p}$ de $\mathbf{x}$. Denotemos $X_{\text{good},\mathfrak{p}}$ para el conjunto de tuplas buenas módulo $\mathfrak{p}$. Nuestro conjunto C será construido como el conjunto de coordenadas de un $L \in X^r$ tal que $(x, L) \in X_{\text{good},\mathfrak{p}}$ para todo $\mathbf{x} \in X$ para muchos primos $\mathfrak{p} \in \mathcal{P}_{I,K}$. Para poder realizar esta construcción primero vamos a probar que para un primo fijo $\mathfrak{p} \in \mathcal{P}_{I,K}$ el conjunto $X_{\text{good},\mathfrak{p}}$ es grande.

Para toda clase residual $\mathbf{a}$ en $Z_{\mathfrak{p}}$, denotemos $X_{\mathbf{a}}$ a la probabilidad de $\mathbf{x} \in X$ tal que $\mathbf{x} \equiv \mathbf{a} \mod (\mathfrak{p})$. Para encontrar muchos (x, L) los cuales son buenos módulos $\mathfrak{p}$ es suficientemente mostrar que la probabilidad de que una tupla (x, L) no sea buena módulo $\mathfrak{p}$ sea pequeña. En otras palabras, es suficiente dar una cota superior $c < 1$ para

$$\sum_{\mathbf{a} \in Z_{\mathfrak{p}}} X_{\mathbf{a}}(1 - X_{\mathbf{a}})^r. \tag{3.5}$$

Si sumamos sobre los $\mathbf{a}$'s tales que $X_{\mathbf{a}} > 1/r$, entonces obtenemos la cota superior $(1-1/r)^r$. Como esta cantidad tiende a e^{-1} cuando $r \to +\infty$, para N grande (dependiente en n y κ), tenemos que

$$\sum_{\mathbf{a}\in Z_{\mathfrak{p}}: X_{\mathbf{a}} > 1/r} X_{\mathbf{a}}(1-X_{\mathbf{a}})^r \leq c_1 < 1 \tag{3.6}$$

para alguna constante positiva c_1. Ahora, si sumamos sobre los $\mathbf{a}$'s tales que $X_{\mathbf{a}} \leq 1/r$, entonces tomando en consideración que $X_{\mathfrak{p}}$ tiene a lo sumo $\alpha \mathcal{N}(\mathfrak{p})^\kappa$ elementos para todo primo $\mathfrak{p} \in \mathcal{P}_{I,K}$, tenemos

$$\sum_{\mathbf{a}\in Z_{\mathfrak{p}}: X_{\mathbf{a}} \leq 1/r} X_{\mathbf{a}}(1-X_{\mathbf{a}})^r \leq \sum_{\mathbf{a}\in Z_{\mathfrak{p}}, X_{\mathbf{a}} \leq 1/r} \frac{1}{r}\cdot 1 \leq \frac{\alpha}{r}\mathcal{N}(\mathfrak{p})^\kappa \leq \frac{\alpha(2\tau(\log(N))^{\frac{n}{n-\kappa}})^\kappa}{\eta(\log(N))^{\frac{n\kappa}{n-\kappa}}} \leq \frac{2^\kappa \alpha \tau^\kappa}{\eta} \leq \frac{1-c_1}{2}, \tag{3.7}$$

donde la última desigualdad puede obtenerse si imponemos la condición

$$\eta \geq C_1 \tau^\kappa \tag{3.8}$$

para alguna constante explícita C_1, dependiente en α y κ. Combinando (3.6) y (3.7) obtenemos la cota superior $c := c_1 + \frac{1-c_1}{2} < 1$ para (3.5). En otras palabras, $|X_{\text{good},\mathfrak{p}}| \geq (1-c)|X|^{r+1}$. Notemos que la constante c es efectiva, e independiente de $\mathfrak{p}$.

Del hecho que $|X_{\text{good},\mathfrak{p}}| \geq (1-c)|X|^{r+1}$, se sigue que:

Hecho 3.15. Para todo ideal primo $\mathfrak{p} \in \mathcal{P}_{I,K}$ existen constantes absolutas c_1 y c_2, ambas independientes de $\mathfrak{p}$, tales que para al menos $c_1|X|^r$ elecciones de $L \in X^r$, existen al menos $c_2|X|$ elementos de $\mathbf{x} \in X$ para las cuales $(x, L) \in X_{\text{good},\mathfrak{p}}$.

En efecto, supongamos que esto falla. Entonces, para algún $\mathfrak{p} \in \mathcal{P}_{I,K}$ y para toda elección de constantes positivas c_1, c_2, tenemos a lo sumo $c_1|X|^r$ elecciones para $L \in X^r$ tales que existen al menos $c_2|X|$ elementos de $\mathbf{x} \in X$ para los cuales $(x, L) \in X_{\text{good},\mathfrak{p}}$. Llamemos $\mathcal{L}$ al conjunto de $L \in X^r$ tales que $(\mathbf{x}, L) \in X_{\text{good},\mathfrak{p}}$. Entonces $\mathcal{L}$ tiene a lo sumo $c_1|X|^r$ elementos. Recordando que ya probamos la cota $|X_{\text{good},\mathfrak{p}}| \geq (1-c)|X|^{r+1}$, tenemos que

$$\begin{aligned}(1-c)|X|^{r+1} \leq |X_{\text{good},\mathfrak{p}}| &\leq |\{(\mathbf{x}, L) \in X_{\text{good},\mathfrak{p}} : L \in \mathcal{L}\}| + |\{(\mathbf{x}, L) \in X_{\text{good},\mathfrak{p}} : L \notin \mathcal{L}\}| \\ &\leq c_1 c_2 |X|^{r+1} + (1-c_1)c_2|X|^{r+1}.\end{aligned} \tag{3.9}$$

Tomando c_1 y c_2 suficientemente pequeños arribamos a una contradicción.

Decimos que un elemento $L \in X^r$ es bueno módulo $\mathfrak{p}$ si $(\mathbf{x}, L)$ es bueno módulo $\mathfrak{p}$ para al menos $c_2|X|$ elementos $\mathbf{x} \in X$. Denotemos $\mathcal{L}_{\mathfrak{p}}$ al conjunto de tales L's. El hecho 3.15 implica que para todo ideal primo $\mathfrak{p} \in \mathcal{P}_{I,K}$ tenemos $|\mathcal{L}_{\mathfrak{p}}| \geq c_1|X|^r$, por lo tanto tenemos

$$\sum_{\mathfrak{p}\in\mathcal{P}_{I,K}} |\mathcal{L}_{\mathfrak{p}}| \geq c_1|X|^r|\mathcal{P}_{I,K}|. \tag{3.10}$$

Se sigue que debe existir algún L' tal que $L' \in \mathcal{L}_{\mathfrak{p}}$ para al menos $c_1|\mathcal{P}_{I,K}|$ ideales primos en $\mathcal{P}_{I,K}$.

Por construcción, tenemos

$$\sum_{\mathbf{x}\in X} \left|\{\mathfrak{p} \in \mathcal{O}_{I,K} : (\mathbf{x}, L') \in \mathcal{L}_{\mathfrak{p}}\}\right| \geq c_1 c_2 |X||\mathcal{P}_{I,K}|. \tag{3.11}$$

Concluimos que existen constantes positivas c_3, c_4 y un subconjunto $X' \subseteq X$ de tamaño $|X'| \geq c_3|X|$, tales que para todo $\mathbf{x} \in X'$ hay al menos $c_3|\mathcal{P}_{I,K}|$ ideales primos $\mathfrak{p} \in \mathcal{P}_{I,K}$ para los cuales $(\mathbf{x}, L') \in \mathcal{L}_{\mathfrak{p}}$.

Tomemos C como el conjunto de coordenadas de L', con lo que C tiene a lo sumo r elementos. Como $\mathcal{N}(\mathfrak{p}) \geq |I| = \tau(\log(N))^{\frac{n}{n-\kappa}}$, tenemos que para todo $\mathbf{x} \in X'$ debe tenerse

$$\sum_{\mathfrak{p}\in\mathcal{P}_{I,K}} 1_{\exists \mathbf{c}\in C:\mathbf{x}\equiv\mathbf{c} \mod(\mathfrak{p})} \log(\mathcal{N}(\mathfrak{p})) \geq c_3|\mathcal{P}_{I,K}|\log(|I|). \tag{3.12}$$

Si K es un cuerpo de números, usamos el Teorema del Ideal de Landau para obtener $|\mathcal{P}_{I,K}| \sim_K \frac{|I|}{\log(|I|)}$. Reemplazando esta cota en (3.12), concluimos la Proposición 3.14. Supongamos ahora que K es un cuerpo funcional sobre $\mathbb{F}_q$. Si $\pi_K(n)$ denota los primos de K de grado n, entonces la Hipótesis de Riemann sobre cuerpos funcionales (ver [**Ros02**, Theorem 5.12]) implica

$$\pi_K(n) = \frac{q^n}{n} + O_g\left(\frac{q^{n/2}}{n}\right), \tag{3.13}$$

donde g es el género de K. Ahora, pueden haber primos en el infinito que son contados en $\pi_K(n)$, pero como hay finitos de tales primos, su grado está acotado por una constante $r(K)$, con lo que para $n > r(K)$, $\pi_K(n)$ cuenta sólo ideales primos de $\mathcal{O}_K$ de grado n. Recordando que $\mathcal{P}_{I,K}$ consiste de primos de grado $H = \log_q(\tau\log(N)^{\frac{n}{n-\kappa}}) = \log_q(|I|)$, tenemos

$$|\mathcal{P}_{I,K}| = \pi_K(H) = \frac{|I|}{\log_q(|I)} + O_g\left(\frac{|I|^{1/2}}{\log_q(|I|)}\right) \gg_{g,q} \frac{|I|}{\log(|I|)}. \tag{3.14}$$

Reemplazando en (3.12) deducimos la Proposición 3.14. □

Observación 3.16. La constante C_1 en la Proposición 3.14 es efectiva, y puede tomarse que dependa linealmente en α. La prueba muestra que si escribimos $|X'| = \delta|X|$, entonces $\delta \geq c_3$ y c_3 es una constante absoluta efectiva.

Ahora, investiguemos la efectividad en la constante implícita en (3.4). Si K es un cuerpo funcional, la constante implícita en la Hipótesis de Riemann (3.13) es efectiva (esto se sigue de la prueba [**Ros02**, Theorem 5.12]). Por lo tanto, la efectividad de (3.4) depende sólo en la cota para el grado de los primos encima de ∞. Pero el grado de tales primos está siempre acotado por el grado $[K : k]$; esto se sigue de [**Sti09**, Proposition 1.1.15].

Ahora, supongamos que K es un cuerpo de números. En este caso se conocen versiones efectivas del teorema de los ideales primos de Landau; por ejemplo, ver [**Dav80**, pp. 95-96] y [**IK04**, Thm. 5.33 y 5.35]. Sin embargo, para probar la Proposición 3.14 sólo necesitamos cotas inferiores y superiores efectivas para $\pi_K(x) = |\{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K : \mathcal{N}(\mathfrak{p}) \leq x\}|$, del orden correcto de magnitud en x. Una cota superior efectiva para $\pi_K(x)$ puede encontrarse, por ejemplo, en [**LMO79**, Theorem 1.4], en donde se estudian versiones efectivas del teorema de Chebotarev. Si $K/\mathbb{Q}$ es una extensión de Galois, sea G el grupo de Galois de $K/\mathbb{Q}$, y sea $C \subseteq G$ una clase de conjugación. Denotemos por $[\frac{K/\mathbb{Q}}{\mathfrak{p}}]$ para el símbolo de Artin. Denotemos:

$$\pi_C(x, K/\mathbb{Q}) := \left|\left\{\mathfrak{p} : \mathfrak{p} \text{ es no ramificado en } K : \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] = C, \mathcal{N}(\mathfrak{p}) \leq x\right\}\right|. \tag{3.15}$$

Entonces existen constantes absolutas efectivas computables A_1, A_2 tales que si $K \neq \mathbb{Q}$, $\Delta_{K/\mathbb{Q}}$ es el valor absoluto del discriminante de K y

$$x > \exp(A_1(\log(\Delta_{K/\mathbb{Q}})(\log\log(\Delta_{K/\mathbb{Q}}))(\log\log\log(\Delta_{K/\mathbb{Q}}))e^{20})), \tag{3.16}$$

entonces

$$\pi_C(x, K/\mathbb{Q}) \leq A_2 \frac{x}{\log(x)}. \tag{3.17}$$

Para obtener una cota inferior efectiva, podemos usar el siguiente resultado de [**TZ17**]. Sea $K/\mathbb{Q}$ una extensión de Galois. Sea G el grupo de Galois $K/\mathbb{Q}$, y $C \subseteq G$ una clase de conjugación. Sea $H \leq G$ el mayor subgrupo abeliano de G tal que $H \cap C \neq \emptyset$, y sea F el cuerpo fijo de H. Para un caracter χ en el grupo dual $\widehat{H}$, sea $\mathfrak{f}_\chi$ el conductor de χ, y definamos

$$\mathfrak{Q}(K/F) = \max\{\mathcal{N}(\mathfrak{f}_\chi) : \chi \in \widehat{H}\}. \tag{3.18}$$

Entonces si

$$x \geq \Delta_K^{694} \mathfrak{Q}(K/F)^{521} + \Delta_K^{232} \mathfrak{Q}(K/F)^{367} [F : \mathbb{Q}]^{290[F:\mathbb{Q}]}, \tag{3.19}$$

tenemos que existe una constante absoluta efectiva computable A_3 tal que

$$\pi_C(x, K/\mathbb{Q}) \geq A_3 \frac{1}{(\Delta_{K/\mathbb{Q}} \mathfrak{Q}(K/F)[F : \mathbb{Q}])^5} \cdot \frac{x}{[K : F] \log(x)}, \tag{3.20}$$

provisto que $\Delta_{K/\mathbb{Q}} \mathfrak{Q}(K/\mathbb{Q})[K : F]^{[F:\mathbb{Q}]}$ es suficientemente grande.

En conclusión, si asumimos la Hipótesis Generalizada de Riemann, o si la extensión $K/\mathbb{Q}$ es una extensión de Galois, de grado suficientemente grande, la constante (3.4) es efectiva.

3.2. Normalización de Noether efectiva. Habiendo construido los conjuntos C y X'de la Proposición 3.14, el próximo paso es construir un polinomio homogéneo no nulo $P \in \mathcal{O}_K[T_0, \ldots, T_m]$ de complejidad pequeña que se anula en C pero no en Z. Luego de que esto esté hecho, vamos a mostrar que un tal polinomio debe anularse en X'. Como $|X'| = \delta|X|$ para algún $\delta > 0$, esto nos permitirá concluir que P se anula en al menos $\delta|X|$ puntos en X, concluyendo el Teorema 3.12 para $\varepsilon = \delta$. El Teorema 3.12 entonces se seguirá luego de $O_\varepsilon(1)$ iteraciones de este resultado. Nuestras herramientas principales serán el Lema 2.25 y la existencia de morfismos (racionales) dominantes $\varphi : Z \to \mathbb{P}^{\dim(Z)}(\overline{k})$. La manera en la que nosotros encontraremos un tal morfismo es mediante el lema de normalización de Noether. Dado que todos los resultados obtenidos hasta ahora han sido efectivos , vamos a dar una versión efectiva del lema de normalización de Noether. La prueba estará basada en la demostración clásica, como en [**Eis95**, Lemma 13.2., Theorem 13.3] o [**Sha74**, Chapter 1, § 5.4, Theorem 9]. Empezamos con el siguiente lema, que fue una pregunta del usuario H. A. Helfgott en mathoverflow, que fue respondida por el usuario Angelo Vistoli. Por completitud, incluimos la prueba.

Lema 3.17 (Comportamiento del grado bajo morfismos). *Sea K un cuerpo arbitrario. Sea $V \subseteq \mathbb{P}^m(\overline{K})$ una variedad proyectiva irreducible definida sobre un cuerpo K, de grado* $\deg(V)$*. Sea $f : V \to \mathbb{P}^n$ un morfismo definido sobre K, $f = (f_0, \ldots, f_n)$, con cada f_i un polinomio homogéneo de grado e. Denotemos W a la clausura Zariski de $f(V)$, y r a la dimensión de W. Entonces el grado de W es a lo sumo* $\deg(V)e^r$.

Demostración. Primero, notemos que podemos asumir que K es algebraicamente cerrado. Por [**Liu02**, Exercise 3.2.17], podemos también asumir que la dimensión de V y W son la misma, y que el morfismo $f : V \to W$ es finito y con fibras genéricamente no vacías. Ahora, sea $L \subseteq \mathbb{P}^n(\overline{K})$ un subespacio linear genérico de codimensión r de W. La cardinalidad de la intersección $L \cap W$ es $\deg(W)$, y esta cantidad está acotada superiormente por la cardinalidad de $f^{-1}(L)$, la cuál es finita. Pero $f^{-1}(L)$ es la intersección de V con $H = V(g_1, \ldots, g_r)$, el conjunto de ceros de r combinaciones

lineales genéricas de los f_i. Si X es una variedad proyectiva (no necesariamente equidimensional), llamemos $\deg(X)$ a la suma de los grados de sus componentes irreducibles. Por el Teorema de Bezout, como en [**Ful84**, Example 8.4.6], si $V_1, \ldots, V_s$ son las componentes irreducibles de $V \cap H$, entonces

$$\deg(f^{-1}(L)) = \deg(V \cap H) = \sum_{i=1}^{s} \deg(V_i) \leq \deg(V) \prod_{i=1}^{r} \deg(g_i) \leq \deg(V) e^r.$$

□

El otro ingrediente que vamos usar para obtener un teorema de normalización de Noether efectivo es el conocido Nullstellensatz Combinatorio.

Teorema 3.18 (Nullstellensatz Combinatorio, [**TV10**, Theorem 9.2]). *Sea K un cuerpo arbitrario, sea $P \in F[T_1, \ldots, T_n]$ un polinomio de grado d el cuál contiene un coeficiente no nulo en $T_1^{d_1} \cdots T_n^{d_n}$ con $d_1 + \ldots + d_n = d$, y sean $S_1, \ldots, S_n$ subconjuntos de K tales que $|S_i| > d_i$ para todo $1 \leq i \leq n$. Entonces existen $x_1 \in S_1, \ldots, x_n \in S_n$ tales que $P(x_1, \ldots, x_n) \neq 0$*

Ahora enunciamos la versión efectiva del teorema de normalización de Noether.

Teorema 3.19 (Versión efectiva del teorema de normalización de Noether). *Sea $V \subseteq \mathbb{P}^m(\bar{k})$ una variedad proyectiva irreducible definida sobre un cuerpo global K. Entonces existe un morfismo finito $\varphi : V \to \mathbb{P}^{\dim(V)}$, definido sobre K, tal que $\varphi(\boldsymbol{x}) = (L_0(\boldsymbol{x}) : \ldots : L_{\dim(V)}(\boldsymbol{x}))$ con L_i formas lineales con coeficientes en k de altura acotada por $\ll_{m,k} \deg(V)^{\dim(V)}$, donde la constante implícita es efectivamente computable.*

Para la prueba, vamos a usar una idea encontrada en el blog de Terence Tao.

Demostración. Sea V una variedad irreducible como en el teorema. Si $V = \mathbb{P}^m$ para algún m, podemos tomar φ la identidad. Si $V \subsetneq \mathbb{P}^m$, entonces existe $\mathbf{x} \in \mathbb{P}^m(\bar{k}) \backslash V(\bar{k})$. Más aún, veamos que podemos elegir $\mathbf{x}$ con coordenadas en k, y de altura pequeña. Elijamos un subespacio proyectivo S de $\mathbb{P}^m(\bar{k})$ de dimensión $m - \dim(V) - 2$, y consideremos el cono[1] $C(S, V)$ formado tomando la unión de todas las rectas que unen un punto en S a un punto en V. Genéricamente es una subvariedad proyectiva de dimensión $m - 1$, es decir una hipersuperficie. Adicionalmente, tiene grado $\deg(V)$, con lo que $C(S, V)$ está definido por un polinomio homogéneo con coeficientes en K, de grado $\deg(V)$. En conclusión, tenemos que V está contenido en una hipersuperficie $V(P) \subseteq \mathbb{P}^m(\bar{k})$, donde $P \in K[T_0, \ldots, T_m]$ es un polinomio homogéneo no nulo de grado $\deg(V)$.

Supongamos que P tiene un coeficiente no nulo en $T_0^{d_0} \cdots T_n^{d_n}$. Notemos que $d_0 + \cdots + d_m = \deg(V)$ con lo que $d_i \leq \deg(V)$ para todo i. Dado que $[\deg(V)]_k = \{x \in k : H(x) \leq \deg(V)\}$ tiene más de $\deg(V)$ elementos, tomando $S_i = [\deg(V)]_k$ para todo i, el Teorema 3.18 implica que existe un punto $(x_0, \ldots, x_m) \in [\deg(V)]_k^{m+1}$ tal que $P(x_0, \ldots, x_m) \neq 0$. En particular, $(x_0, \ldots, x_m) \neq 0$. Sea $\mathbf{x}_1 \in \mathbb{P}^m(\bar{k})$ el punto con coordenadas proyectivas $(x_0 : \ldots : x_m)$. Por construcción, $\mathbf{x}_1 \in \mathbb{P}^m(\bar{k}) \backslash V(\bar{k})$. Ahora, construiremos formas lineales $L_{1,1}(T_0, \ldots, T_m), \ldots, L_{1,m}(T_0, \ldots, T_m) \in k[T_0, \ldots, T_m]$ tales que $V(L_{1,1}, \ldots, L_{1,m}) = \{\mathbf{x}_1\}$. Notemos que los coeficientes de tales formas lineales conforman una base del espacio vectorial $V_1 := \langle (x_0, \ldots, x_m) \rangle^{\perp}$. Por el Teorema 2.26, el Teorema 2.27, y (2.33)

[1] Este argumento parece ser estándar en geometría algebraica; por ejemplo, puede verse usado en [**Mar10**, Thm. 1] para probar que la imagen de una variedad proyectiva por el d-uple embedding es intersección de cuádricas.

podemos encontrar una base $\mathbf{y}_1, \ldots, \mathbf{y}_m \in k^{m+1}$ de V_1 tal que

$$\begin{aligned}\prod_{i=1}^{m} H(1 : \mathbf{y}_i) &\leq C(k)^m H_{\mathrm{Ar}}(x_0 : \ldots : x_m) \leq \sqrt{m+1}C(k)^m H(x_0 : \ldots : x_m) \\ &\leq \sqrt{m+1}C(k)^m \max_i\{H(x_i)\} \leq \sqrt{m+1}C(k)^m \deg(V).\end{aligned} \tag{3.21}$$

Definimos $\varphi_1 : X \to \mathbb{P}^{m-1}$ como la proyección lejos de $\mathbf{x}_1$, es decir

$$\varphi_1(\mathbf{x}) = (L_{1,1}(\mathbf{x}) : \ldots : L_{1,m}(\mathbf{x})). \tag{3.22}$$

Por lo tanto φ_1 es un morfismo finito [**Sha74**, Chatper 1, § 5.3, Theorem 7], con $L_{1,1}, \ldots, L_{1,m}$ formas lineales con coeficientes de altura acotada por $\ll_{m,k} \deg(V)$. Más aún, por el Lema 3.17, $\deg(\varphi_1(X)) \leq \deg(V)$. Si $\varphi_1(X) = \mathbb{P}^{m-1}$, terminamos. Caso contrario, repetimos el mismo argumento. De esta manera obtenemos una sucesión de morfismos finitos $\varphi_{i+1} : \varphi_i(X) \to \mathbb{P}^{m-i+1}$, definido como

$$\varphi_{i+1}(\mathbf{x}) = (L_{i+1,1}(\mathbf{x}) : \ldots : L_{i+1,m-i+1}(\mathbf{x})), \tag{3.23}$$

con $L_{i+1,1}, \ldots, L_{i+1,m-i+1}$ formas lineales con coeficientes en k de altura acotada por $\ll_{m,k} \deg(V)$. Como la sucesión $\varphi_1, \varphi_2, \ldots$ termina en $i = m - \dim(X)$, concluimos que existe un morfismo finito $\varphi : X \to \mathbb{P}^{\dim(X)}$ tal que

$$\varphi(\mathbf{x}) = (L_0(\mathbf{x}) : \ldots : L_{\dim(X)}(\mathbf{x})), \tag{3.24}$$

con $L_0, \ldots, L_m$ formas lineales con coeficientes en k de altura acotada por $\ll_{m,k} \deg(V)^{\dim(V)}$. □

Remark 3.20. En la literatura, se conocen versiones efectivas del lema de normalización para cuerpos de números. Por ejemplo, ver [**KPS01**, Lemma 2.14, Prop. 4.5]. Le agradezco al Profesor Sombra por esta referencia.

3.3. Construcción del polinomio auxiliar y conclusión de la prueba. Sean $C \subseteq X$ y X' los conjuntos de la Proposición 3.14. Como ya hemos explicado, el primer paso es construir un polinomio de complejidad baja que se anula en C, mediante el Lema 2.25. Si $Z = \mathbb{P}^m(\bar{k})$, hallar un polinomio homogéneo no nulo $P \in O_K[T_0, \ldots, T_m]$ de grado D, que se anula en C equivale a resolver un sistema lineal de ecuaciones $A \cdot \mathbf{c} = 0$. Por lo tanto, podemos usar el Lema 2.25 para hallar un polinomio no nulo de grado D tal que sus coeficientes tienen altura pequeña. Sin embargo, en el caso $Z \subsetneq \mathbb{P}^m(\bar{k})$, si aplicamos el lema 2.25 directamente, hallaríamos un polinomio homogéneo no nulo $P \in O_K[T_0, \ldots, T_m]$ de baja complejidad, anulándose en C, pero podría ocurrir que P se anula en Z. Para evitar esta dificultad, vamos a usar el Teorema 3.19 para encontrar nuevas variables $Y_0, \ldots, Y_n$ algebraicamente independientes sobre $\bar{k}$, y luego aplicar el Lema 2.25 para hallar un polinomio en este nuevo conjunto de variables.

Prueba del Teorema 3.12. Por el Teorema 3.19, existe un morfismo polinomial $\mathbf{F} : Z \to \mathbb{P}^n(\bar{k})$, $\mathbf{F}(\mathbf{x}) := (F_0(\mathbf{x}) : \ldots : F_n(\mathbf{x}))$, con cada $Y_i = F_i \in O_k[T_0, \ldots, T_m]$ una forma lineal con coeficientes de altura acotada por una constante efectiva computable $c = c(m, k, Z) > 0$. Denotemos $\tilde{C} \subseteq \mathbb{P}^n(K)$ a la imagen de $C \subseteq \mathbb{P}^m(K)$ bajo $\mathbf{F}$. Notemos que $|C| \leq |\tilde{C}|$. Si $\mathbf{x} \in [N]_{\mathbb{P}^m(K)}$, la Proposición 2.22 da

$$H(F_0(\mathbf{x}) : \ldots : F_n(\mathbf{x})) \leq c(Z)H(\mathbf{x}) \leq C(m, k, Z)N, \tag{3.25}$$

donde $C(m, k, Z)$ es una constante dependiente sólo en m, k y Z. Denotemos $M = C(m, k, Z)N$. La desigualdad (3.25) significa que $\tilde{C} \subseteq [M]_{\mathbb{P}^n(K)}$. Ahora, sea $D > 0$ un entero a ser elegido más

adelante, y sea $\mathcal{R}$ el conjunto de monomios de grado D en $Y_0, \dots, Y_n$. Entonces $R := |\mathcal{R}| = \binom{D+n}{n}$. Esto es también el número de n-tuplas $(i_0, \dots, i_n) \in \mathbb{N}_0^n$ con $i_0 + \cdots + i_n = D$. Si $\mathbf{y} \in \tilde{C}$, elijamos coordenadas $(y_0 : \dots : y_n)$ como en el Lema 2.20. Como $\mathbf{y} \in [M]_{\mathbb{P}^n(K)}$, del Lema 2.20 concluimos

$$H(1 : y_0 : \dots : y_n) \leq M^{(dn+1)d}. \tag{3.26}$$

Para tales coordenadas de $\mathbf{y}$ e $I = (i_0, \dots, y_n) \in \mathcal{R}$, denotemos $\mathbf{y}^I := y_0^{i_0} \cdots y_n^{i_n}$. Entonces $A := (\mathbf{y}^I)_{\mathbf{y} \in \tilde{C}, I \in \mathcal{R}}$ es una matriz $|\tilde{C}| \times R$ con entradas en O_K. Además, debido al Corolario 2.23 y la elección de coordenadas de $\mathbf{y}$, tenemos

$$H(\mathbf{y}^I) \leq H(1 : y_0 : \dots : y_n)^D \leq M^{(dn+1)dD}. \tag{3.27}$$

Ahora, elijamos D tal que las siguientes desigualdades se cumplen:

$$((2d^2+1)n!|\tilde{C}|)^{1/n} \leq ((2d^2+1)n!|C|)^{1/n} \leq ((2d^2+1)n!r)^{1/n} < D \ll_{n,d} r^{1/n}. \tag{3.28}$$

La desigualdad $D > ((2d^2+1)n!r)^{1/n}$ da $R = \binom{D_n}{n} > (2d^2+1)r$. Además, esto implica

$$\frac{r}{\binom{D+n}{n} - 2d^2 r} \leq 1. \tag{3.29}$$

La desigualdad $D \ll_{n,d} r^{1/n}$ da

$$R = \binom{D+n}{n} \ll_{n,d} r \tag{3.30}$$

para r suficientemente grande, y por lo tanto, para N suficientemente grande. Dado que $|\tilde{C}| \leq |C| \leq r < R$, el K-subespacio de soluciones de la ecuación $A \cdot \mathbf{y} = 0$ tiene dimensión positiva, por lo tanto podemos aplicar el Lema 2.25 y (3.29) para obtener una solución no nula $\mathbf{c} = (c_I)_{I \in \mathcal{R}} \in O_K^R$ tal que

$$H(1 : \mathbf{c}) \ll_K \left(RM^{(dn+1)d^2D}\right)^{\frac{4d^2|\tilde{C}|}{R-2d^2|\tilde{C}|}} \ll_K (RM^{(dn+1)d^2D})^{4d^2}. \tag{3.31}$$

La solución $\mathbf{c} = (c_I)_{I \in \mathcal{R}}$ da un polinomio no nulo homogéneo $P(Y) = \sum_{I \in \mathcal{R}} c_I Y^I$ de grado D, que se anula en $\tilde{C}$, y tal que los coeficientes verifican la cota (3.31). Usando las cotas $D \ll_n r^{1/n}$ y (3.30) concluimos

$$H(1 : \mathbf{c}) \ll_{K,n,m} r^{4d^2} M^{c(K,n)r^{1/n}}, \tag{3.32}$$

para alguna constante positiva $c(K, n)$. Tomando N suficientemente grande, dependiente en κ, n, m, K, Z, de la desigualdad anterior y (3.3) deducimos

$$H(1 : \mathbf{c}) \ll_{K,n,m,\kappa} N^{c'(K,n)r^{1/n}} \tag{3.33}$$

para alguna constante positiva $c'(K, n)$. En conclusión, el polinomio P es no nulo, tiene coeficientes en O_K, se anula en $\tilde{C}$, y tiene complejidad $\ll_{K,n,m,\kappa} r^{1/n} = \eta^{1/n}(\log(N))^{\kappa/n-\kappa}$, donde la última desigualdad es por la definición (3.2). Recordando que $Y_i = F_i(T_0, \dots, T_m)$ es un polinomio lineal con coeficientes en O_K, concluimos que obtenemos un polinomio

$$Q := P(F_0(T_0, \dots, T_m), \dots, F_n(T_0, \dots, T_m)) \in O_K[T_0, \dots, T_m] \backslash \{0\},$$

que se anula en C, no se anula en Z, y tiene grado $\ll_{K,n,m,\kappa} \eta^{1/n}(\log(N))^{\kappa/(n-\kappa)}$.

Ahora queremos probar que Q se anula en el conjunto más grande X' de la Proposición 3.14. Esto será deducido del hecho que Q se anula en C, luego de elegir adecuadamente las constantes η, τ. Para poder hacer esto, necesitamos tener control del tamaño de la imagen del polinomio Q en X'. Notemos que como $H(Q(\mathbf{x}))$ depende de la representación $\mathbf{x} = (x_0 : \dots : x_n)$, necesitamos elegir

coordenadas adecuadas. Esto lo hacemos de la manera siguiente. Dado $\mathbf{x} \in [N]_{\mathbb{P}^m(K)}$, elijamos coordenadas $(x_0 : \ldots : x_m)$ como en el Lema 2.20, y denotemos $\mathbf{x}' = (x_0, \ldots, x_m)$ al correspondiente punto afín. Ahora, definimos $\mathbf{y}'$ como el punto afín $\mathbf{F}(\mathbf{x}') = (F_0(\mathbf{x}'), \ldots, F_n(\mathbf{x}'))$. La elección de coordenadas de $\mathbf{x}$ y el Corolario 2.23 dan

$$H(1 : \mathbf{y}') \leq c(m,k,Z)H(1 : \mathbf{x}) \leq c(m,k,Z)N^{(dn+1)d}. \tag{3.34}$$

Aplicando el Corolario 2.23 a nuestro polinomio Q en el punto $\mathbf{x}'$, y usando (3.33) y (3.34) obtenemos

$$H(Q(\mathbf{x}')) = H(P(\mathbf{y}')) \leq RH(1 : \mathbf{c})H(1 : \mathbf{y}')^D \ll_{K,n,m,\kappa} N^{c''(K,n)r^{1/n}} \tag{3.35}$$

para alguna constante positiva $c''(K,n)$. En particular, por el Lema 2.31, tenemos que para todo $\mathbf{x} \in [N]_{\mathbb{P}^m(K)}$,

$$\log(\mathcal{N}(Q(\mathbf{x}'))) \ll_{K,n,m,\kappa} r^{1/n}\log(N) \ll_{K,n,m,\kappa} \eta^{1/n}(\log(N))^{n/(n-\kappa)} \ll_{K,m,Z,\kappa} \eta^{1/n}(\log(N))^{\frac{n}{n-\kappa}}. \tag{3.36}$$

Si $\mathbf{x} \in X'$ y $Q(\mathbf{x}) \neq 0$, entonces $Q(\mathbf{x}') \neq 0$ y tenemos

$$\sum_{\mathfrak{p}\in\mathcal{P}_{I,K}} 1_{\mathfrak{p}|Q(\mathbf{x}')}\log(\mathcal{N}(\mathfrak{p})) \leq \log\left(\prod_{\mathfrak{p}|Q(\mathbf{x}')}\mathcal{N}(\mathfrak{p})\right) = \log(\mathcal{N}(Q(\mathbf{x}'))) \ll_{K,m,Z,\kappa} \eta^{1/n}(\log(N))^{n/(n-\kappa)}. \tag{3.37}$$

Eligiendo adecuadamente η y τ, vamos a ver que (3.37) no ocurre.

Sea de nuevo $\mathbf{x} \in X'$. Sea $\mathfrak{p}$ un ideal primo que contribuye al lado izquierdo en la suma de la Proposición 3.14. Entonces existe $\mathbf{z} \in C$ tal que $\mathbf{x} \equiv \mathbf{z} \mod(\mathfrak{p})$. Como Q se anula en C, por el Hecho 3.8 tenemos $Q(\mathbf{x}) \equiv Q(\mathbf{z}) \equiv 0 \mod(\mathfrak{p})$, con lo que debemos tener $\mathfrak{p}|Q(\mathbf{x})$. Concluimos que todo ideal primo $\mathfrak{p}$ que contribuye al lado izquierdo de la suma de la Proposición 3.14 también contribuye al lado izquierdo de (3.37). Entonces de la Proposición 3.14 tenemos que el lado izquierdo de (3.37) es $\gg_K |I| \gg_K \tau(\log(N))^{n/(n-\kappa)}$. Eligiendo η y τ que satisfacen

$$\tau \geq C_2\eta^{1/n} \tag{3.38}$$

para una constante C_2 suficientemente grande, dependiente de K, n, m, Z y κ. Como por la Proposición 3.14 también requerimos que $\eta \geq C_1\tau^\kappa$, alcanza con elegir

$$\eta \geq (C_1C_2^\kappa)^{n/(n-\kappa)}. \tag{3.39}$$

Entonces $Q(\mathbf{x}') = Q(\mathbf{x}) = 0$. Como esto vale para todo $\mathbf{x} \in X'$, concluimos la demostración. □

Observación 3.21. Como la Proposición 3.14 es efectiva si K es un cuerpo funcional, y para K de grado suficientemente grande si K es un cuerpo de números (ver Observación 3.16), como así también es efectivo el Teorema 3.19, concluimos que todas las constantes en el Teorema 3.12 son efectivamente computables, si K tiene grado suficientemente grande.

Observación 3.22. En la prueba del Teorema 3.12, fue suficiente elegir η verificando $\eta \geq (C_1C_2)^{n/(n-\kappa)}$ y $\tau \geq C_2\eta^{1/n}$ para concluir el teorema. En particular, podemos imponer la condición adicional que τ es más grande que alguna constante absoluta $C > 0$.

Concluimos esta sección probando que el Teorema 3.12 implica el siguiente resultado

Corolario 3.23. *Para $n > 0$, todo número real $0 \leq \kappa < n$ y todo cuerpo global K, existe $\tau = \tau(n,\kappa,K) \geq 1$ tal que vale lo siguiente. Sea I el intervalo real $[\tau(\log(N))^{\frac{n}{n-\kappa}}, 2\tau(\log(N))^{\frac{n}{n-\kappa}}]$.*

Escribamos $\mathcal{P}_{I,K}$ para el conjunto de ideales primos $\mathfrak{p} \subseteq \mathcal{O}_K$ definido como

$$\mathcal{P}_{I,K} := \begin{cases} \{\mathfrak{p} \subseteq \mathcal{O}_K : \mathcal{N}(\mathfrak{p}) \in I\} \text{ if } K \text{ is a number field} \\ \{\mathfrak{p} \subseteq \mathcal{O}_K : \mathcal{N}(\mathfrak{p}) = \tau(\log(N))^{\frac{n}{n-\kappa}}\} \text{ if } K \text{ is a function field} \end{cases}. \tag{3.40}$$

Para todo $X \subseteq [N]_K^n$, consideremos el embedding $X \hookrightarrow \mathbb{P}^n(K)$, dado por $\boldsymbol{x} \mapsto (1 : \boldsymbol{x})$. Denotemos $\tilde{X}$ la imagen de X por este embedding. Si $|\tilde{X}_\mathfrak{p}| \ll \mathcal{N}(\mathfrak{p})^\kappa$ para todo primo $\mathfrak{p} \in \mathcal{P}_{I,K}$, y todo $\varepsilon > 0$, existe algún $P \in \mathcal{O}_K[X_1, \dots, X_n]$ no nulo, de complejidad $\ll_{\kappa,n,\varepsilon,K} (\log(N))^{\frac{n}{n-\kappa}}$ anulándose en al menos $(1-\varepsilon)|X|$ puntos de X. En particular, tomando $X \subseteq [N]_{\mathcal{O}_K}^n$ obtenemos el Teorema 3.4.

Demostración . Sea $X \subseteq [N]_K^n$ un conjunto como en el Corolario 3.23. Sea $\mathbf{x} \in [N]_K^n$. Entonces (2.33) implica que $H(1 : \mathbf{x}) \leq N^{[K:k]}$. Consideremos el embedding $[N]_K^n \hookrightarrow [N^{[K:k]}]_{\mathbb{P}^n(K)}$ dado por $\mathbf{x} \mapsto (1 : \mathbf{x})$. Entonces $\tilde{X}$ satisface las hipótesis del Teorema 3.12, con lo que podemos aplicar este teorema a $\tilde{X}$. Obtenemos un polinomio no nulo homogéneo $P(X_0, \dots, X_n)$ de la complejidad deseada, que se anula en al menos $(1-\varepsilon)|\tilde{X}|$ puntos de $\tilde{X}$. Ahora $P(1, X_1, \dots, X_n)$ es un polinomio que satisface la conclusión del Corolario 3.23. □

CAPÍTULO 4

Una conjetura en Geometría Diofántica

1. Introducción

Para K un cuerpo de números, y $X \subseteq \mathbb{R}^n$, denotemos por $X(K)$ el subconjunto de puntos con coordenadas K-racionales. Para $x \in K$, sea $H(x)$ la altura afín de un número algebraico. Para $T \geq 1$, sea

$$X(K,T) := \{\mathbf{x} \in X(K) : H(x_i) \leq T \ \forall i\}. \tag{4.1}$$

Un problema fundamental en Geometría Diofántica y Teoría de Trascendencia. es obtener cotas para $X(K,T)$ cuando X es un conjunto no algebraico. Cuando X es el gráfico de $f : [0,1] \to \mathbb{R}$ una función analítica trascendente, en [**Pil91**, Theorem9], Pila prueba que para todo $\varepsilon > 0$ existe una constante positiva $c = c(X,\varepsilon)$ tal que

$$|X(\mathbb{Q},T)| \leq cT^{\varepsilon}. \tag{4.2}$$

Para $X \subseteq \mathbb{R}^n$ en general, si queremos obtener cotas comparables a (4.2) necesitamos trabajar con la parte trascendente de X. La parte algebraica de X, denotada X^{alg}, es el conjunto de $\mathbf{x} \in X$ tales que existe un subconjunto semi-algebraico, conexo, de dimensión positiva $C \subseteq X$ con $\mathbf{x} \in C$. La parte trascendental de X, denotada por X^{trans}, es el complemento $X \backslash X^{\text{alg}}$.

Para generalizar (4.2) a conjuntos de dimensiones superiores, Pila y Wilkie en [**PW06**] estudian la parte trascendente de un conjunto $X \subseteq \mathbb{R}^n$ definible en una estructura o-minimal.

Teorema 4.1 ([**PW06**, Theorem 1.8]). *Sea $X \subseteq \mathbb{R}^n$ un conjunto, definible en una estructura o-minimal, y sea $\varepsilon > 0$. Existe una constante positiva $c = c(X,\varepsilon)$ tal que para todo $T \geq 1$ tenemos*

$$|X^{trans}(\mathbb{Q},T)| \leq cT^{\varepsilon}. \tag{4.3}$$

El Teorema 4.1 fue luego generalizado por Pila en [**Pil09**], obteniendo un resultado más uniforme, que implica el mismo tipo de cota (4.3) para cuerpos de números, pero con la constante c dependiente en el grado del cuerpo.

En general, la cota en el Teorema 4.1 es la mejor posible, pero si consideramos algunas estructuras o-minimales específicas, se conjetura que la cota puede mejorarse. Este es el contenido de la conjetura de Wilkie.

Conjetura 4.2 (Conjetura de Wilkie, [**PW06**, Conjecture 1.11]). Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en la estructura o-minimal $\mathbb{R}_{\text{exp}}$. Para todo cuerpo de números $K \subseteq \mathbb{R}$, existen constantes positivas $c_1 = c_1(X,K)$, $c_2 = c_2(X)$ tales que

$$|X^{\text{trans}}(K,N)| \leq c_1(\log(N))^{c_2} \tag{4.4}$$

para todo $N > e$.

Notemos que la Conjetura 4.2 tiene consecuencias profundas en Teoría de Trascendencia. En efecto, en [**Pil10**] y [**But17**] se muestra que si la Conjetura 4.2 vale para conjuntos específicos X con la constante c_2 igual a la dimensión $\dim(X)$, entonces se sigue la siguiente versión real de la conjetura de cuatro exponenciales: sean $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{R}$ con la propiedad que e^{λ_i} es algebraica para todo i. Supongamos que λ_1 y λ_3 son $\mathbb{Q}$-linealmente independientes, y que λ_1 y λ_4 son $\mathbb{Q}$-linealmente independientes. Entonces $\lambda_1\lambda_2 \neq \lambda_3\lambda_4$.

Podemos preguntarnos si la cota en la Conjetura 4.2 vale para otras estructuras o-minimales. Por ejemplo, tenemos la siguiente generalización natural de la Conjetura 4.2.

Conjetura 4.3. Sea $f_1, \ldots, f_r$ una cadena Pfaffiana y supongamos que $\tilde{\mathbb{R}} = (\mathbb{R}, <, +, -, \cdot, f_1, \ldots, f_r)$ es una expansión model complete del cuerpo real. Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en la estructura o-minimal $\tilde{\mathbb{R}}$. Para todo cuerpo de números $K \subseteq \mathbb{R}$, existen constantes positivas $c_1 = c_1(X, K)$, $c_2 = c_2(X)$ tales que

$$|X^{\text{trans}}(K, N)| \leq c_1(\log(N))^{c_2} \tag{4.5}$$

para todo $N > e$.

Si la dimensión de X es igual a 1, entonces la Conjetura 4.2 y la Conjetura 4.3 se sabe que valen por trabajo de Butler [**But12**] y Jones y Thomas [**JT12**]. Si X tiene dimensión más grande que 1, la Conjetura 4.2 se sabe sólo para la familia de superficies

$$\{(x, y, z) \in (0, \infty)^3 : (\log(x))^a(\log(y))^b(\log(z))^c = 1\},\ (a, b, c) \in \mathbb{Q}^3 \tag{4.6}$$

por trabajo de Pila [**Pil10**] cuando $(a, b, c) = (1, 1, -1)$ y Butler [**But12**] en el caso general. Si $X \subseteq \mathbb{R}^3$ es definible en una estructura o-minimal como en la Conjetura 4.3, entonces, bajo la hipótesis que X posee una "mild parametrization" (ver [**Pil10**, § 2]), en [**JT12**] Jones y Thomas prueban que X satisface la Conjetura 4.3. Esto puede generalizarse para un conjunto $X \subseteq \mathbb{R}^n$ de dimensión 2, como fue mostrado en [**Sch18**].

Notemos que, mientras la Conjetura 4.3 permanece abierta, Binyamini y Novikov probaron que para conjuntos definibles en la estructura o-minimal restringida $\mathbb{R}^{RE} := (\mathbb{R}, <, +, \cdot, \exp|_{[0,1]}, \sin|_{[0,\pi]})$ la cota en la Conjetura 4.2 vale, en una forma más fuerte (ver [**BN17**, Theorem 2]).

El objetivo de este capítulo es probar que la Conjetura 4.2 y la Conjetura 4.3 pueden interpretarse en términos de un principio local-global. Más precisamente, probamos:

Teorema 4.4 ([**Par19**, Theorem 4.3]). *Sea $f_1, \ldots, f_r$ una cadena Pfaffiana y supongamos que $\tilde{\mathbb{R}} = (\mathbb{R}, <, +, -, \cdot, f_1, \ldots, f_r)$ es una expansión model complete del cuerpo real. Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en la estructura o-minimal $\tilde{\mathbb{R}}$. Para todo cuerpo de números $K \subseteq \mathbb{R}$ y todo $T > e$ denotemos $X^{\widetilde{trans}}(K, N)$ para la imagen de $X^{trans}(K, N)$ bajo el embedding $\boldsymbol{x} \in \mathbb{R}^n \mapsto (1 : \boldsymbol{x}) \in \mathbb{P}^n(\mathbb{R})$. Si X tiene dimensión a lo sumo 2, entonces X satisface la Conjetura 4.3 para el cuerpo de números $K \subseteq \mathbb{R}$ si y sólo si existen constantes positivas $\alpha = \alpha(X, K)$, $\tau = \tau(X, K)$, $\kappa = \kappa(X)$, con $0 \leq \kappa(X) < n$ tales que*

$$\left|\left(X^{\widetilde{trans}}(K, T)\right)_{\mathfrak{p}}\right| \leq \alpha \mathcal{N}(\mathfrak{p})^{\kappa} \tag{4.7}$$

para todo $T > e$ y todo ideal primo $\mathfrak{p}$ con $\mathcal{N}(\mathfrak{p}) \geq \tau(\log(N))^{\frac{n}{n-\kappa}}$.

2. Parametrización de un conjunto definible

La prueba del Teorema 4.1 en [**PW06**] empieza mostrando que los puntos a estudiar residen en pocas (i.e. $O_{X,\varepsilon}(T^{\varepsilon})$) hipersuperficies de grado adecuado $d(\varepsilon)$; luego el argumento procede por

inducción en la dimensión de X. Por lo tanto es necesario tener una estimación de la misma forma que el Teorema 4.1 para aquellas intersecciones con hipersuperficies pero con la constante uniforme sobre todas las intersecciones de X con hipersuperficies de grado fijo, es decir, un resultado para familias definibles de conjuntos. Más precisamente, Pila y Wilkie prueban la siguiente versión uniforme del Teorema 4.1:

Teorema 4.5. *Sea $Z \subseteq \mathbb{R}^n \times \mathbb{R}^m$ una familia definible, y sea $\varepsilon > 0$. Existe una constante $c(Z, \varepsilon)$ con la siguiente propiedad. Sea X una fibra de Z. Entonces*

$$|X^{trans}(\mathbb{Q}, T)| \leq c(Z, \varepsilon) T^{\varepsilon}. \tag{4.8}$$

Por razones técnicas, es necesaria una versión más fuerte del Teorema 4.5; referimos los detalles a [**PW06**].

La parte diofantina de la prueba sigue el método del determinante de Bombieri-Pila. Mientras tanto la parte analítica de la prueba se centra en el problema de encontrar parametrizaciones uniformes de las fibras X en una familia definible, la uniformidad siendo en el número de funcion $(0,1)^{\dim(X)} \to X$ de clase C^r requeridas para cubrir y X y, al mismo tiempo, en las cotas de los tamaños de todas sus derivadas parciales hasta cierto orden finito prefijado r. Para poder formalizar este último argumento, recordamos la noción de una r-reparametrización.

Definición 4.6 (Parametrización). Sea $X \subseteq \mathbb{R}^n$ definible. Una función definible $\phi : (0,1)^{\dim(X)} \to X$ se dice una parametrización parcial de X. Un conjunto finito S de parametrizaciones parciales de X se dice una parametrización de X si $\bigcup_{\phi \in S} \text{trange}(\phi) = X$.

Una parametrización S de X se dice una r-parametrización si toda $\phi \in S$ es de clase C^r y tiene la propiedad que $\phi^{(\alpha)}$ está acotada para cada $\alpha \in \mathbb{N}^{\dim(X)}$ con $|\alpha| \leq r$, donde $|\alpha|$ es la suma de las coordenadas de α.

Definición 4.7 (Reparametrización). Supongamos que S es una r-parametrización del conjunto definible $X \subseteq \mathbb{R}^m$ y que $F : X \to \mathbb{R}^n$ es una función definible. Entonces decimos que S es una r-reparametrización de F si, para cada $\phi \in S$, $F \circ \phi$ es de clase C^r y $(F \circ \phi)^{(\alpha)}$ está acotada para todo $\alpha \in \mathbb{N}^{\dim(X)}$ con $|\alpha| \leq r$.

Inspirados por resultados de Yomdin y Gromov [**Yom87, Gro87**] para parametrizaciones de conjuntos semi-algebracios, Pila y Wilkie [**PW06**] probaron:

Teorema 4.8 (Teorem de reparametrización, [**PW06**, Theorem 2.3, Theorem 2.5]). *Sea $r \in \mathbb{N}$.*

(i) Para todo conjunto $X \subseteq \mathbb{R}^n$ definible, acotado, existe una r-parametrización de X.

(ii) Para toda función $F : X \to \mathbb{R}^n$ definible, acotada, existe una r-reparametrización de F.

Es importante mencionar que en [**PW06**], el Teorema 4.8 está probado en una manera más general. Aquí sólo mencionaremos que del Teorema 4.8 podemos deducir el siguiente resultado uniforme.

Corolario 4.9 ([**PW06**, Corollary 5,2]). *Sean $n, m, r \geq 1$ enteros, y supongamos que $X \subseteq (0,1)^n \times \mathbb{R}^m$ es una familia definible. Entonces existe $N \in \mathbb{N}$ y, para cada $\boldsymbol{y} \in \mathbb{R}^m$, un conjunto $S_{\boldsymbol{y}}$ de N funciones, cada una aplicando $(0,1)^{\dim(X_{\boldsymbol{y}})}$ a $X_{\boldsymbol{y}}$ y todas de clase C^r, tales que*

(1) $\bigcup_{\phi \in S_{\boldsymbol{y}}} range(\phi) = X_{\boldsymbol{y}}$;

(2) $|\phi^{(\alpha)}(\boldsymbol{x})| \leq 1$ para cada $\phi \in S_{\boldsymbol{y}}$, $\alpha \in \mathbb{N}^{\dim(X_{\boldsymbol{y}})}$ con $|\alpha| \leq r$ y para todo $\boldsymbol{x} \in (0,1)^{\dim(X_{\boldsymbol{y}})}$.

Más aún, las funciones que constituyen $S_{\mathbf{y}}$ dependen definiblemente en $\mathbf{y}$.

Usando el Corolario 4.9, el método del determinante, y un argumento inductivo astuto, Pila y Wilkie prueban el Teorema 4.5, y en consecuencia el Teorema 4.1. Sin embargo, el Corolario 4.9 no alcanza para probar la Conjetura 4.2. Para poder probar la Conjetura 4.2, en [**Pil07, Pil10**] se propone una noción de parametrización más fuerte, que ahora recordamos. Primero necestiamos la noción de "mild functions", que son otra formulación de las funciones Gevrey en ecuaciones diferenciales en derivadas parciales.

Definición 4.10 (Mild functions). Sea $G : \mathbb{N}^m \to (0,\infty)$. Decimos que una función $f : (0,1)^m \to (0,1)$ es G-mild si es de clase C^∞ y

$$|\partial^\mu f(\mathbf{x})| \leq G(\mu) \tag{4.9}$$

para todo $\mu \in \mathbb{N}^m$ y $\mathbf{x} \in (0,1)^m$. Una función $F : (0,1)^m \to (0,1)^n$ se dice G-mild si todas sus funciones coordenadas lo son.

Si $G(n) = n!(An^C)^n$ para algún A y C, una función G-mild se dice una función (A,C)-mild . Más precisamente, una función $f : (0,1)^m \to (0,1)$ es (A,C)-mild si es de clase C^∞ y para todo $\mathbf{x} \in (0,1)^m$ y todo $\mu = (\mu_1,\ldots,\mu_m) \in \mathbb{N}^m$ tenemos

$$|\partial^\mu f(x)| \leq \mu!(A|\mu|^C)^{|\mu|}. \tag{4.10}$$

Aquí $\mu! := \mu_1 \cdots \mu_m$ y $|\mu| = \sum_{i=1}^m \mu_i$, y estamos asumiendo $0^0 = 1$ con lo que (4.10) vale automáticamente para $\mu = 0$.

Definición 4.11 (Mild parametrization). Sea $X \subseteq (0,1)^n$ de dimensión k. Una parametrización (J,G)-mild de X es una colección finita de funciones Φ tal que cada $\phi \in \Phi$ es G-mild, $|\Phi| = J$, y

$$X = \bigcup_{\phi\in\Phi} \text{range}(\phi). \tag{4.11}$$

Si una tal Φ existe decimos que X tiene una parametrización G-mild. Si $G(n) = n!(An^C)^n$ para algún A y C, una parametrización (J,G)-mild se dice una parametrización (J,A,C)-mild.

La observación clave de Pila es que si un conjunto X tiene una parametrización(J,A,C)-mild entonces los puntos racionales de X están cubiertos por pocas hipersuperficies.

Teorema 4.12 ([**Pil10**, Corollary 3.3]). *Supongamos que $X \subseteq (0,1)^n$ es un conjunto definible de dimensión k y que tiene una parametrización (J,A,C)-mild. Sea f un entero positivo y $F \subseteq \mathbb{R}$ un cuerpo de números de grado f sobre $\mathbb{Q}$. Entonces $X(F,T)$ está contenido en a lo sumo*

$$Jc(k,n)^f A^{(k+1)(1+o(1))} \left(f\log(T)\right)^{C\left(\frac{n(k+1)}{n-k}\right)(1+o(1))} \tag{4.12}$$

intersecciones de X con hipersurperficies (posiblemente reducibles) de grado

$$d = \left\lfloor (f\log(T))^{\frac{k}{n-k}} \right\rfloor, \tag{4.13}$$

donde $c(k,n)$ es una constante positiva explícita, y "$1+o(1)$" es tomado tomando $T \to +\infty$ con constantes implícitas dependiendo sólo en k,n.

Remarquemos que la hipótesis que $X \subseteq (0,1)^n$ siempre puede obtenerse, mediante composición de las funciones $x \mapsto \pm x^{\pm 1}$, y notando que la altura es estable bajo estas funciones.

El Teorema 4.12 motiva las siguientes dos conjeturas, ambas formuladas por Pila en [**Pil10**].

Conjetura 4.13 ([**Pil10**, Conjecture 2.5]). Todo conjunto $X \subseteq (0,1)^n$ definible en $\mathbb{R}_{\exp}$ tiene una parametrización mild.

Conjetura 4.14 ([**Pil10**, Conjecture 3.4]). Sea $Y \subseteq (0,1)^n$ definible en $\mathbb{R}_{\exp}$. Existen constantes positivas C_1, C_2, C_3, C_4, C_5 dependiendo sólo en Y con la siguiente propiedad. Sea $\mathcal{F}$ una familia algebraica de conjuntos algebraicos cerrados en $\mathbb{R}^n$ de grado $d = d(\mathcal{F})$, y supongamos que $V \in \mathcal{F}$. Entonces $Y \cap V$ es $(C_2 d^{C_3}, C_4 d^{C_5}, C_1)$-mild.

Es claro que la Conjetura 4.14 es más fuerte que la Conjetura 4.13. Además, Pila prueba en [**Pil10**, Corollary 4.5] que la Conjetura 4.14 implica la Conjetura 4.2. Sin embargo, incluso la Conjetura 4.13 permanece abierta, y se espera que sea muy difícil. Hay varias razones para esto. La primera, que la Conjetura 4.13 sólo se conoce para los reductos de $\mathbb{R}_{\text{an}}$ que son expansiones del cuerpo real ordenado (ver [**JMT11**, Proposition 0.2]). La segunda razón, es que en general, una estructura o-minimal con muy buenas propiedades puede tener conjuntos sin parametrizaciones mild.

Teorema 4.15 ([**Tho11**, Theorem 1.7]). *Para toda función $G : \mathbb{N} \to (0, \infty)$, existe una estructura o-minimal, polinomialmente acotada $\tilde{\mathbb{R}}$ que es una expansión model complete del cuerpo ordenado real con descomposición en celdas analíticas y un conjunro $X \subseteq (0,1)^2$ definible en $\overline{\mathbb{R}}$ de dimensión* 1 *tal que X no tiene una parametrización G-mild.*

El Teorema 4.15 es un resultado muy negativo, pues las estructuras o-minimales que son polinomialmente acotadas, model complete, con descomposición en celdas analíticas están entre las estructuras con mejor comportamiento. Entonces, si la Conjetura 4.13 vale, cualquier prueba de la conjetura debe usar alguna propiedad específica de $\mathbb{R}_{\exp}$.

3. Funciones Pfaffianas

En esta sección vamos a recordar propiedades básicas de las funciones Pfaffianas que vamos a requerir para nuestro trabajo en la conjetura de Wilkie. Las referencias son la tesis de Khovanskii [**Kho91**] y el artículo [**GV04**]. Primero, recordemos la noción de una cadena Pfaffiana (real) y una función Pfaffiana (real).

Definición 4.16. Una cadena Pfaffiana de orden $r \geq 0$ y grado $\alpha \geq 1$ en un dominio abierto $G \subseteq \mathbb{R}^n$ es una sucesión de funciones analíticas $f_1, \ldots, f_r$ en G satisfaciendo ecuaciones diferenciales

$$df_j(\mathbf{x}) = \sum_{1 \leq i \leq n} g_{ij}((\mathbf{x}, f_1(\mathbf{x}), \ldots, f_j(\mathbf{x}))dx_i \tag{4.14}$$

para $1 \leq j \leq r$. Aquí $g_{ij}(\mathbf{x}, y_1, \ldots, y_j)$ son polinomios en $\mathbf{x} = (x_1, \ldots, x_n)$, $y_1, \ldots, y_j$ de grado no excediendo α. Una función $f(\mathbf{x}) = P(\mathbf{x}, f_1(\mathbf{x}), \ldots, f_r(\mathbf{x}))$, donde $P(\mathbf{x}, y_1, \ldots, y_r)$ es un polinomio de grado no excediendo $\beta \geq 1$, se dice una función Pfaffiana de orden r y grado (α, β). Notemos que una función Pfaffiana f está definida sólo en el dominio G donde todas las funciones $f_1, \ldots, f_r$ son analíticas, aún si f misma puede extenderse como función analítica en un dominio más grande.

Ejemplo 4.17. Aquí proveemos algunos ejemplos básicos de funciones Pfaffianas.

(I) Las funciones Pfaffianas de orden 0 y grado $(1, \beta)$ son polinomios de grado no excediendo β.

(II) La función exponencial $f(x) = e^{ax}$ es una función Pfaffiana de orden 1 y grado $(1, 1)$ en $\mathbb{R}$, debido a la ecuación $df(x) = af(x)dx$. Más en general, para $i = 1, 2, \ldots, r$, sea

$E_i(x) := e^{E_{i-1}(x)}$, $E_0(x) = ax$. Entonces $E_r(x)$ es una función Pfaffiana de orden r y grado $(r, 1)$, pues $dE_r(x) = aE_1(x) \dots E_r(x)dx$.

(III) La función $f(x) = 1/x$ es una función Pfaffiana de orden 1 y grado $(2, 1)$ en el dominio $\{x \in \mathbb{R} : x \neq 0\}$, debido a la ecuación $df(x) = -f^2(x)dx$.

(IV) La funciónlogaritmo $f(x) = \log(|x|)$ es una función Pfaffiana de orden 2 y grado $(2, 1)$ en el dominio $\{x \in \mathbb{R} : x \neq 0\}$, debido a las ecuaciones $df(x) = g(x)dx$ y $dg(x) = -g^2(x)dx$, donde $g(x) = 1/x$.

(V) La función $f(x) = x^\alpha$ con $\alpha \neq 0$ puede verse como una función Pfaffiana de orden 2 y grado $(2, 1)$ en el dominio $\{x \in \mathbb{R} : x \neq 0\}$ (pero no en $\mathbb{R}$), debido a las ecuaciones $df(x) = \alpha f(x)g(x)$ y $dg(x) = -g^2(x)dx$, donde $g(x) = 1/x$.

Recordemos algunas propiedades básicas de las funciones Pfaffianas.

Lema 4.18 ([**GV04**, Lemma 2.4]). *La suma (resp. producto) de dos funciones Pfaffianas f_1 y f_2 de órdenes r_1 y r_2 y grados (α_1, β_1) y (α_2, β_2) respectivamente, es una función Pfaffiana de orden $r_1 + r_2$ y grado $(\alpha, \max\{\beta_1, \beta_2\})$ (resp. $(\alpha, \beta_1 + \beta_2)$), donde $\alpha = \max\{\alpha_1, \alpha_2\}$. Si dos funciones están definidas por la misma cadena Pfaffiana de orden r, entonces los órdenes de la suma y del producto coinciden con r.*

Lema 4.19 ([**GV04**, Lemma 2.5]). *Una derivada parcial de una función Pfaffiana de orden r y grado (α, β) es una función Pfaffiana que tiene la misma cadena Pfaffiana de orden r y grado $(\alpha, \alpha + \beta - 1)$.*

Ahora volvemos al resultado fundacional de la teoría de funciones Pfaffianas, que es que el número de componentes conexas[1] de una variedad Pfaffiana está acotada en términos de la complejidad de las funciones Pfaffianas definiendo la variedad.

Teorema 4.20 (Khovanskii, [**GV04**, Corollary 3.3]). *Consideremos un sistema de ecuaciones $f_1 = \cdots = f_k = 0$, donde f_i, $1 \leq i \leq k$ son funciones Pfaffianas en un dominio $G \subseteq \mathbb{R}^n$, teniendo una cadena Pfaffiana común de orden r y grados (α, β_i) respectivamente. Entonces el número de componentes conexas de $X := \{f_1 = \cdots = f_k = 0\}$ no excede*

$$2^{r(r-1)/2+1}\beta(\alpha + 2\beta - 1)^{n-1}((2n-1)(\alpha+\beta) - 2n + 2)^r, \tag{4.15}$$

donde $\beta := \max_{1 \leq i \leq k}\{\beta_i\}$.

El otro resultado que usaremos es una estratificación efectiva de Gabrielov-Vorobjov para conjuntos más generales que ceros de funciones Pfaffianas.

Definición 4.21 (Conjunto semi-Pfaffiano). Un conjunto $X \subseteq \mathbb{R}^n$ se dice semi-Pfaffiano en un dominio abierto $G \subseteq \mathbb{R}^n$ si consiste de puntos en G satisfaciendo una combinación Booleana $\mathcal{F}$ de algunas ecuaciones y desigualdades atómicas $f = 0$, $g > 0$, con f, g funciones Pfaffianas teniendo una cadena Pfaffiana común definida en G. Escribimos $X = \{\mathcal{F}\}$. Un conjunto semi-Pfaffiano se dice básico si la combinación Booleana es sólo una conjunción de ecuaciones y desigualdades estrictas, i.e. un conjunto de la forma

$$\mathbf{x} \in \mathbb{R}^n : f_1(\mathbf{x}) = \cdots = f_I(\mathbf{x}) = 0, g_1(\mathbf{x}) > 0, \dots, g_J(\mathbf{x}) > 0\}, \tag{4.16}$$

[1]Vale una afirmación más fuerte: se puede acotar la suma de los números de Betti de un conjunto semi-Pfaffiano en términos de la complejidad de las funciones Pfaffianas definiéndolo. Ver [**GV04**, Theorem 3.4]

donde $f_1, \ldots, f_I, g_1, \ldots, g_J : G \to \mathbb{R}$ son funciones Pfaffianas. Si estas funciones tienen una misma cadena de orden r y grado (α, β), decimoes que el conjunto (4.16) tiene formato [2] (I, J, r, α, β).

Para un conjunto básico Pfaffiano (4.16) de formato (I, J, r, α, β), y un número real dado t, definimos

$$B(t) := (\alpha + \beta + 1)^{(r+1)^m}. \tag{4.17}$$

Teorema 4.22 ([**GV04**, Theorem 6.2]). *Existe una constante absoluta c tal que lo siguiente vale. Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto semi-Pfaffiano con formato (I, J, r, α, β). Entonces existe una partición de X en a lo sumo $I^n B(c)$ conjuntos semi-Pfaffianos básicos, con todas las funciones involucradas teniendo la misma cadena que las funciones definiendo X, y el formato de cada estrato de la partición está acotado coordenada a coordenada por $(I^n B(c), K + 2^n, r, \alpha, B(c))$. Además, para cada estrato Y de codimensión m, existen, entre las funciones definiendo Y, algunas $h_1, \ldots, h_m$ anulándose idénticamente a lo largo de Y tales que $dh_1 \wedge \cdots dh_m \neq 0$ en cada punto de Y.*

4. Conjuntos definibles como conjuntos mal distribuidos

4.1. Una conjetura local-global. Como intento para probar la Conjetura 4.2 y su generalización la Conjetura 4.3, proponemos las siguientes conjeturas. En lo que sigue, $\tilde{\mathbb{R}} = (\mathbb{R}, <, +, -, \cdot, f_1, \ldots, f_r)$ es una expansión model complete del cuerpo real por una función Pfaffiana $f_1, \ldots, f_r$. Además, si $X \subseteq \mathbb{R}^n$, vamos a denotar $\tilde{X}$ para la imagen de X en $\mathbb{P}^n(\mathbb{R})$ por el embedding $\mathbf{x} \mapsto (1 : \mathbf{x})$. También recordemos la noción de la parte algebraica de un conjunto.

Definición 4.23 (Parte algebraica de un conjunto). Sea $X \subseteq \mathbb{R}^n$ un conjunto definible en una estructura o-minimal. La parte algebraica de X, que denotamos X^{alg}, es el conjunto de puntos $\mathbf{x} \in X$ para los cuales existe un conjunto semi-algebraico, conexo $Y \subseteq X$ de dimensión positiva con $\mathbf{x} \in Y$. Definimos la parte trascendente de X como el complemento $X^{\text{trans}} = X \backslash X^{\text{alg}}$.

La primera conjetura que afirmamos nos dice que todo el conjunto $X(K)$ es esparso al nivel de clases residuales módulo muchos primos.

Conjetura 4.24 (Conjetura de mala distribución A). Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en la estructura o-minimal $\tilde{\mathbb{R}}$. Entonces existen constantes positivas $\alpha = \alpha_1(X, K)$, $\tau = \tau(X, K)$, $\kappa = \kappa(X)$, con $0 \leq \kappa < n$ tales que

$$\left| \left(\widetilde{X(K, N)} \right)_{\mathfrak{p}} \right| \leq \alpha \mathcal{N}(\mathfrak{p})^{\kappa} \tag{4.18}$$

para todo $N > e$ y todo ideal primo $\mathfrak{p}$ con $\mathcal{N}(\mathfrak{p}) \geq \tau(\log(N))^{\frac{n}{n-\kappa}}$.

Una conjetura menos fuerte que la Conjetura 4.24 sería que el conjunto $X^{\text{trans}}(K)$ es ralo al nivel de clases residuales:

Conjetura 4.25 (Conjetura de mala distribución B). Supongamos que $X \subseteq \mathbb{R}^n$ es un conjunto definible en una estructura o-minimal $\tilde{\mathbb{R}}$. Entonces existen constantes positivas $\alpha = \alpha_1(X, K)$, $\tau = \tau(X, K)$, $\kappa = \kappa(X)$, con $0 \leq \kappa < n$ tales que

$$\left| \left(\widetilde{X^{\text{trans}}(K, N)} \right)_{\mathfrak{p}} \right| \leq \alpha \mathcal{N}(\mathfrak{p})^{\kappa} \tag{4.19}$$

[2] De hecho, en [**GV04**] el formato sería (r, N, α, β, n) donde $N \geq I + J$. Aquí seguimos a [**JT12**], pues la dimensión del espacio ambiente será conocida.

para todo $N > e$ y para todo ideal primo $\mathfrak{p}$ with $\mathcal{N}(\mathfrak{p}) \geq \tau(\log(N))^{\frac{n}{n-\kappa}}$.

Observación 4.26. Es claro que la Conjetura 4.24 implica la Conjetura 4.25. Además, notemos que en general, no podemos esperar que la Conjetura 4.24 y la Conjetura 4.25 valgan para todo primo $\mathfrak{p}$. En efecto, toemos $f(x) = 2^x$ y consideremos el gráfico de f. Entonces si $K = \mathbb{Q}$ y $p \ll \log\log(N)$ es un primo, $|X(\mathbb{Z}, N)_p| \sim pu_p$, donde u_p es el orden de 2 en $(\mathbb{Z}/p\mathbb{Z})^\times$. Como esperamos que $u_p = p - 1$ para muchos primos, esperamos $|(X^{\text{trans}}(\mathbb{Z}, N))_p| = |X(\mathbb{Z}, N)_p| \sim p^2$ para muchos primos $p \ll \log\log(N)$.

Observación 4.27. Por el Teorema 4.12 y la estimación de Schwarz-Zippel, los puntos racionales de un conjunto definible en $\tilde{\mathbb{R}}$ con una "mild parametrization" satisface la Conjetura 4.24. Más aún, podemos afirmar una versión uniforme de la Conjetura 4.24, análoga en uniformidad a la Conjetura 4.14.

Conjetura 4.28 (Conjetura de mala distribución uniforme). Sea $X \subseteq \mathbb{R}^n$ definible en $\tilde{\mathbb{R}}$. Existe una constante positiva $c = c(X)$, tal que para toda variedad dada $V \subseteq \mathbb{R}^n$ definida por polinomios de grado a lo sumo $d = d(V)$, tal que $\dim(X \cap V) < \dim(V)$, existe una constante positiva $\alpha = \alpha(X, K, d)$, que depende polinomialmente de d, constantes positivas $\tau = \tau(X, K)$, $\kappa = \kappa(\dim(V), \dim(V \cap X), X)$, con $0 \leq \kappa < \dim(V)$ tales que

$$\left|\left(\widetilde{(X \cap V)}(K, N)\right)_{\mathfrak{p}}\right| \leq \alpha \mathcal{N}(\mathfrak{p})^\kappa \tag{4.20}$$

para todo ideal primo $\mathfrak{p}$ con $\mathcal{N}(\mathfrak{p}) \geq \tau(\log(N))^{\frac{n}{n-\kappa}}$.

Ahora vamos a probar que la Conjetura 4.25 es equivalente a la Conjetura 4.3 para conjuntos de dimensión a lo sumo 2. Para hacer esto, requerimos una reducción. Primero mostramos que para probar la Conjetura 4.3 para conjuntos de dimensión n, es suficiente trabajar con gráficos de funciones definibles $\phi : U \to \mathbb{R}$, donde $U \subseteq \mathbb{R}^{n-1}$ es una celda analítica.

Lema 4.29 (Reducción al gráfico de funciones). *Sea $n \geq 1$ un entero positivo. Supongamos que la Conjetura 4.3 vale para conjuntos $X \subseteq \mathbb{R}^n$ los cuáles son gráficos de funciones analíticas $\phi : U \subseteq \mathbb{R}^i \to \mathbb{R}$ definibles en $\tilde{\mathbb{R}}$, para todo $1 \leq i < n$, con U una celda abierta analítica. Entonces todo conjunto $X \subseteq \mathbb{R}^m$ de dimensión n satisface la Conjetura 4.3.*

Demostración. La prueba sigue el argumento delineado en [**But12**, Page 646], que también aparece en la prueba del Teorema 4.1 en [**PW06**]. Argumentamos por inducción en n, el caso $n = 1$ siendo trivial. Sea $X \subseteq \mathbb{R}^m$ un conjunto definible en $\tilde{\mathbb{R}}$ de dimensión n y fijemos un cuerpo de números $K \subseteq \mathbb{R}$. Si $(x_1, \ldots, x_n)$ denota las coordenadas de $\mathbb{R}^n$, proyectamos X en cada plano coordenado $(x_{i_1}, \ldots, x_{i_{n+1}})$ con $i_1 < ldots < i_{n+1}$, obteniendo $\binom{m}{n+1}$ subconjuntos de $\mathbb{R}^{n+1}$, digamos X_i para $1 \leq i \leq \binom{m}{n+1}$. Estos subconjuntos son todos definibles y si $\mathbf{x} \in X(K)$ entonces la imagen de $\mathbf{x}$ bajo estas proyecciones estará en K^n, por lo tanto no perdemos ningún punto algebraico en este proceso. Más aún si $\mathbf{x} \in X^{\text{trans}}$ entonces la imagen de $\mathbf{x}$ bajo estas proyecciones debe estar en X_i^{trans} para al menos un i, pues si X_i es semi-algebraico alrededor de $\mathbf{x}$ para todo i entonces X mismo debe ser semi-algebraico alrededor de $\mathbf{x}$, por lo tanto $\mathbf{x} \notin X^{\text{trans}}$.

Ahora, X_i es un conjunto definible en $\tilde{\mathbb{R}}$. Dado que $\tilde{\mathbb{R}}$ admite descomposición en celdas analíticas (ver Capítulo 1), tenemos que cada X_i es una unión finita de celdas analíticas, que son el gráfico de funciones analíticas definibles $\phi : C \to \mathbb{R}$ donde $C \subseteq \mathbb{R}^n$ es una celda analítica, o bien son de la forma $(f, g)_C = \{(\mathbf{x}, y) \in \mathbb{R}^{n+1} : \mathbf{x} \in C \text{ y } f(\mathbf{x} < y < g(\mathbf{x}))\}$, con $C \subseteq \mathbb{R}^n$ una celda analítica y $f, g : C \to \mathbb{R}$ funciones analíticas definibles. Notemos que las últimas celdas satisfacen

$(f,g)_C^{\text{alg}} = (f,g)_C$, con lo que la única contribución a $X_i^{\text{trans}}(K,N)$ proviene de las celdas que son gráficos de funciones analíticas definibles $\phi : C \subseteq \mathbb{R}^n \to \mathbb{R}$. Si C es una celda anaítica abierta, entonces el gráfico de ϕ satisface la Conjetura 4.3. Si C es una celda analítica de dimensión estrictamente más pequeña que n, el gráfico de ϕ es un subconjunto definible de $\mathbb{R}^{n+1}$ de dimensión a lo sumo $n-1$, por lo tanto satisface la Conjetura 4.3 por inducción. concluimos

$$|X_i^{\text{trans}}(K,T)| \leq c_1(X_i,K)(\log(T))^{c_2(X_i)}. \tag{4.21}$$

Notemos que las constantes $c_1(X_i,K)$ dependen en X, i.e. podemos tomar $c_1(X_i,K) = c_1(X,K)$. Por lo tanto, arribamos a la desigualdad

$$|X^{\text{trans}}(K,T)| \leq \sum_{i=1}^{\binom{m}{n}} |X_i^{\text{trans}}(K,T)| \leq c_1(X,K)(\log(T))^{c_2(X)}. \tag{4.22}$$

□

El Lema 4.29 dice que para estudiar la Conjetura 4.3, necesitamos probar la Conjetura 4.3 para gráficos de funciones analíticas definibles $\phi : U \to \mathbb{R}$ con U una celda analítica abierta. Para poder estudiar estas funciones, requerimos una herramienta adicional de Teoría de Modelos.

4.2. Estructuras localmente polinomialmente acotadas. Recordemos la noción de una estructura o-minimal polinomialmente acotada.

Definición 4.30 (Estructuras polinomialmente acotadas). Una estructura $(\mathbb{R},\mathcal{S})$ expandiendo el cuerpo real ordenado se dice polinomialmente acotada si toda función definible $f : \mathbb{R} \to \mathbb{R}$ es eventualmente acotada por un polinomio. Más precisamente para toda $f : \mathbb{R} \to \mathbb{R}$ definible existe $x_0 \in \mathbb{R}$ y $n \in \mathbb{N}$ tal que si $x > x_0$, se tiene $|f(x)| \leq x^n$.

Notemos que los conjuntos semi-algebraicos son una estructura o-minimal polinomialmente acotada (esto se sigue de [**BCR87**, Proposition 2.6.1]), y más aún, cualquier reducto de $\mathbb{R}_{\text{an}}$ es polinomialmente acotada (ver [**vdD86**]). En contraste, $\mathbb{R}_{\text{exp}}$ no es polinomialmente acotada, pues la exponencial no puede ser acotada por ningún polinomio. Por otro lado, estructura o-minimal es polinomialmente acotada si y sólo si la exponencial no es definible (ver [**Mil94**]). Sin embargo, $\mathbb{R}_{\text{exp}}$ resulta que es localmente polinomialmente acotada, una noción introducida en [**JW08**] por Jones y Wilkie. Para definir esta propiedad, vamos a usar la siguiente notación. Dada una familia $\mathcal{F}$ de funciones suaves $f : \mathbb{R}^n \to \mathbb{R}$, para varios n, denotamos $\mathcal{F}^{\text{res}}$ para la colección de todas las funciones de la forma $f|_B$ con $f \in \mathcal{F}$ y B una caja abierta en $\mathbb{R}^n$.

Definición 4.31 (Estructuras localmente polinomialmente acotadas, ver [**JW08**]). Una estructura o-minimal $(\mathbb{R},<,+,-,\cdot,0,1,\mathcal{F}^{\text{res}})$ donde $\mathcal{F}$ es una familia de funciones suaves $f : \mathbb{R}^n \to \mathbb{R}$, para varios n, se dice localmente polinomialmente acotada si tiene una teoría model complete, y la estructura $(\mathbb{R},<,+,-,\cdot,0,1,\mathcal{F}^{\text{res}})$ es polinomialmente acotada.

Por lo tanto, $\mathbb{R}_{\text{exp}}$, y más en general toda expansión model complete o-minimal $\tilde{\mathbb{R}}$ como en la Conjetura 4.3, es una estructura localmente polinomialmente acotada. La propiedad que vamos a usar de las estructuras localmente polinomialmente acotadas que fue observada en [**JW08**] es que una función definible en una tal estructura está esencialmente definida de manera implícita por funciones adecuadas. Para ser más precisos, primero damos la siguiente noción.

Definición 4.32 (Funciones definidas de manera implícita). Sea $(\mathbb{R}, <, +, -, \cdot, 0, 1, \mathcal{F})$ una estructura o-minimal localmente polinomialmente acotada. Definimos $\tilde{\mathcal{F}}$ como la menor colección de funciones conteniendo $\mathcal{F}$ y todos los polinomios sobre $\mathbb{Q}$, que es cerrada bajo las operaciones de $\mathbb{Q}$-álgebra y bajo diferenciación parcial. Para cada n, sea R_n la $\mathbb{Q}$-álgebra consistiendo de todas las funciones n-arias en $\tilde{\mathcal{F}}$. Entonces $f : U \to \mathbb{R}$, donde $U \subseteq \mathbb{R}^n$ es abierto, está definida de manera implícita sobre $\mathcal{F}$ si existe $m \geq 1$, funciones $g_1(\mathbf{x}, \mathbf{y}), \ldots, g_m(\mathbf{x}, \mathbf{y}) \in R_{n+m}$ y funciones definibles $\phi_1, \ldots, \phi_m : U \to \mathbb{R}$ tales que

(1) $f = \phi_i$ para algún $i = 1, \ldots, m$,
(2) $g_i(\mathbf{x}, \mathbf{y}, \phi_1(\mathbf{x}, \mathbf{y}), \ldots, \phi_m(\mathbf{x}), \mathbf{y}) = 0$ para todo $1 \leq i \leq m$,
(3) $\det\left(\dfrac{\partial(g_1, \ldots, g_n)}{\partial \mathbf{y}}\right)(\mathbf{x}, \mathbf{y}, \phi_1(\mathbf{x}, \mathbf{y}), \ldots, \phi_m(\mathbf{x}, \mathbf{y})) \neq 0.$

Cuando $\mathcal{F} = \{f_1, \ldots, f_r\}$ es una cadena Pfaffiana, los $g_1, \ldots, g_m$ son funciones Pfaffianas con cadena común $f_1, \ldots, f_r$. En este caso, decimos que f está definida de manera implícita por funciones Pfaffianas con cadena común $f_1, \ldots, f_r$.

Ahora podemos enunciar la consecuencia del hecho que $\tilde{\mathbb{R}} = (\mathbb{R}, <, +, -, \cdot, 0, 1, f_1, \ldots, f_r)$ sea localmente polinomialmente acotada, con $f_1, \ldots, f_r$ una cadena Pfaffiana.

Teorema 4.33 ([**JW08**, Corollary 3.5]). *Sea $f : U \to \mathbb{R}$ una función definible en $\tilde{\mathbb{R}}$, con $U \subseteq \mathbb{R}^n$ un conjunto abierto. Entonces existen abiertos $U_1, \ldots, U_k \subseteq U$ con $\dim(U \setminus \bigcup_{i=1}^n U_i) < n$ tales que $f|_{U_i}$ está definida de manera implícita por funciones Pfaffianas con cadena común $f_1, \ldots, f_r$.*

Del Teorema 4.33 y el Teorema 4.29 deducimos:

Lema 4.34 (Reducción a gráficos de funciones definidas de manera implícita por funciones Pfaffianas). *Sea $n \geq 1$ un entero positivo. Supongamos que la Conjetura 4.3 vale para conjuntos $X \subseteq \mathbb{R}^n$ los cuales son gráficos de funciones analíticas $\phi : U \subseteq \mathbb{R}^i \to \mathbb{R}$ definibles in $\tilde{\mathbb{R}}$, para todo $1 \leq i < n$, con U una celda analítica abierta, que están definidas de manera implícita por funciones Pfaffianas. Entonces todo conjunto $X \subseteq \mathbb{R}^m$ de dimensión n satisface la Conjetura 4.3.*

Proof. Esto se sigue del Teorema 4.29 y el Teorema 4.33 aplicado a cada función $\phi : U \to \mathbb{R}$. □

La razón por la cuál el Teorema 4.33 será útil para nosotros es que la intersección del gráfico de una función $f : U \subseteq \mathbb{R}^2 \to \mathbb{R}$ definida de manera implícita por funciones Pfaffianas con una hipersuperficie tiene un buen comportamiento:

Teorema 4.35 ([**JT12**, Lemma 3.3, Proposition 5.3]). *Sea $\tilde{\mathbb{R}} = (\mathbb{R}, <, +, -, \cdot, 0, 1, f_1, \ldots, f_r)$ una expansión o-minimal del cuerpo real ordenado, con $f_1, \ldots, f_r$ una cadena Pfaffiana. Sea $i = 2$ o 3, y sea $f : U \subseteq \mathbb{R}^i \to \mathbb{R}$ una función definida de manera implícita por funciones Pfaffianas, con U una celda analítica abierta. Existen constantes positivas $c_1 = c_1(K)$, $c_2 = c_2(f)$ y un polinomio $Q \in \mathbb{R}[t]$ de grado $O_f(1)$ con coeficientes acotados por $O_f(1)$, tal que para todo polinomio $P \in \mathbb{R}[X_j]_{1 \leq j \leq i+1}$ de grado d, se tiene*

$$|(X \cap V(P))^{trans}(K, T)| \leq c_1(K) Q(d) (\log(T))^{c_2}. \tag{4.23}$$

Observación 4.36. El caso $i = 2$ en el Teorema 4.35 se sigue inmediatamente de las cotas de Khovanskii (ver Teorema 4.20). Mientras tanto, cuando $i = 2$, se sigue del Teorema 4.22, pero la prueba no es trivial.

4.3. Equivalencia entre la Conjetura 4.3 y la Conjetura 4.25. Ahora podemos probar el resultado principal de este capítulo.

Teorema 4.37 ([**Par19**, Theorem 4.3]). *Sea $X \subseteq \mathbb{R}^n$ un conjunto definible en $\tilde{\mathbb{R}}$ de dimensión a lo sumo 2. Entonces X verifica la Conjetura 4.25 si y sólo si X verifica la Conjetura 4.3.*

Demostración. Notemos que si $n = 1$, ambas conjeturas son triviales. Supongamos entonces que $n > 1$. Empezamos probando que la Conjetura 4.3 implica la Conjetura 4.25 sin la restricción en la dimensión de X.

Supongamos que la Conjetura 4.3 vale para algún conjunto $X \subseteq \mathbb{R}^n$ con $n > 1$ definible en $\tilde{\mathbb{R}}$. Podemos suponer que $c_2 \geq \frac{n}{n-1}$. Tomemos κ de manera que $\frac{n}{n-\kappa} = c_2$ y $\kappa \geq 1$. Entonces si $\mathfrak{p}$ es un primo en O_K tal que $N(\mathfrak{p}) \geq c_1(\log(N))^{n/(n-\kappa)} = c_1(\log(N))^{c_2}$, tenemos que

$$\left|\left(\tilde{X}^{\text{trans}}(K,N)\right)_{\mathfrak{p}}\right| \leq |X^{\text{trans}}(K,N)| \leq c_1(\log(N))^{c_2} \leq N(\mathfrak{p}) \leq N(\mathfrak{p})^{\kappa}. \tag{4.24}$$

Tomando $\alpha = 1$, $\kappa = \frac{c_2-1}{c_2}n$ y $\tau \geq c_1$, concluimos que X satisface la Conjetura 4.25.

Para la otra implicación, por el Lema 4.34 podemos suponer que X es el gráfico de una función analítica $\phi : U \subseteq \mathbb{R}^i \to \mathbb{R}$ definible en $\tilde{\mathbb{R}}$, definida de manera implícita por funciones Pfaffianas, con U una celda analítica abierta. Por hipótesis, X satisface la Conjetura 4.25, por lo tanto podemos aplicar el Corolario 3.23 con $\varepsilon = \frac{1}{2}$ a $X^{\text{trans}}(K,N)$, para hallar un polinomio no nulo $Q \in O_K[T_j]_{1\leq j\leq i+1}$ de grado a lo sumo $\ll_{\kappa,K} (\log(N))^{\frac{\kappa}{i+1-\kappa}}$ anulándose en al menos la mitad de los puntos de $X^{\text{trans}}(K,N)$. Esto quiere decir que

$$\left|X^{\text{trans}}(K,N) \cap V(Q)\right| \geq \frac{1}{2}|X^{\text{trans}}(K,N)|. \tag{4.25}$$

Ahora, notemos que

$$X^{\text{trans}}(K,N) \cap V(Q) \subseteq (X \cap V(Q))^{\text{trans}}(K,N). \tag{4.26}$$

Por el Teorema 4.35, tenemos que para todo polinomio no nulol $P \in \mathbb{R}[X_j]_{1\leq j\leq i+1}$ de grado d se verifica la cota

$$\left|(X \cap V(P))^{\text{trans}}(K,N)\right| \leq c_1(X,K)d^{c_2(X)}(\log(N))^{c_3(X)}, \tag{4.27}$$

donde $c_1(X,K)$, $c_2(X)$, $c_3(X)$ son constantes positivas efectivas. Aplicando (4.27) al polinomio Q que construimos, y usando (4.25) y (4.26) concluimos que X satisface la Conjetura 4.3. □

Observación 4.38. La razón técnica por la cuál la prueba del Teorema 4.37 vale sólo para conjuntos de dimensión a lo sumo 2 es porque usamos Teorema 4.35 que no parece generalizarse a conjuntos de dimensión superior a 2. Esto se debe a la naturaleza inductiva de la prueba del teorema y de los conjuntos definibles en una estructura o-minimal. Específicamente, si partimos de un conjunto definible $X \subseteq \mathbb{R}^3$ de dimensión a lo sumo 2, cuya complejidad está controlada, entonces su intersección con una hipersuperficie $V(P)$ en general tendrá dimensión a lo sumo 1 (caso contrario $X \cap V(P)$ es de naturaleza algebraica y en consecuencia $(X \cap V(P))^{\text{trans}} = \emptyset$). La cantidad de estratos de $X \cap V(P)$ y su complejidad está controlada en términos de la complejidad de X y el grado de P (esto es consecuencia del Teorema 4.22). Puesto que la conjetura de Wilkie es conocida para conjuntos de dimensión 1, de manera uniforme en la complejidad del conjunto (ver [**But12**, Thm 3.5] y [**JT12**, Prop. 4.3]), deducimos que $X \cap V(P)$ satisface la conjetura de Wilkie.

Supongamos ahora que $X \subseteq \mathbb{R}^4$ es un conjunto de dimensión al menos 3. Entonces, para toda hipersuperficie $V(P)$ se tiene que $X \cap V(P)$ tiene en general dimensión a lo sumo 2. De nuevo, la

cantidad y la complejidad de los estratos de $X \cap V(P)$ está controlada por el Teorema 4.22. Si un estrato de $X \cap V(P)$ tiene dimensión a lo sumo 1, entonces como en el caso del párrafo anterior, vamos a tener que satisface la conjetura de Wilkie. Sin embargo, en el caso general van a aparecer estratos E_i de dimensión 2. En esta situación no hay razón por la cual los subconjuntos E_i tienen que satisfacer la conjetura de Wilkie. Aún peor, aunque sepamos que la conjetura de Wilkie vale para conjuntos de dimensión 2, los estratos E_i dependen de la hipersuperficie $V(P)$, con lo que para poder seguir el argumento requerimos que la conjetura de Wilkie valga "uniformemente" en la complejidad de cada E_i, es decir, en la complejidad de X y el grado de P, requiriendo que la dependencia en el grado sea polinomial. Por este motivo la condición que un conjunto X admita una "mild parametrization" o que satisfaga la Conjetura 4.25 no es suficiente para deducir que X satisface la Conjetura 4.3.

Observación 4.39. Del Teorema 4.37 concluimos que la Conjetura 4.24 implica la Conjetura 4.3 para conjuntos de dimensión a lo sumo 2. Más aún, es fácil de ver que la Conjetura 4.28 implica la Conjetura 4.3 para todo conjunto definible en $\tilde{\mathbb{R}}$.

Bibliografía

[BCR87] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle*, volume 12 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1987.

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[BN17] Gal Binyamini and Dmitry Novikov. Wilkie's conjecture for restricted elementary functions. *Ann. of Math. (2)*, 186(1):237–275, 2017.

[BP89] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.

[But12] Lee A. Butler. Some cases of Wilkie's conjecture. *Bull. Lond. Math. Soc.*, 44(4):642–660, 2012.

[But17] Lee A. Butler. A Diophantine approach to the three and four exponentials conjectures. *Ramanujan J.*, 42(1):199–221, 2017.

[BV83] E. Bombieri and J. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[CL07] Ernest S. Croot, III and Vsevolod F. Lev. Open problems in additive combinatorics. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 207–233. Amer. Math. Soc., Providence, RI, 2007.

[Dav80] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1980. Revised by Hugh L. Montgomery.

[Daw15] Christopher Daw. The André-Oort conjecture via o-minimality. In *O-minimality and diophantine geometry*, volume 421 of *London Math. Soc. Lecture Note Ser.*, pages 129–158. Cambridge Univ. Press, Cambridge, 2015.

[DvdD88] J. Denef and L. van den Dries. p-adic and real subanalytic sets. *Ann. of Math. (2)*, 128(1):79–138, 1988.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[Fuk10] Lenny Fukshansky. Algebraic points of small height missing a union of varieties. *J. Number Theory*, 130(10):2099–2118, 2010.

[Ful84] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1984.

[Gab68] A. M. Gabrièlov. Projections of semianalytic sets. *Funkcional. Anal. i Priložen.*, 2(4):18–30, 1968.

[Gro87] M. Gromov. Entropy, homology and semialgebraic geometry. *Astérisque*, (145-146):5, 225–240, 1987. Séminaire Bourbaki, Vol. 1985/86.

[GV04] Andrei Gabrielov and Nicolai Vorobjov. Complexity of computations with Pfaffian and Noetherian functions. In *Normal forms, bifurcations and finiteness problems in differential equations*, volume 137 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 211–250. Kluwer Acad. Publ., Dordrecht, 2004.

[GW10] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry I*. Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010. Schemes with examples and exercises.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[HV09] H. A. Helfgott and A. Venkatesh. How small must ill-distributed sets be? In *Analytic number theory*, pages 224–234. Cambridge Univ. Press, Cambridge, 2009.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Jac74] Nathan Jacobson. *Basic algebra. II*. W. H. Freeman and Co., San Francisco, Calif., 1974.

[JMT11] G. O. Jones, D. J. Miller, and M. E. M. Thomas. Mildness and the density of rational points on certain transcendental curves. *Notre Dame J. Form. Log.*, 52(1):67–74, 2011.

[JT12] G. O. Jones and M. E. M. Thomas. The density of algebraic points on certain Pfaffian surfaces. *Q. J. Math.*, 63(3):637–651, 2012.

[JW08] G. O. Jones and A. J. Wilkie. Locally polynomially bounded structures. *Bull. Lond. Math. Soc.*, 40(2):239–248, 2008.

[Kho91] A. G. Khovanskiĭ. *Fewnomials*, volume 88 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1991. Translated from the Russian by Smilka Zdravkovska.

[KPS01] Teresa Krick, Luis Miguel Pardo, and Martín Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109(3):521–598, 2001.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[LGR09] Olivier Le Gal and Jean-Philippe Rolin. An o-minimal structure which does not admit C^∞ cellular decomposition. *Ann. Inst. Fourier (Grenoble)*, 59(2):543–562, 2009.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[Loi94] Ta Lê Loi. Analytic cell decomposition of sets definable in the structure $\mathbf{R}_{\exp}$. *Ann. Polon. Math.*, 59(3):255–266, 1994.

[Mar10] E. Marchionna, editor. *Questions on algebraic varieties*, volume 51 of *Centro Internazionale Matematico Estivo (C.I.M.E.) Summer Schools*. Springer, Heidelberg; Fondazione C.I.M.E., Florence, 2010. Lectures from the Centro Internazionale Matematico Estivo (C.I.M.E.) Summer School held in Varenna, September 7–17, 1969, Reprint of the 1970 original [MR0271105].

[Mil94] Chris Miller. Exponentiation is hard to avoid. *Proc. Amer. Math. Soc.*, 122(1):257–259, 1994.

[Par19] Marcelo Paredes. Ill-distributed sets over global fields and exceptional sets in Diophantine Geometry. *arXiv e-prints*, page arXiv:1901.00562, January 2019.

[Pil91] J. Pila. Geometric postulation of a smooth function and the number of rational points. *Duke Math. J.*, 63(2):449–463, 1991.

[Pil04] Jonathan Pila. Integer points on the dilation of a subanalytic surface. *Q. J. Math.*, 55(2):207–223, 2004.

[Pil05] Jonathan Pila. Rational points on a subanalytic surface. *Ann. Inst. Fourier (Grenoble)*, 55(5):1501–1516, 2005.

[Pil07] Jonathan Pila. The density of rational points on a Pfaff curve. *Ann. Fac. Sci. Toulouse Math. (6)*, 16(3):635–645, 2007.

[Pil09] Jonathan Pila. On the algebraic points of a definable set. *Selecta Math. (N.S.)*, 15(1):151–170, 2009.

[Pil10] Jonathan Pila. Counting rational points on a certain exponential-algebraic surface. *Ann. Inst. Fourier (Grenoble)*, 60(2):489–514, 2010.

[Pil15] Jonathan Pila. Functional transcendence via o-minimality. In *O-minimality and diophantine geometry*, volume 421 of *London Math. Soc. Lecture Note Ser.*, pages 66–99. Cambridge Univ. Press, Cambridge, 2015.

[PS13] Ya'acov Peterzil and Sergei Starchenko. Definability of restricted theta functions and families of abelian varieties. *Duke Math. J.*, 162(4):731–765, 2013.

[PW06] J. Pila and A. J. Wilkie. The rational points of a definable set. *Duke Math. J.*, 133(3):591–616, 2006.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[RSW03] J.-P. Rolin, P. Speissegger, and A. J. Wilkie. Quasianalytic Denjoy-Carleman classes and o-minimality. *J. Amer. Math. Soc.*, 16(4):751–777, 2003.

[RT96] Damien Roy and Jeffrey Lin Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.

[Sca12] Thomas Scanlon. Counting special points: logic, Diophantine geometry, and transcendence theory. *Bull. Amer. Math. Soc. (N.S.)*, 49(1):51–71, 2012.

[Sch79] Stephen Hoel Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[Sch18] Harry Schmidt. Counting rational points and lower bounds for Galois orbits. *arXiv e-prints*, page arXiv:1802.02192, February 2018.

[Sha74] I. R. Shafarevich. *Basic algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1974. Translated from the Russian by K. A. Hirsch, Die Grundlehren der mathematischen Wissenschaften, Band 213.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[Tho11] Margaret E. M. Thomas. An o-minimal structure without mild parameterization. *Ann. Pure Appl. Logic*, 162(6):409–418, 2011.

[Thu93] Jeffrey Lin Thunder. Asymptotic estimates for rational points of bounded height on flag varieties. *Compositio Math.*, 88(2):155–186, 1993.

[Thu95] Jeffrey Lin Thunder. Siegel's lemma for function fields. *Michigan Math. J.*, 42(1):147–162, 1995.

[TV10] Terence Tao and Van H. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010. Paperback edition [of MR2289012].

[TZ17] Jesse Thorner and Asif Zaman. An explicit bound for the least prime ideal in the Chebotarev density theorem. *Algebra Number Theory*, 11(5):1135–1197, 2017.

[vdD86] Lou van den Dries. A generalization of the Tarski-Seidenberg theorem, and some nondefinability results. *Bull. Amer. Math. Soc. (N.S.)*, 15(2):189–193, 1986.

[vdD98] Lou van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998.

[vdDM94] Lou van den Dries and Chris Miller. On the real exponential field with restricted analytic functions. *Israel J. Math.*, 85(1-3):19–56, 1994.

[VdP68] A. J. Van der Poorten. Transcendental entire functions mapping every algebraic number field into itself. *J. Austral. Math. Soc.*, 8:192–193, 1968.

[Wal12] Miguel N. Walsh. The inverse sieve problem in high dimensions. *Duke Math. J.*, 161(10):2001–2022, 2012.

[Wal14] Miguel N. Walsh. The algebraicity of ill-distributed sets. *Geom. Funct. Anal.*, 24(3):959–967, 2014.

[Wan92] Da Qing Wan. Heights and zeta functions in function fields. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 455–463. de Gruyter, Berlin, 1992.

[Wil96] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc.*, 9(4):1051–1094, 1996.

[Wil99] A. J. Wilkie. A theorem of the complement and some new o-minimal structures. *Selecta Math. (N.S.)*, 5(4):397–421, 1999.

[Yom87] Y. Yomdin. Volume growth and entropy. *Israel J. Math.*, 57(3):285–300, 1987.