UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Caracterización de conjuntos mal distribuidos sobre clases residuales en variedades algebraicas definidas sobre cuerpos globales

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

Juan Manuel Menconi

Director de tesis: Román Sasyk
Consejero de estudios: Fernando Cukierman
Lugar de trabajo: Instituto Argentino de Matemática Alberto P. Calderón y Departamento de Matemática, FCEN, UBA

Caracterización de conjuntos mal distribuidos sobre clases residuales en variedades algebraicas definidas sobre cuerpos globales

Resumen

En esta tesis se estudia la estructura que debe tener un conjunto de puntos racionales de altura acotada, en el sentido de geometría diofántica, que está dentro de una variedad proyectiva, geométricamente irreducible, definida sobre un cuerpo global K, el cual se encuentra mal distribuido en clases residuales para muchos módulos primos. Esto se prueba mediante la siguiente estrategia: primero se reduce el problema al estudio de conjuntos dentro de una variedad afín y luego se prueba como reducir el caso de una variedad afín de dimensión d a un espacio afín de dimensión d. Por tratarse de resultados uniformes en términos del grado y dimensión de la variedad, como paso intermedio, en esta tesis se prueba una versión efectiva del Lema de Normalización de Noether.

El resultado para subconjuntos dentro del espacio afín establece que si un conjunto de puntos con coordenadas en el anillo de enteros de un cuerpo global K, de altura acotada, se encuentra mal distribuido en clases residuales para muchos primos, este comportamiento se debe a que el conjunto es pequeño o bien a que una proporción grande del mismo posee una fuerte estructura algebraica, es decir, es el conjunto de ceros de un polinomio de grado acotado y coeficientes de altura acotada. Esto generaliza resultados de Walsh.

Si bien la teoría de alturas para el caso de cuerpos de números está bien documentada, no sucede así en el caso de cuerpos funcionales. Es por esto que en esta tesis se prueban resultados sobre alturas en cuerpos funcionales. Por ejemplo, se prueba que puntos del espacio proyectivo de altura acotada se pueden levantar a puntos del espacio afín, de altura acotada, y también se da una cota superior para los puntos de altura acotada en el grupo de S-unidades de un cuerpo funcional.

Palabras clave: Conjuntos mal distribuidos en clases residuales, altura en cuerpos globales, variedades sobre cuerpos globales, normalización de Noether efectiva sobre cuerpos globales.

Characterization of badly distributed sets over residual classes in algebraic varieties defined over global fields

Abstract

This thesis studies the structure that a set of rational points of bounded height must have, in the sense of diophantine geometry, contained in a geometrically irreducible projective variety defined over a global field K, badly distributed in residual classes for many prime modules. We prove this using the following strategy: first we reduce the problem to the study of subsets of affine varieties and then we prove how to reduce the case of an affine variety of dimension d to an affine space of dimension d. Since the results are uniform in terms of the degree and dimension of the variety, as an intermediate step, in this thesis an effective version of Noether's Normalization Lemma is proven.

The result for subsets of the affine space states that if a set of points with coordinates in the ring of integers of a global field K, of bounded height, is badly distributed in residual classes for many primes, this behavior is due to the fact that the set is small or because a large proportion of it has a strong algebraic structure, that is, it is the set of zeros of a polynomial of bounded degree and coefficients of bounded height. This generalizes result of Walsh.

Although the theory of heights for the case of number fields is well documented, this is not so in the case of functional fields. This is why in this thesis results for heights in functional fields are proven. For example, it is proven that points of the projective space of bounded height can be lifted to points of the affine space, of bounded height, and an upper bound for the number of points of bounded height in the group of S-units in a functional field.

Keywords: Badly distributed sets in residues classes, heights in global fields, varieties over global fields, effective Noether's normalization over global fields.

Índice general

Introducción

Sea S un conjunto aleatorio de números enteros. En combinatoria aritmética, es habitual establecer "teoremas inversos", en el sentido de que si S posee alguna propiedad aritmética específica, entonces S pertenece a una determinada familia de subconjuntos de enteros; así, se proporciona una clasificación para ese tipo de S. A los efectos de esta tesis, la propiedad aritmética en cuestión a estudiar es la equidistribución del conjunto S. Aquí, por un subconjunto equidistribuido de números enteros S nos referiremos a que S está bien distribuido módulo p para muchos primos p (tenga en cuenta que esto es más débil que estar bien distribuido módulo m para muchos módulos m). Se espera que un conjunto aleatorio S esté bastante bien distribuido. Por lo tanto, un "problema inverso" aquí sería comprender si un conjunto que ocupa pocas clases residuales módulo p para muchos primos p tiene alguna estructura específica. En esta generalidad, esto se ha enunciado de la siguiente manera.

Problema Inverso de Criba (ver [**CL07, HV09**]). *Supongamos que un conjunto $S \subseteq \{0, \dots, N\}^d$ ocupa muy pocas clases residuales módulo p para muchos primos p. Entonces, S es pequeño o posee alguna estructura algebraica fuerte.*

Para dar un ejemplo concreto que motivó este tipo de problema, consideremos un subconjunto $S \subseteq \{0, \dots, N\}$ que satisface que $S_p := \{x \pmod p : x \in S\}$ tiene como mucho αp elementos para muchos primos en el intervalo $[1, N]$, con $0 < \alpha < 1$. La criba de Gallagher (Teorema 1 en [**Gal71**]) implica que $|S| \leq c(\alpha)N^{\alpha}$. Supongamos además que $|S_p| \leq \frac{p-1}{2}$ para todo $p \leq N^{\frac{1}{2}}$. La criba grande implica (ver [**Mon68**])

$$|S| \leq CN^{\frac{1}{2}}, \tag{1}$$

donde C es una constante absoluta. La cota (1) es esencialmente óptima, ya que si consideramos S como el conjunto de los cuadrados que se encuentran en $\{0, \dots, N\}$, vemos que S ocupa como mucho $\frac{1}{2}(p-1)$ clases residuales para todos los primos p y $|S| \sim N^{\frac{1}{2}}$. Más generalmente, si S es la imagen de un polinomio cuadrático $aX^2+bX+c \in \mathbb{Z}[X]$, también tenemos que S ocupa como mucho $\frac{p-1}{2}$ clases residuales para todos los primos p que no dividen al coeficiente principal a y $|S| \sim N^{\frac{1}{2}}$. Por lo tanto, podemos preguntarnos si hay otros ejemplos para los cuales la cota (1) sea casi óptima. Esta discusión sobre la criba grande junto con el ejemplo de los cuadrados, llevó a Helfgott y Venkatesh [**HV09**] e independientemente a Croot y Elsholtz [**CL07**] a conjeturar que cualquier conjunto

S mal distribuido de tamaño cercano a $N^{\frac{1}{2}}$ debería ser "esencialmente" la imagen de un polinomio cuadrático. Más precisamente, plantearon la siguiente conjetura.

Conjetura (Problema 7.4 en [**CL07**], Predicción en [**HV09**]). *Sea $S \subseteq \{0, \dots, N\}$ de tamaño $|S| \geq N^{\varepsilon}$ ocupando menos de αp clases residuales para algún $0 < \alpha < 1$ y todo primo p. Entonces todos salvo $O(N^{o(1)})$ elementos de S están contenidos en el conjunto de valores de un polinomio $f \in \mathbb{Z}[X]$ con coeficientes y grado acotados en términos de α y ε.*

Observamos que la conjetura se conoce como el problema inverso para la criba grande (ver Conjetura 1.4 en [**Gre08**]). El nombre se debe a que la conjetura clasifica todos los conjuntos de números enteros S que se obtienen después de cribar $\frac{p-1}{2}$ clases residuales módulo p sobre los primos $p \leq N^{\frac{1}{2}}$, y que tienen un tamaño cercano a $N^{\frac{1}{2}}$. En la Sección 4.2 de [**HV09**] Helfgott y Venkatesh observaron que la conjetura implica que hay $O(N^{\varepsilon})$ puntos en una curva irracional, lo cual se considera un problema muy difícil. En el mismo artículo [**HV09**], los autores demostraron la siguiente variante en "dimensiones superiores" de la conjetura.

Teorema 0.1 (Teorema 1.1 en [**HV09**]). *Sean $\varepsilon, \alpha > 0$. Existen constantes $c_1 = c_1(\alpha, \varepsilon)$ y $c_2 = c_2(\alpha, \varepsilon)$ tal que lo siguiente sucede. Sea $S \subseteq \{0, \dots, N\}^2$ un subconjunto tal que el numero de clases residuales $\{(x, y) \pmod p : (x, y) \in S\}$ es a lo sumo αp para todo primo p. Entonces, al menos una de las siguientes afirmaciones vale:*

- *$|S| \leq c_1 N^{\varepsilon}$;*
- *existe un polinomio no nulo de grado c_2 en $\mathbb{Z}[X, Y]$, que se anula en al menos $(1 - \varepsilon)|S|$ puntos de S.*

El argumento de la demostración del Teorema 0.1 se basa en el criba más grande de Gallagher. Específicamente, adaptaron el método del determinante de Bombieri-Pila (ver [**BP89**]) para dar una versión bidimensional de la criba de Gallagher. Además, sus métodos dieron otra prueba de las estimaciones de Bombieri-Pila para curvas planas (ver Teorema 5 en [**BP89**]). Si bien la demostración del Teorema 0.1 está estrechamente vinculada a la demostración original de [**BP89**], es notable que el método de [**HV09**] utilice "datos locales", es decir, el tamaño de las clases residuales de los puntos en una curva, en lugar de datos analíticos como en [**BP89**], que es útil en otros contextos (ver, [**Sed17**], donde se obtiene un análogo del Teorema 5 en [**BP89**] para cuerpos funcionales de género 0).

Helfgott y Venkatesh conjeturaron que un resultado similar al Teorema 0.1 debería ser válido para subconjuntos de enteros que se encuentran en $\mathbb{Z}^d$ para $d \geq 3$. Sus métodos, sin embargo, parecen manejar sólo el caso en el que S ocupa muy pocas clases residuales, específicamente como máximo αp clases residuales para todos los primos p. Notar que estos conjuntos no son lo que esperaríamos de un conjunto genérico mal distribuido, donde el número de clases residuales puede ser a lo sumo $O(p^{d-1})$. Utilizando un sutil

argumento inductivo, junto con la criba más grande y el método polinomial, en [**Wal12**], Walsh resolvió esta conjetura demostrando el siguiente teorema.

TEOREMA 0.2 (Teorema 1.1 en [**Wal12**]). *Sean $0 \leq k < d$ enteros y sean $\varepsilon, \alpha, \eta > 0$ números reales positivos. Entonces, existe una constante C dependiendo sólo de los parámetros anteriores, tal que para cualquier conjunto $S \subseteq \{0, \dots, N\}^d$ ocupando a lo sumo αp^k clases residuales para todo primo p, al menos una de las siguientes afirmaciones vale:*

- *(S es pequeño) $|S| \lesssim_{d,k,\varepsilon,\alpha} N^{k-1+\varepsilon}$;*
- *(S es fuertemente algebraico) existe un polinomio no nulo de grado a lo sumo C en $\mathbb{Z}[X_1, \dots, X_d]$ con coeficientes acotados por N^C anulándose en al menos $(1-\eta)|S|$ puntos de S.*

Enfaticemos el punto importante de que el Teorema 0.2 significa que existen constantes c, C dependiendo de los parámetros $d, k, \varepsilon, \alpha, \eta$ tales que para cualquier conjunto S satisfaciendo la hipótesis del teorema, se tiene que $|S| \leq cN^{k-1+\varepsilon}$ o existe un polinomio distinto de cero $f \in \mathbb{Z}[X_1, \dots, X_d]$ de grado como mucho C y coeficientes acotados por N^C que se anula en más de $(1-\eta)|S|$ puntos de S.

En este tesis estamos interesados en investigar el problema inverso de criba en el contexto de cuerpos globales. Para ello, sea K un cuerpo global y denotemos por $\mathcal{O}_K$ su anillo de enteros. Una generalización natural a cuerpos globales de subconjuntos que se encuentran en $\{0, \dots N\}^d$ es considerar los subconjuntos $S \subseteq \{\mathbf{x} \in \mathcal{O}_K^d : H(\mathbf{x}) \leq N\}$ donde H es una función altura, en el sentido de la geometría diofántica. Si dicho subconjunto S es pequeño, o si se encuentra en el conjunto de ceros de $\mathcal{O}_K$-puntos de una variedad afín $Z \subseteq \mathbb{A}^d$ de dimensión $l < d$ definida sobre K, entonces por cotas clásicos tenemos que para todos los primos $\mathfrak{p}$ en K, $Z(\mathcal{O}_K/\mathfrak{p})$ tiene como mucho $\lesssim_Z |\mathcal{O}_K/\mathfrak{p}|^l$ puntos. Por lo tanto, uno puede preguntarse si un principio similar al del Problema Inverso de Criba se cumple en el contexto de los cuerpos globales. En esta tesis adaptamos la prueba de Walsh para demostrar que este es efectivamente el caso. Más precisamente, se demuestra el siguiente resultado.

TEOREMA 0.3. *Sean $0 \leq k < d$ enteros y sean $\varepsilon, \alpha, \eta > 0$ números reales positivos. Sea K un cuerpo global de grado d_K. Para $x \in K$ sea $H(x)$ la altura absoluta multiplicativa de x. Entonces, existe una constante $C = C(d, k, \varepsilon, \alpha, \eta, K)$ tal que para cualquier conjunto $S \subseteq \{x \in \mathcal{O}_K : H(x) \leq N\}^d$ ocupando menos de $\alpha|\mathcal{O}_K/\mathfrak{p}|^k$ clases residuales para todo primo $\mathfrak{p}$, al menos una de las siguientes afirmaciones vale:*

- *(S es pequeño) $|S| \lesssim_{d,k,\varepsilon,\alpha,K} N^{d_K(k-1)+\varepsilon}$;*
- *(S es fuertemente algebraico) existe un polinomio no nulo de grado a lo sumo C en $\mathcal{O}_K[X_1, \dots, X_d]$ con coeficientes de altura acotada por N^C anulándose en al menos $(1-\eta)|S|$ puntos de S.*

La razón por la cual el exponente d_K aparece en el primer caso del Teorema 0.3 es porque estamos contando $\mathcal{O}_K$ puntos con K una extensión de $\mathbb{Q}$ posiblemente no trivial y se espera tener una potencia d_K-ésima de las cantidades habituales. Por ejemplo, la línea $x = y$ tiene $\sim_{K,\varepsilon} N^{d_K+\varepsilon}$ $\mathcal{O}_K$-puntos de altura absoluta a lo sumo N.

En algunas situaciones, es posible tener información adicional sobre S, por ejemplo, que S ya se encuentra en una variedad afín Z definida sobre K, digamos geométricamente irreducible. En este caso, el enunciado del Teorema 0.3 es trivial, ya que la segunda condición se cumple. Sin embargo, puede suceder que S ocupe incluso menos clases residuales que Z. En este caso, podemos demostrar un resultado más preciso que el Teorema 0.3, como se puede ver en el siguiente teorema.

TEOREMA 0.4. *Sean $0 \le k < d$ enteros, $D, M > 0$ enteros positivos, y sean $\varepsilon, \alpha, \eta > 0$ números reales positivos. Sea K un cuerpo global de grado d_K. Para $x \in K$ sea $H(x)$ la altura absoluta multiplicativa de x. Entonces, existe una constante $C = C(d, k, \varepsilon, \alpha, \eta, K, D, M)$ tal que para cualquier conjunto $S \subseteq \{x \in \mathcal{O}_K : H(x) \le N\}^M$ ocupando menos de $\alpha|\mathcal{O}_K/\mathfrak{p}|^k$ clases residuales para todo primo $\mathfrak{p}$, y que esta contenida en una variedad afín $Z \subseteq \mathbb{A}^M$ definida sobre K, geométricamente irreducible de dimensión d y grado D, al menos una de las siguientes afirmaciones vale:*

- *(S es pequeño) $|S| \lesssim_{d,k,\varepsilon,\alpha,K,D,M} N^{d_K(k-1)+\varepsilon}$;*
- *(S es fuertemente algebraico) existe un polinomio de grado a lo sumo C en $\mathcal{O}_K[X_1, \dots, X_M]$ con coeficientes de altura acotada por N^C anulándose en al menos $(1-\eta)|S|$ puntos de S, que se no anula sobre Z.*

En aplicaciones diofánticas, normalmente uno está interesado en los puntos racionales de alguna variedad algebraica. Por tanto, uno puede preguntarse si el Teorema 0.4 admite una "versión proyectiva". Aquí también se demuestra dicha versión. Además, como en [**Wal12**], sólo requerimos que nuestros conjuntos ocupen pocas clases residuales para un subconjunto "denso" de primos pequeños. Todo esto se resume en el siguiente teorema.

TEOREMA 0.5. *Sean $0 \le k < d-1$ enteros, $D, M > 0$ enteros positivos, y sean $\varepsilon, \alpha, \kappa, \eta > 0$ números reales positivos. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2(d+1)}}$ y sea*

$$P \subseteq \mathcal{P}(Q) := \{\mathfrak{p} \text{ primo de } \mathcal{O}_K : |\mathcal{O}_K/\mathfrak{p}| \le Q\}$$

un subconjunto de primos que cumple

$$w(P) := \sum_{\mathfrak{p} \in P} \frac{\log(|\mathcal{O}_K/\mathfrak{p}|)}{|\mathcal{O}_K/\mathfrak{p}|} \ge \kappa w(\mathcal{P}(Q)).$$

Para $\mathbf{x} \in \mathbb{P}^M(K)$ sea $H(\mathbf{x})$ su altura absoluta multiplicativa. Entonces, existe una constante $C = C(d, k, \varepsilon, \alpha, \eta, K, D, M)$ tal que para cualquier conjunto $S \subseteq \{\mathbf{x} \in \mathbb{P}^M(K) : H(\mathbf{x}) \le N\}$ ocupando menos de $\alpha|\mathcal{O}_K/\mathfrak{p}|^k$ clases residuales para todo primo $\mathfrak{p}$ (i.e. la

imagen de S en $\mathbb{P}^M(\mathcal{O}_K/\mathfrak{p})$ posee a lo sumo $\alpha|\mathcal{O}_K/\mathfrak{p}|^k$ elementos), y que esta contenida en una variedad proyectiva $Z \subseteq \mathbb{P}^M$ definida sobre K, geométricamente irreducible de dimensión d y grado D, al menos una de las siguientes afirmaciones vale:

- *(S es pequeño) $|S| \lesssim_{d,k,\varepsilon,\alpha,K,D,M} N^{d_K k+\varepsilon}$;*
- *(S es fuertemente algebraico) existe un polinomio homogéneo de grado a lo sumo C en $\mathcal{O}_K[X_0,\dots,X_M]$ con coeficientes de altura acotada por N^C anulándose en al menos $(1-\eta)|S|$ puntos de S, que se no anula sobre Z.*

Sería interesante saber si el Teorema 0.5 sigue siendo válido en el caso extremo $k = d-1$. La discusión sobre este caso se hará el final de la Sección §2 del Capítulo 4.

Las pruebas que aquí se presentan siguen la estrategia general desarrollada por Walsh en [**Wal12**]. Sin embargo, dada la naturaleza de los enunciados de nuestros teoremas, surgen varias dificultades nuevas. Primero necesitamos adaptar dos tipos de estimaciones sobre $\mathbb{Z}$ a las estimaciones correspondientes sobre cuerpos globales: las relativas al comportamiento de las alturas y las relativas a la distribución de primos. Para ello, en el Capítulo 1 comenzamos definiendo la función altura que se utilizará a lo largo de esta tesis. Si bien la teoría de las alturas para cuerpos de números está muy bien documentada, podría decirse que no es así en el caso de los cuerpos funcionales. Específicamente, aquí se demuestran dos afirmaciones para alturas en cuerpos funcionales que no se logro encontrar en la literatura. Estas son la Proposición 1.1 del Capítulo 1, que establece que los puntos en $\mathbb{P}^n$ de altura $\lesssim 1$ se elevan a puntos en $\mathbb{A}^{n+1}$ de altura $\lesssim_K 1$, y la Proposición 1.3 del Capítulo 1, que da una cota superior para el número de puntos de altura acotada en el grupo de S-unidades de un cuerpo funcional. Ambos resultados son bien conocidos para cuerpos de números (ver, por ejemplo, la Sección 13.4 del Capítulo 13 de [**Ser89**] y la Sección 3 de [**Lan83**], respectivamente). Con respecto a la distribución de primos, en la Sección §1 del Capítulo 2, después de recordar el teorema del ideal primo de Landau para cuerpos de números y la hipótesis de Riemann sobre cuerpos funcionales, extendemos la criba más grande de Gallagher, tal como se presentó en [**Wal12**], a cuerpos globales.

El segundo tipo de dificultad es que trabajamos con conjuntos que se encuentran en variedades algebraicas y que las cotas de nuestros teoremas son uniformes en el grado y la dimensión de tales variedades algebraicas. Esto se soluciona en el Capítulo 3 esencialmente en dos pasos. Primero usamos un argumento estándar para reducir el Teorema 0.5 a un enunciado relativo a variedades afines. Luego, usamos el teorema de normalización de Noether para hacer un cambio de variables y reducir el Teorema 0.5 a un enunciado sobre conjuntos mal distribuidos en un espacio afín. Debido a la uniformidad de nuestros cotas, necesitamos tener un buen control en el cambio de variables. Por lo tanto, se debío demostrar en el Teorema 3.3 del Capítulo 3 un teorema de normalización de Noether efectivo, que puede ser de interés por derecho propio.

Finalmente, en el Capítulo 4 demostramos el Teorema 0.5. En las pruebas seguimos la dependencia de los parámetros, lo que trae la última dificultad técnica de esta tesis.

Los resultados centrales de esta tesis fueron publicados en el artículo [**MPS21**].

Capítulo 1

Alturas en cuerpos globales

En este primer capítulo se recordará la teoría de valores absolutos sobre cuerpos globales y se establecerán las normalizaciones de los mismos, que se utilizarán para definir la función de altura a utilizar en esta tesis y recordar sus propiedades básicas. A su vez, se probarán resultados sobre estimaciones del número de puntos en el grupo de S-unidades para cuerpos globales, los cuales son bien conocidos para el caso de cuerpos de números, pero no sucede así en el caso de cuerpos funcionales. La presentación en esta sección ha sido influenciada por las referencias estándar [**BG06, HS00, Lan83, Ser89**].

1. Valores absolutos y alturas relativas

A lo largo de esta tesis, K denota un cuerpo global, es decir, una extensión finita y separable de $\mathbb{Q}$ o $\mathbb{F}_q(T)$, en cuyo caso asumimos además que el cuerpo de constantes es $\mathbb{F}_q$. Denotaremos por d_K el grado de la extensión $K/\Bbbk$, donde $\Bbbk$ denota indistintamente los cuerpos base $\mathbb{Q}$ o $\mathbb{F}_q(T)$.

Sea K un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros. Entonces cada embedding $\sigma : K \hookrightarrow \mathbb{C}$ induce un lugar v, mediante la ecuación

$$\|x\|_v := |\sigma(x)|_\infty^{\frac{n_v}{d_K}},$$

donde $|\cdot|_\infty$ denota el valor absoluto de $\mathbb{R}$ o $\mathbb{C}$ y $n_v = 1$ o 2 respectivamente. Tales lugares se llamarán lugares en el infinito y se denotarán por $M_{K,\infty}$. Observar que $\sum_{v\in M_{K,\infty}} n_v = d_K$. Estos son todos los lugares Arquímedianos de K. Dado que los embeddings complejos vienen en pares que difieren en la conjugación compleja, tenemos que $|M_{K,\infty}| \leq d_K$.

Sea ahora $\mathfrak{p}$ un ideal primo distinto de cero del cuerpo de números K, y denotamos con $\mathrm{ord}_\mathfrak{p}$ la valuación $\mathfrak{p}$-ádica. Asociado a $\mathfrak{p}$, tenemos el lugar v en K dado por la ecuación

$$\|x\|_v := |x|_\mathfrak{p} := \mathcal{N}_K(\mathfrak{p})^{-\frac{\mathrm{ord}_\mathfrak{p}(x)}{d_K}},$$

donde $\mathcal{N}_K(\mathfrak{p})$ denota el cardinal del cociente finito $\mathcal{O}_K/\mathfrak{p}$. También denotaremos $\mathcal{O}_\mathfrak{p}$ a la localización en $\mathfrak{p}$ del anillo $\mathcal{O}_K$. Dichos lugares se llamarán lugares finitos y se denotarán por $M_{K,\mathrm{fin}}$. Estos son todos los lugares no arquimedianos de K. El conjunto de lugares de K es entonces la unión $M_{K,\infty} \cup M_{K,\mathrm{fin}}$, y lo denotamos por M_K. Para cualquier subconjunto finito $S \subseteq M_K$ que contenga los lugares infinitos $M_{K,\infty}$, definimos el anillo

de S-enteros de K como el conjunto

$$\mathcal{O}_{K,S} \coloneqq \{x \in K : \|x\|_v \leq 1 \text{ para todo } v \in M_K, v \notin S\}.$$

Observar que $\mathcal{O}_K = \mathcal{O}_{K,S}$ para $S = M_{K,\infty}$. La norma de un ideal distinto de cero $I \subseteq \mathcal{O}_{K,S}$, denotado por $\mathcal{N}_{K,S}(I)$, es simplemente el cardinal del cociente finito $\mathcal{O}_{K,S}/I$. Los ideales primos de $\mathcal{O}_{K,S}$ corresponden a los ideales primos $\mathfrak{p}\mathcal{O}_{K,S}$ donde $\mathfrak{p}$ es un primer ideal de $\mathcal{O}_K$ que no está en S.

Ahora, supongamos que K es un cuerpo funcional de una variable sobre $\mathbb{F}_q$, tal que $\mathbb{F}_q$ es algebraicamente cerrado en K (en otras palabras , el cuerpo de constante de K es $\mathbb{F}_q$). Un primo en K es, por definición, un anillo de valuación discreta $\mathcal{O}$ con ideal maximal $\mathfrak{p}$ tal que $\mathbb{F}_q \subsetneq \mathfrak{p}$ y el cuerpo de fracciones de $\mathcal{O}$ es igual a K. Por abuso de notación, cuando nos referimos a un primo en K, nos referiremos al ideal maximal $\mathfrak{p}$. También denotaremos $\mathcal{O}_\mathfrak{p}$ al anillo de valuación discreta correspondiente. Asociado a $\mathfrak{p}$, tenemos la valuación $\mathfrak{p}$-ádica, que denotaremos por $\mathrm{ord}_\mathfrak{p}$. El grado de $\mathfrak{p}$, denotado por $\deg(\mathfrak{p})$ será la dimensión de $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ como un $\mathbb{F}_q$-espacio vectorial, el cual es finito. Luego la norma de $\mathfrak{p}$ se define como $\mathcal{N}_K(\mathfrak{p}) \coloneqq q^{\deg(\mathfrak{p})}$. Cualquier primo $\mathfrak{p}$ de K induce un lugar v en K por la ecuación

$$\|x\|_v \coloneqq |x|_\mathfrak{p} \coloneqq \mathcal{N}_K(\mathfrak{p})^{-\frac{\mathrm{ord}_\mathfrak{p}(x)}{d_K}}.$$

Estos son todos los lugares de K. El conjunto de todos los lugares en K se denota por M_K. Como en el caso de los cuerpos de números, para cualquier subconjunto finito no vacío $S \subseteq M_K$, definimos el anillo de S-enteros de K como el conjunto

$$\mathcal{O}_{K,S} \coloneqq \{x \in K : \|x\|_v \leq 1 \text{ para todo } v \in M_K, v \notin S\}.$$

Dado $x \in \mathcal{O}_{K,S}$ definimos $\mathcal{N}_{K,S}(x) \coloneqq \prod_{\mathfrak{p} \notin S} \mathcal{N}_K(\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(x)}$. Por definición, $\mathrm{ord}_\mathfrak{p}(x) \geq 0$ para todo $\mathfrak{p} \notin S$, de modo que $\mathcal{N}_{K,S}(x)$ es un entero positivo. Un primo en $\mathcal{O}_{K,S}$ será cualquier primo $\mathfrak{p} \in K$ que no esté en S. Cuando $S = \{v\}$, generalmente denotaremos $\mathcal{O}_{K,S} = \mathcal{O}_K$. Si $w \in M_\Bbbk$ es el lugar debajo de v, denotaremos $M_{K,\infty} \coloneqq \{v' \in M_K : v'|w\}$. Observar que $|M_{K,\infty}| \leq d_K$.

Ahora, dado un cuerpo global K, definimos la altura proyectiva multiplicativa absoluta de K de un punto $\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$, como la función

$$H(\mathbf{x}) \coloneqq \prod_{v \in M_K} \max_i \{\|x_i\|_v\},$$

y la altura proyectiva multiplicativa relativa por

$$H_K(\mathbf{x}) \coloneqq H(\mathbf{x})^{d_K}.$$

Si $x \in K$, $H_K(x)$ siempre denotará la altura proyectiva $H_K(1 : x)$. Las siguientes desigualdades se siguen de la definición de la altura

$$H_K(x \cdot y) \leq H_K(x) \cdot H_K(y), \tag{2}$$

$$H_K(x + y) \leq 2^{d_K} H_K(x) H_K(y). \tag{3}$$

Además, de la fórmula del producto se deduce que para todo $x \in K^*$,

$$H_K(x) = H_K(x^{-1}). \tag{4}$$

Para nuestros propósitos, será necesario comprender cómo se comporta la altura afín de un punto bajo la acción de un polinomio. Es fácil ver (Proposición B.2.5. (a) en [**HS00**]) que si $P(T_1, \ldots, T_n) = \sum_{(i_1,\ldots,i_n)} c_{i_1,\ldots,i_n} T_1^{i_1} \cdots T_n^{i_n}$, $\mathbf{c} = (c_{i_1,\ldots,i_n})_{i_1,\ldots,i_n}$ y R es la cantidad de $(i_1, \ldots, i_n)$ con $c_{i_1,\ldots,i_n} \neq 0$, tenemos

$$H_K(P(\mathbf{x})) \leq R^{d_K} H_K(1 : \mathbf{c}) H_K(1 : \mathbf{x})^{\deg(P)}. \tag{5}$$

Dado un conjunto de lugares S y $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{O}_{K,S}^n$, se tienen las cotas

$$H_K(x_1 : \ldots : x_n) \leq H_K(1 : x_1 : \ldots : x_n) \leq \max_i \{H_K(x_i)\}^{|S|}. \tag{6}$$

Ademas, para cada $x \in \mathcal{O}_{K,S} \backslash \{0\}$, se tiene que

$$\mathcal{N}_K(x) \leq H_K(x). \tag{7}$$

En el resto de la tesis utilizaremos la siguiente notación,

$$[N]_{\mathcal{O}_K}^n := \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{O}_K^n : \max_i \{H_K(x_i)\} \leq N\}, \tag{8}$$

$$[N]_{\mathbb{A}^n(\mathcal{O}_K)} := \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{O}_K^n : H_K(1 : x_1 : \ldots : x_n) \leq N\}. \tag{9}$$

$$[N]_{\mathbb{P}^n(K)} := \{\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K) : H_K(\mathbf{x}) \leq N\}. \tag{10}$$

Observar que dado que $\max_i\{H_K(x_i)\} \leq H_K(1 : x_1 : \ldots : x_n)$, para todo $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ se tiene que

$$[N]_{\mathbb{A}^n(\mathcal{O}_k)} \subseteq [N]_{\mathcal{O}_K}^n. \tag{11}$$

2. Estimaciones efectivas para alturas sobre cuerpos globales

En el Capítulo 3 necesitaremos levantar un conjunto acotado del espacio proyectivo a un conjunto en el espacio afín. La siguiente proposición establece que esto se puede hacer de manera controlada.

PROPOSITION 1.1. *Sea K un cuerpo global, sea S un conjunto finito de lugares, con la condición adicional de que $M_{K,\infty} \subseteq S$ si K es un cuerpo de números, y sea $d \geq 1$ un número entero. Entonces existe $c = c(K, S, d)$ tal que por cada $\mathbf{x} \in \mathbb{P}^d(K)$ existe $(y_0, \ldots, y_d) \in \mathcal{O}_{K,S}^{d+1}$ un levantado de $\mathbf{x}$ tal que*

$$H_K(1 : y_0 : \ldots : y_d) \leq c H_K(\mathbf{x}).$$

En cuerpos de números y para $S = M_{K,\infty}$, la Proposición 1.1 se prueba en el Capítulo 13, Sección 13.4 de [**Ser89**]. Allí, Serre también observó que la constante c puede hacerse efectiva. Para probar la Proposición 1.1, se adaptó la prueba de Serre a cuerpos globales y anillos generales de S-enteros. Dado que todos los resultados de está tesis son efectivos, se aprovecha la oportunidad para cumplir con la observación de Serre realizando el trabajo adicional necesario para hacer explícita la dependencia de c en K y S.

Demostración de la Proposición 1.1. El resultado es trivial si $K = \Bbbk = \mathbb{Q}$ y $S = \{\infty\}$ o $K = \Bbbk = \mathbb{F}_q(T)$ y S es el lugar correspondiente al punto del infinito en $\mathbb{P}^1(K)$: para cualquier conjunto de coordenadas de $\mathbf{x}$, limpiar denominadores y sacar factor común. De esta forma obtenemos coordenadas $(x_0 : \ldots : x_d)$ tales que $x_i \in \mathcal{O}_\Bbbk$, $\operatorname{mcd}(x_0, \ldots, x_d) = 1$ y

$$H_K(1 : x_0 : \ldots : x_d) = H_K(\mathbf{x}).$$

Para el caso general, será conveniente probar primero la cota de la Proposición 1.1 para la altura absoluta. Sea $\mathbf{x} \in \mathbb{P}^d(K)$ y elijamos las coordenadas $(x_0, \ldots, x_d)$ con $x_i \in \mathcal{O}_{K,S}$. Si $\mathfrak{a}_{x_0,\ldots,x_d} := \sum_{i=0}^d x_i \mathcal{O}_{K,S}$ entonces

$$H(\mathbf{x}) = \frac{1}{\mathcal{N}_K(\mathfrak{a}_{x_0,\ldots,x_d})^{\frac{1}{d_K}}} \prod_{v \in S} \max_i \|x_i\|_v.$$

Observar que el ideal $\mathfrak{a}_{x_0,\ldots,x_d}$ depende de las coordenadas, pero su clase ideal depende solo de $\mathbf{x}$. Por lo tanto, si tomamos ideales íntegros $\mathfrak{a}_1, \ldots, \mathfrak{a}_l$ que representan todas las clases ideales de $\mathcal{O}_{K,S}$, satisfaciendo la cota de Minkowski $\mathcal{N}_K(\mathfrak{a}_j) \lesssim_K 1$ para todo j (cuando K es un cuerpo funcional, esta cota puede deducirse de la Sección §8.9. del Capítulo V de [**Lor96**]), se tiene que $\mathfrak{a}_{x_0,\ldots,x_d}\mathfrak{a}_j^{-1} = \alpha\mathcal{O}_{K,S}$ para algún j y algún $\alpha \in K^\times$. Por lo tanto, $\alpha^{-1}\mathcal{O}_{K,S} \cdot \mathfrak{a}_{x_0,\ldots,x_d} = \mathfrak{a}_j$. Concluimos que $(x_0', \ldots, x_d') := (\alpha^{-1}x_0, \ldots, \alpha^{-1}x_d)$ son coordenadas de $\mathbf{x}$ que satisfacen $\alpha^{-1}x_i \in \mathcal{O}_{K,S}$ para todo i y $\mathfrak{a}_{x_0',\ldots,x_d'} = \mathfrak{a}_j$. En particular,

$$H(\mathbf{x}) = \frac{1}{\mathcal{N}_K(\mathfrak{a}_j)^{\frac{1}{d_K}}} \prod_{v \in S} \max_i \|x_i'\|_v.$$

Ahora, usamos el siguiente lema, cuya demostración se dará luego de que terminemos la demostración de la Proposición 1.1

Lema 1.2. *Sea K un cuerpo global y S un conjunto de lugares que contiene los lugares infinitos cuando K es un cuerpo de números. Existe una constante $c'_{K,S} > 1$, que depende únicamente de K, S, tal que para cada $\mathbf{x} = (x_v)_{v \in S} \in (\mathbb{R}_{>0})^{|S|}$ existe $\varepsilon \in \mathcal{O}_{K,S}^\times$ y $t > 0$ que verifican*

$$\left(c'_{K,S}\right)^{-1} \frac{x_v}{t} \le \|\varepsilon\|_v \le c'_{K,S} \frac{x_v}{t} \text{ para todo } v \in S. \tag{12}$$

Sea $c'_{K,S}$ la constante del Lema 1.2. Fijemos cualquier $v_0 \in S$. Tomando $(x_v)_{v \in S} := (\max_i \|x_i'\|_v)_{v \in S}$, el Lema 1.2 implica que existen $t > 0$ y $\varepsilon \in \mathcal{O}_{K,S}^\times$ tales que

$$\begin{aligned} \left(c'_{K,S}\right)^{-2} \max_i \|\varepsilon^{-1}x_i\|_{v_0} \le \left(c'_{K,S}\right)^{-1} t \le \max_i \|\varepsilon^{-1}x_i'\|_v \\ \le c'_{K,S} t \le \left(c'_{K,S}\right)^2 \max_i \|\varepsilon^{-1}x_i'\|_{v_0}, \end{aligned} \tag{13}$$

para todo $v \in S$. En particular, si $h := \max_i \|\varepsilon^{-1}x_i'\|_{v_0}$, de (13) y el hecho de que $\prod_{v\in S}\|\varepsilon^{-1}\|_v = 1$ se deduce que

$$H(\mathbf{x}) = \frac{1}{\mathcal{N}_K(\mathfrak{a}_j)^{\frac{1}{d_K}}}\prod_{v\in S}\max_i\|\varepsilon^{-1}x_i'\|_v \gtrsim_{K,S} \prod_{v\in S}\max_i\{\|\varepsilon^{-1}x_i'\|_{v_0}\} \gtrsim_{K,S} h^{|S|}. \tag{14}$$

Ahora, notar que (13) y (14) implican que para todo $v \in S$

$$\|\varepsilon^{-1}x_j'\|_v \le \max_w\max_i\|\varepsilon^{-1}x_i'\|_w \lesssim_{K,S} h \lesssim_{K,S} H(\mathbf{x})^{\frac{1}{|S|}}.$$

Luego,

$$H(1 : \varepsilon^{-1}x_0' : \ldots : \varepsilon^{-1}x_d') \lesssim_{K,S} H(\mathbf{x}).$$

Tomando $y_j := \varepsilon^{-1}x_j'$, se concluye que las coordenadas $(y_0, \ldots, y_d)$ satisfacen la conclusión de la Proposición 1.1. □

Demostración del Lema 1.2. Notar que la ecuación (1.2) es equivalente a probar que existen $t > 0$ y una unidad ε tales que

$$\log(t) + \log(\|\varepsilon\|_v) = \log(h_v) + O_K(1) \text{ para todo } v \in S. \tag{15}$$

Notamos $(1)_{v\in S}$ al vector en $\mathbb{R}^{|S|}$ con coordenadas todas iguales a 1 y sea W el $\mathbb{Z}$-módulo dado por

$$W := \left\langle \{(\log(\|\varepsilon\|_v))_{v\in S} : \varepsilon \in \mathcal{O}_{K,S}^\times\}, (1)_{v\in S}\right\rangle_{\mathbb{Z}} \subseteq \mathbb{R}^{|S|}.$$

Si notamos por $\|\cdot\|$ a la norma l^∞ en $\mathbb{R}^{|S|}$, vemos que para demostrar (15) es suficiente encontrar una constante positiva C_W tal que para cualquier $\mathbf{x} \in \mathbb{R}^{|S|}$ exista $\mathbf{w} \in W$ que satisfaga

$$\|\mathbf{x} - \mathbf{w}\| \le C_W. \tag{16}$$

Más aún, podemos tomar $c'_{K,S} = \exp(C_W)$. En general, es fácil ver que si $W \subseteq \mathbb{R}^{|S|}$ es un subgrupo aditivo que satisface que $\mathbb{R}^{|S|}/W$ es compacto, y Ω es un conjunto acotado que contiene un representante de cada clase de $\mathbb{R}^{|S|}/W$, entonces (16) se verifica con $C_W = \sup_{\mathbf{y}\in\Omega}\|\mathbf{y}\|$. En nuestro caso, el subgrupo

$$W_1 := \left\langle \{(\log(\|\varepsilon\|_v)_{v\in S}) : \varepsilon \in \mathcal{O}_{K,S}^\times\}\right\rangle \subseteq \mathbb{R}^{|S|}$$

define un lattice de rango $|S|-1$ en el hiperplano $\{(x_v)_{v\in S} \in \mathbb{R}^{|S|} : \sum_{v\in S} x_v = 0\}$. Más aún, (ver Proposición 5.4.7 (b) y Teorema 5.4.9 (b) en [**TV91**]) se tiene que el volumen de W_1 satisface la cota:

$$\det(W_1) \le \begin{cases} |S|^{\frac{1}{2}} R_K h_K \displaystyle\prod_{v\in M_{K,\mathrm{fin}}\cap S} \log(\mathcal{N}(\mathfrak{p}_v)) & \text{si } K \text{ es un cuerpo de números,} \\ |S|^{\frac{1}{2}}\left(1 + q + \dfrac{|X(\mathbb{F}_q)| - q - 1}{g_K}\right)^{g_K} & \text{si } K \text{ es el cuerpo de funciones de una curva } X \text{ sobre } \mathbb{F}_q. \end{cases} \tag{17}$$

En (17), como es usual, R_K y h_K denotan respectivamente el regulador y el número de clases de K, y $\mathfrak{p}_v$ es el primo correspondiente al lugar finito v. Mientras tanto, cuando K es un cuerpo funcional, g_K denota el género de la curva X.

Usando (17), se puede demostrar que existe un sistema fundamental de unidades $\{\varepsilon_1, \dots, \varepsilon_{|S|-1}\}$ tal que

$$\prod_{i=1}^{|S|-1} \log(H(\varepsilon_i)) \lesssim_{|S|,d_K} \det(W_1), \tag{18}$$

donde la constante implícita es efectiva. Se puede encontrar una prueba de (18) en la Proposición 4.3.9(i) en [**EG15**] para cuerpos de números, pero la misma prueba se aplica a los cuerpos funcionales. Por otro lado, dados elementos distintos de cero $z_1, \dots, z_m \in \mathcal{O}_{K,S}$ que son multiplicativamente independientes, existen cotas inferiores efectivas bien conocidas de la forma $\prod_{i=1}^{m} \log(H(z_i)) \gtrsim_{d_K,|S|} 1$. De hecho, para los cuerpos funcionales esto es obvio; para cuerpos de números, podemos usar el teorema de Dobrowolski (ver, por ejemplo, el Teorema 4.4.1. en [**BG06**]) o estimaciones más fuertes, como la dada en el Corolario 3.1 en [**LM04**]. Así, de (18) deducimos

$$\max_{1\le i\le |S|-1} \log(H(\varepsilon_i)) \lesssim_{|S|,d_K} \det(W_1). \tag{19}$$

De (19) concluimos que podemos encontrar un dominio fundamental $\Omega_{W_1} \subseteq \mathbb{R}^{|S|}$ tal que $\max_{\mathbf{y}\in\Omega_{W_1}} \|\mathbf{y}\| \lesssim_{|S|,d_K} \det(W_1)$. Además, deducimos que existe un dominio fundamental $\Omega_W \subseteq \mathbb{R}^{|S|}$ con $\max_{\mathbf{y}\in\Omega_W} \|\mathbf{y}\| \lesssim_{|S|,d_K} \det(W_1)$ y, por lo tanto, la constante C_W es efectiva y puede tomarse de la forma $O_{|S|,d_K}(\det(W_1))$. Luego podemos tomar $C'_{K,S} = \exp(C_W)$. □

En el Capítulo 4 necesitaremos estimaciones para el número de puntos en $\mathcal{O}_K$ de altura dada. Esto es abordado por la siguiente proposición.

Proposition 1.3 (S-puntos enteros de altura acotada). *Sea K un cuerpo global, y sea $S \subseteq M_K$ un subconjunto finito no vacío de lugares de K (que requerimos que contenga los lugares infinitos cuando K es un cuerpo de números, y el lugar v fijado para definir $\mathcal{O}_K$ cuando K es un cuerpo funcional). Entonces*

$$|\{x \in \mathcal{O}_{K,S} : H_K(x) \le N\}| \le c''(K) N (\log(N))^{|S|}.$$

Cuando K es un cuerpo de números, se tienen estimaciones más finas que la Proposición 1.3; por ejemplo, vea el Teorema 5.2 en [**Lan83**] para el caso $S = M_{K,\infty}$ y el Teorema 1,1 en [**Bar15**] para S arbitrarios. Más aún, el Teorema 1.1 en [**Bar15**] da estimaciones efectivas. Dado que no se pudo encontrar una referencia para la Proposición 1.3 para cuerpos funcionales, se proporciona una prueba en esta tesis. El argumento de la demostración, sigue esencialmente el caso del cuerpos de números como en el Teorema 5.2 en [**Lan83**], reemplazando el argumento de la geometría de números por estimaciones de la dimensión de algunos espacios de divisores.

Demostración de la Proposición 1.3 para cuerpos funcionales. Supongamos que K es un cuerpo funcional con cuerpo de constantes $\mathbb{F}_q$. Se tiene la función

$$\varphi : [N]_{\mathcal{O}_{K,S}} \to \{D \in \mathrm{Div}(K) : D \geq 0, \deg(D) \leq \log_q(N)\} \times \{D \in \mathrm{Div}(K) : D = \sum_{v \in S} a_v \cdot v, |a_v| \leq \log_q(N)\},$$

$$\varphi(x) := \left(\sum_{v \notin S} \mathrm{ord}_v(x) \cdot v, \sum_{v \in S} \mathrm{ord}_v(x) \cdot v \right).$$

Observar que, salvo constantes, la asignación $x \mapsto \mathrm{div}(x)$ es inyectiva. Luego, φ posee fibras de q elementos. Es claro que

$$\left| \left\{ D \in \mathrm{Div}(K) : D = \sum_{v \in S} a_v \cdot v : |a_v| \leq \log_q(N) \right\} \right| \leq (\log(N))^{|S|}. \tag{20}$$

Por el Lema 5.6 en [**Ros02**], el número de clases de divisores de grado cero, $h := h_K$, es finito. Por el Lema 5.8 en [**Ros02**], para cada entero n, hay h clases de divisores de grado n. Supongamos que $n \geq 0$ y que $\{\overline{A}_1, \ldots, \overline{A}_h\}$ son las clases de divisores de grado n. Si b_n es el número de divisores efectivos de grado n, entonces se cumple que $b_n = \sum_{i=1}^{h} \frac{q^{l(\overline{A}_i)}-1}{q-1}$, donde $l(\overline{A}_i)$ es la dimensión del espacio de Riemann-Roch asociado a $\overline{A}_i$. Por el Ejercicio 18 en [**Ros02**], $l(\overline{A}_i) \leq \deg(\overline{A}_i) + 1 = n + 1$, luego

$$b_n = \sum_{i=1}^{h} \frac{q^{l(\overline{A}_i)} - 1}{q-1} \leq h \frac{q^{n+1} - 1}{q-1} \leq 2hq^n.$$

Entonces:

$$\left| \{ D \in \mathrm{Div}(K) : D \geq 0, \deg(D) \leq \log_q(N) \} \right| = \sum_{i \leq \log_q(N)} b_i \leq 2h \sum_{i \leq \log_q(N)} q^i \leq 2hN. \tag{21}$$

Por (20) y (21) se concluye que

$$|[N]_{\mathcal{O}_{K,S}}| \leq 2qhN(\log(N))^{|S|}.$$

Observar que por Proposición 5.11 in [**Ros02**], $h \leq (\sqrt{q}+1)^{2g}$, donde g es el género de K. Luego,

$$|[N]_{\mathcal{O}_{K,S}}| \lesssim_{q,g} N(\log(N))^{|S|}.$$

□

Capítulo 2

La criba más grande sobre cuerpos globales

En este capítulo, extendemos el griba más grande de Gallagher a cuerpos globales, así como también una versión un poco más general, que será necesaria para los resultados de esta tesis. Con este fin, primero recordamos algunas desigualdades básicas relacionadas con la distribución de números primos en cuerpos globales.

1. Distribucion de números primos sobre cuerpos globales

Sea K un cuerpo global. Para cada primo $\mathfrak{p}$ de $\mathcal{O}_K$ se tiene un mapa de reducción $\pi_\mathfrak{p} : \mathbb{P}^n(K) \to \mathbb{P}^n(\mathcal{O}_K/\mathfrak{p})$. Si $\mathbf{x}, \mathbf{y} \in \mathbb{P}^n(K)$ por $\mathbf{x} \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ nos referimos a que $\pi_\mathfrak{p}(\mathbf{x}) = \pi_\mathfrak{p}(\mathbf{y})$. Observar que si $f \in \mathcal{O}_K[X_0, \dots, X_n]$ es un polinomio homogéneo tal que $f(\mathbf{x}) = 0$, entonces $\mathbf{x} \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ implica que $f(\mathbf{y}) \equiv f(\mathbf{x}) \equiv 0 (\mathrm{mod}\ \mathfrak{p})$. Similarmente, tenemos un mapa de reducción $\pi_\mathfrak{p} : \mathcal{O}_K^n \to (\mathcal{O}_K/\mathfrak{p})^n$, y para $\mathbf{x}, \mathbf{y} \in \mathcal{O}_K^n$ denotamos $\mathbf{x} \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ si $\pi_\mathfrak{p}(\mathbf{x}) = \pi_\mathfrak{p}(\mathbf{y})$.

Si $S \subseteq [N]_{\mathbb{A}^n(\mathcal{O}_K)}, [N]^n_{\mathcal{O}_K}$, o $[N]_{\mathbb{P}^n(K)}$ y $\mathfrak{p}$ es un primo de $\mathcal{O}_K$ usamos la notación $[S]_\mathfrak{p} := \pi_\mathfrak{p}(S)$ donde $\pi_\mathfrak{p}$ es el correspondiente mapa de reducción. Para cualquier $Q > 0$, denotamos:

$$\mathcal{P} := \{\mathfrak{p} \text{ primo de } \mathcal{O}_K\},$$
$$\mathcal{P}(Q) := \{\mathfrak{p} \in \mathcal{P} : \mathcal{N}_K(\mathfrak{p}) \leq Q\}.$$

Si $P \subseteq \mathcal{P}(Q)$, denotamos

$$w(P) := \sum_{\mathfrak{p} \in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})},$$

esto da una noción de la densidad de P dentro de $\mathcal{P}(Q)$. Efectivamente, si K es un cuerpo global, existen constantes $c_{1,K}, c_{2,K}, c_{3,K}$ y $c_{4,K}$ tales que para todo $Q > 0$ se satisface que

$$c_{1,K} \log(Q) \leq w(\mathcal{P}(Q)) \leq c_{2,K} \log(Q), \tag{22}$$

y

$$c_{3,K} Q \leq \sum_{\mathfrak{p} \in \mathcal{P}(Q)} \log(\mathcal{N}_K(\mathfrak{p})) \leq c_{4,K} Q. \tag{23}$$

De hecho, si K es un cuerpo de números, (22) y (23) se siguen del teorema de los ideales primos de Landau (ver el Corolario 1 de la página 358 en [**Nar04**]). Mientras tanto, si K es un cuerpo funcional sobre $\mathbb{F}_q$ de género g, esto se deduce de la hipótesis de

Riemann sobre cuerpos funcionales (ver Teorema 5.12 en [**Ros02**]). En este caso, las constantes también dependerán del (grado del) primo v que elijamos para definir $\mathcal{O}_K$.

2. La criba más grande sobre cuerpos globales

En esta sección generalizaremos la criba de Gallagher (Teorema 1 en [**Gal71**]) al caso de cuerpos globales.

LEMA 2.1 (Criba de Gallagher). *Sea $X \subseteq [N]_{\mathcal{O}_K}$ y P una familia finita de primos de $\mathcal{O}_K$. Supongamos que X ocupa a lo sumo $g(\mathfrak{p})$ clases residuales para cada $\mathfrak{p} \in P$. Entonces,*

$$|X| \leq \frac{\sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) - \log(2^{d_K} N^2)}{\sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{g(\mathfrak{p})} - \log(2^{d_K} N^2)} \tag{24}$$

siempre que el denominador sea positivo.

DEMOSTRACIÓN. Para cada $a \pmod{\mathfrak{p}}$, definimos $X(a,\mathfrak{p}) := \{x \in X : x \equiv a \pmod{\mathfrak{p}}\}$. Dado que X ocupa a lo sumo $g(\mathfrak{p})$ clases residuales para cada $\mathfrak{p} \in P$, por la desigualdad de Cauchy-Schwarz tenemos que

$$|X|^2 = \left(\sum_{a \pmod{\mathfrak{p}}} |X(a,\mathfrak{p})| \right)^2 \leq g(\mathfrak{p}) \sum_{a \pmod{\mathfrak{p}}} |X(a,\mathfrak{p})|^2,$$

o lo que es lo mismo

$$\frac{|X|^2}{g(\mathfrak{p})} \leq \sum_{a \pmod{\mathfrak{p}}} |X(a,\mathfrak{p})|^2. \tag{25}$$

Observemos que $|X(a,\mathfrak{p})|^2 = \sum_{x,y\in X} 1_{x\equiv y\equiv a \pmod{\mathfrak{p}}}$. De esta manera,

$$\sum_{a \pmod{\mathfrak{p}}} |X(a,\mathfrak{p})|^2 = |X| + \sum_{\substack{x,y\in X \\ x\neq y}} 1_{x\equiv y \pmod{\mathfrak{p}}}.$$

Luego, si multiplicamos (25) por $\log(\mathcal{N}_K(\mathfrak{p}))$ y sumando sobre todo $\mathfrak{p} \in P$ obtenemos que

$$\begin{aligned}|X|^2 \sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{g(\mathfrak{p})} &\leq |X| \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) + \sum_{\mathfrak{p}\in P} \sum_{\substack{x,y\in X\\ x\neq y}} 1_{x\equiv y(\mathrm{mod}\ \mathfrak{p})} \log(\mathcal{N}_K(\mathfrak{p})) \\ &= |X| \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) + \sum_{\substack{x,y\in X\\ x\neq y}} \log\left(\prod_{\substack{\mathfrak{p}\in P\\ x\equiv y(\mathrm{mod}\ \mathfrak{p})}} \mathcal{N}_K(\mathfrak{p}) \right) \qquad (26) \\ &\leq |X| \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) + \sum_{\substack{x,y\in X\\ x\neq y}} \log(\mathcal{N}_K(x-y)).\end{aligned}$$

Usando (7) y (3) obtenemos que $\mathcal{N}_K(x-y) \leq 2^{d_K} H_K(x) H_K(y) \leq 2^{d_K} N^2$. Luego,

$$|X|^2 \sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{g(\mathfrak{p})} \leq |X| \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) + (|X|^2 - |X|) \log(2^{d_K} N^2). \qquad (27)$$

Reordenando, llegamos a la desigualdad enunciada. □

Observar que el resultado anterior sigue valiendo para conjuntos $X \subseteq [N]^n_{\mathcal{O}_K}$. En efecto, si $\pi_1 : K^n \to K$ denota la proyección en la primera coordenada, entonces $\mathbf{x} \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ implica que $\pi_1(\mathbf{x}) \equiv \pi_1(\mathbf{y}) (\mathrm{mod}\ \mathfrak{p})$. Luego, lo único que hay que notar es que en la última desigualdad de (26), se tiene que

$$\prod_{\substack{\mathfrak{p}\in P\\ \mathbf{x}\equiv\mathbf{y}(\mathrm{mod}\ \mathfrak{p})}} \mathcal{N}_K(\mathfrak{p}) \leq \prod_{\substack{\mathfrak{p}\in P\\ \pi_1(\mathbf{x})\equiv\pi_1(\mathbf{y})(\mathrm{mod}\ \mathfrak{p})}} \mathcal{N}_K(\mathfrak{p}) \leq \log(\mathcal{N}_K(\pi_1(x) - \pi_1(y))).$$

A continuación, probaremos una versión un poco más general de la criba de Gallagher, en la cual tedremos control sobre la distribución en clases residuales, no de un conjunto X, sino de una proporción positiva del mismo. Esta variante será necesaria más adelante.

LEMA 2.2. *Sea $X \subseteq [N]_{\mathcal{O}_K}$, $Q = N^\gamma$, $\gamma > 0$. Sean κ, μ números reales positivos. Supongamos que se tiene un conjunto de primos $P \subseteq \mathcal{P}(Q)$ con $w(P) \geq \kappa w(\mathcal{P}(Q))$ tal que para cada primo $\mathfrak{p} \in P$ existen al menos $\mu|X|$ elementos de X ocupando como mucho $\alpha\mathcal{N}(\mathfrak{p})$ clases residuales para algún $\alpha > 0$ independiente de $\mathfrak{p}$. Entonces, existe una constante $C_1 = C_1(\kappa, \mu, \gamma, K)$ tal que si $\alpha \leq C_1$, debe ser $|X| < Q$.*

DEMOSTRACIÓN. Por hipótesis, para cada primo $p \in P$, tenemos un conjunto $X_p \subseteq X$ de cardinal al menos $\mu|X|$ que ocupa a lo sumo $\alpha\mathcal{N}_K(\mathfrak{p})$ clases residuales. Aplicando la desigualdad de Cauchy-Schwarz como se hizo para obtener 25, conseguimos que

$$\frac{(\mu|X|)^2}{\alpha\mathcal{N}_K(\mathfrak{p})} \leq \sum_{a(\mathrm{mod}\ \mathfrak{p})} |X_p(a,\mathfrak{p})|^2 \leq \sum_{a(\mathrm{mod}\ \mathfrak{p})} |X(a,\mathfrak{p})|^2.$$

Al igual que antes, si multiplicamos por $\log(\mathcal{N}_K(\mathfrak{p}))$ y sumando sobre todo $\mathfrak{p} \in P$, utilizando las propiedades de la altura relativa $H_K(x)$, llegamos a que

$$\frac{(\mu|X|)^2}{\alpha} \sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \leq |X| \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) + (|X|^2 - |X|)\log(2^{d_K} N^2). \tag{28}$$

Usando (22) y recordando que por hipótesis, $\sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} = w(P) \geq \kappa w(\mathcal{P}(Q))$, el lado izquierdo de (28) es al menos

$$\frac{(\mu|X|)^2}{\alpha} \kappa c_{1,K} \log(Q),$$

mientras que si usamos (23) y tomamos $N \geq 2^{d_K}$, el lado derecho de (28) es como mucho

$$|X| c_{4,K} Q + |X|^2 3 \log(N).$$

Luego, llegamos a que

$$\frac{(\mu|X|)^2}{\alpha} \kappa c_{1,K} \log(Q) \leq |X| c_{4,K} Q + |X|^2 3 \log(N).$$

Recordando que $Q = N^\gamma$, esto último es equivalente a

$$\left(\frac{\mu^2 \kappa \gamma}{\alpha} c_{1,K} - 3\right) \log(N) \leq c_{4,K} \frac{Q}{|X|}$$

Si α es suficientemente chico, esto solo puede pasar si $|X| < Q$. En particular, basta con tomar

$$\alpha \leq C_1(\kappa, \mu, \gamma, K) := \frac{\kappa \mu^2 \gamma}{c_{5,K}},\ c_{5,K} := \frac{2(c_{4,K} + 3)}{c_{1,K}}, \tag{29}$$

□

LEMA 2.3. *Sea $Q = N^\gamma$ para algún $\gamma > 0$ y sea $P \subseteq \mathcal{P}(Q)$ un conjunto de primos con $w(P) \geq \kappa w(\mathcal{P}(Q))$ para algún $\kappa > 0$. Sea $S \subseteq [N]^d_{\mathcal{O}_K}$ un conjunto que ocupa menos de α clases residuales módulo $\mathfrak{p}$ para cada primo $\mathfrak{p} \in P$ y alguna constante α, independiente de $\mathfrak{p}$. Entonces, para N suficientemente grande, existe una constante $C_2 = C_2(\alpha, \kappa, \gamma, K)$ tal que $|S| \leq C_2$.*

DEMOSTRACIÓN. Como se mencionó más arriba, el Lema 2.1 es válido para subconjuntos de $[N]^d_{\mathcal{O}_K}$. Por lo tanto, si lo aplicamos al conjunto S, el cual ocupa menos de $g(\mathfrak{p}) = \alpha$ clases residuales módulo $\mathfrak{p}$ para cada primo $\mathfrak{p} \in P$, la desigualdad (24) nos dice que

$$|S|^2 \sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\alpha} \leq |S| \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) + (|S|^2 - |S|)\log(2^{d_K} N^2).$$

Para $N \geq 2^{d_K}$, llegamos a que

$$3\log(N) \geq \left(\frac{1}{\alpha} - \frac{1}{|S|}\right) \sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})). \tag{30}$$

Veamos que P no puede tener muchos primos de norma pequeña. Sea a un parámetro a determinar, escribamos la densidad de P como

$$w(P) = \sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} = \sum_{\substack{\mathcal{N}_K(\mathfrak{p})<Q^a \\ \mathfrak{p}\in P}} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} + \sum_{\substack{\mathcal{N}_K(\mathfrak{p})\geq Q^a \\ \mathfrak{p}\in P}} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})}.$$

Luego, alguno de estos dos términos, deber ser mayor o igual a la mitad de la densidad de P. Supongamos que el primero lo es, es decir,

$$\sum_{\substack{\mathcal{N}_K(\mathfrak{p})<Q^a \\ \mathfrak{p}\in P}} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \geq \frac{1}{2} w(P). \tag{31}$$

Por hipótesis, $w(P) \geq \kappa w(\mathcal{P}(Q))$, por lo que aplicando (22), el lado derecho de (31) es a lo sumo $\frac{\kappa}{2} c_{1,K} \log(Q)$, mientras que el lado izquierdo de (31) es como mucho $c_{2,K} \log(Q^a) \leq w(\mathcal{P}(Q^a))$. Por lo tanto,

$$c_{2,K} \log(Q^a) \leq \frac{\kappa}{2} c_{1,K} \log(Q),$$

o lo que es lo mismo,

$$a \geq \frac{\kappa c_{1,K}}{2c_{2,K}}.$$

De esta manera, si tomamos $a = \frac{1}{2}\frac{\kappa c_{1,K}}{2c_{2,K}}$, será

$$\sum_{\substack{\mathcal{N}_K(\mathfrak{p})\geq Q^a \\ \mathfrak{p}\in P}} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \geq \frac{1}{2} w(P).$$

Luego, por lo anterior tenemos que

$$\sum_{\mathfrak{p}\in P} \log(\mathcal{N}_K(\mathfrak{p})) = \sum_{\mathfrak{p}\in P} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \mathcal{N}_K(\mathfrak{p}) \geq \sum_{\substack{\mathcal{N}_K(\mathfrak{p})\geq Q^a \\ \mathfrak{p}\in P}} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} Q^a \geq \frac{1}{2} w(P) Q^a.$$

La hipótesis $w(P) \geq \kappa w(\mathcal{P}(Q))$ y la desigualdad (22), implican que el lado derecho de la desigualdad anterior es al menos $\frac{1}{2}\kappa c_{1,K} \log(Q) Q^a$. Por lo tanto, (30) implica que

$$3\log(N) \geq \left(\frac{1}{\alpha} - \frac{1}{|S|}\right) \frac{1}{2} \kappa c_{1,K} \log(Q) Q^a.$$

Recordando que $Q = N^\gamma$, vemos que para N suficientemente grande, esto solo puede suceder si $|S| \leq \alpha$. □

Capítulo 3

Cambio de variables efectivo

El resultado principal de este capítulo es que el Teorema 0.5 se deduce de un resultado similar para espacios afines. Para hacer eso, se van a hacer dos reducciones. El primer paso es reducir el problema al de estudiar subconjuntos de variedades afines. Notar que esto es estándar, por ejemplo, ver el Capítulo 14 en [**Ser89**], donde se obtiene un límite superior para el número de puntos racionales en un conjunto delgado(thin sets) que se encuentra en un espacio proyectivo como consecuencia de un límite análogo para conjuntos delgado del espacio afín. El segundo paso es reducir aún más este problema pasando de una variedad afín de dimensión d al espacio afín $\mathbb{A}^d$. Para ello, se realiza un cambio de variables. Esto se logrará mediante la normalización de Noether. Dado que el Teorema 0.5 es uniforme en el grado y dimensión de la variedad, se requiere cierta efectividad en la normalización. Para ello, se proporciona una versión efectiva del teorema de normalización de Noether, con métodos bastante elementales.

1. Reducción al caso afín

Para comodidad del lector, recordamos el enunciado del Teorema 0.5.

Teorema 0.5. Sean $0 \leq k < d-1$ enteros, $D, M > 0$ enteros positivos, y sean $\varepsilon, \alpha, \kappa, \eta > 0$ números reales positivos. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2(d+1)}}$ y sea

$$P \subseteq \mathcal{P}(Q) := \{\mathfrak{p} \text{ primo de } \mathcal{O}_K : |\mathcal{O}_K/\mathfrak{p}| \leq Q\}$$

un subconjunto de primos que cumple

$$w(P) := \sum_{\mathfrak{p} \in P} \frac{\log(|\mathcal{O}_K/\mathfrak{p}|)}{|\mathcal{O}_K/\mathfrak{p}|} \geq \kappa w(\mathcal{P}(Q)).$$

Para $\mathbf{x} \in \mathbb{P}^M(K)$ sea $H(\mathbf{x})$ su altura absoluta multiplicativa. Entonces, existe una constante $C = C(d, k, \varepsilon, \alpha, \eta, K, D, M)$ tal que para cualquier conjunto $S \subseteq \{\mathbf{x} \in \mathbb{P}^M(K) : H(\mathbf{x}) \leq N\}$ ocupando menos de $\alpha|\mathcal{O}_K/\mathfrak{p}|^k$ clases residuales para todo primo $\mathfrak{p}$ (i.e. la imagen de S en $\mathbb{P}^M(\mathcal{O}_K/\mathfrak{p})$ posee a lo sumo $\alpha|\mathcal{O}_K/\mathfrak{p}|^k$ elementos), y que esta contenida en una variedad proyectiva $Z \subseteq \mathbb{P}^M$ definida sobre K, geométricamente irreducible de dimensión d y grado D, al menos una de las siguientes afirmaciones vale:

- (S es pequeño) $|S| \lesssim_{d,k,\varepsilon,\alpha,K,D,M} N^{d_K k+\varepsilon}$;

- (S es fuertemente algebraico) existe un polinomio homogéneo de grado a lo sumo C en $\mathcal{O}_K[X_0, \ldots, X_M]$ con coeficientes de altura acotada por N^C anulándose en al menos $(1-\eta)|S|$ puntos de S, que se no anula sobre Z.

Para llevar a cabo el primer paso de lo mencionado al inicio de este capítulo, se procede a enunciar la siguiente variante del Teorema 0.5 para variedades afines.

Teorema 3.1 (Caso Afín del Teorema 0.5). *Sean $0 \leq k < d$ enteros, D, M enteros positivos, y sean $\varepsilon, \alpha, \kappa, \eta > 0$ números reales positivos. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2(d+1)}}$ y sea $P \subseteq \mathcal{P}(Q)$ un subconjunto que cumple $w(P) \geq \kappa w(\mathcal{P}(Q))$. Entonces existe una constante $C = C(d, k, \varepsilon, \alpha, \eta, K, D, M)$, tal que para cualquier conjunto $S \subseteq [N]_{\mathbb{A}^{M+1}(\mathcal{O}_K)}$ que ocupa menos de $\alpha \mathcal{N}_K(\mathfrak{p})^k$ clases residuales para cada primo $\mathfrak{p}$, y que se encuentra sobre una variedad afín $Z \subseteq \mathbb{A}^{M+1}$ definida sobre K, geométricamente irreducible de dimensión $d+1$ y grado D, al menos una de las siguientes situaciones sucede:*

- *(S es pequeño) $|S| \lesssim_{d,k,\varepsilon,K,D,M} N^{k-1+\varepsilon}$;*
- *(S es fuertemente algebraico) existe un polinomio homogéneo de grado como mucho C y coeficientes de altura acotada por N^C en $\mathcal{O}_K[X_0, \ldots, X_M]$ que se anula en al menos $(1-\eta)|S|$ puntos de S, que no se anula sobre Z.*

Observación 3.2. Hay que hacer dos comentarios sobre el enunciado del Teorema 3.1. Primero, en el caso de que S sea pequeño, d_K no aparece en el exponente de N. Esto se debe al hecho de que aquí se usa la altura relativa a K en lugar de la altura absoluta como en el Teorema 0.5. Esto se debe a que simplificará parte de la notación de las demostraciones y también que refleja con mayor precisión la naturaleza del problema que se esta estudiando, que es relativo al cuerpo global K. La segunda observación es sobre los parámetros k, d y M; la elección de $M+1$ en lugar de M y Z de dimensión $d+1$ en lugar de dimensión d se debe a que se levanta un subconjunto $S \subseteq Z \subseteq \mathbb{P}^M$ ocupando menos de $\lesssim \mathcal{N}_K(\mathfrak{p})^k$ clases residuales para cada primo $\mathfrak{p}$, con Z una variedad proyectiva. Por lo tanto, el conjunto elevado $\overline{S}$ estará en el cono afín $C(Z) \subseteq \mathbb{A}^{M+1}$ que es una variedad geométricamente irreducible de dimensión $d+1$ y grado D.

Demostración de que el Teorema 3.1 implica Teorema 0.5. Sea S como en el enunciado del Teorema 0.5. En particular, $|[S]_{\mathfrak{p}}| \leq \alpha \mathcal{N}_K(\mathfrak{p})^k$ para todo primo $\mathfrak{p}$ y para algún α positivo y $0 \leq k < \dim(Z)$. Por la Proposición 1.1, es posible levantar S a un subconjunto $\overline{S} \subseteq [cN]_{\mathbb{A}^{M+1}(\mathcal{O}_K)}$ contenido en el cono afín $C(Z) \subseteq \mathbb{A}^{M+1}$, donde c es una constante positiva que depende solo de K. Observar que $C(Z)$ posee dimensión $\dim(Z)+1$ y grado $\deg(Z)$. Sea $\mathfrak{p} \in P$. Acotemos $[\overline{S}]_{\mathfrak{p}}$. Dado $\mathbf{x}' = (x_0, \ldots, x_{M+1}) \in \overline{S}$, hay dos posibilidades: $\mathfrak{p} | x_i$ para todo i, o existe i_0 tal que $\mathfrak{p} \nmid x_{i_0}$. En el segundo caso, $(x_0 (\mathrm{mod}\ \mathfrak{p}), \ldots, x_{M+1} (\mathrm{mod}\ \mathfrak{p}))$ define un punto en $\mathbb{P}^M(\mathcal{O}_K/\mathfrak{p})$ que coincide con la reducción módulo $\mathfrak{p}$ de $\mathbf{x} = (x_0 : \ldots : x_{M+1}) \in S$. Recordar que cada punto en $\mathbb{P}^M(\mathcal{O}_K/\mathfrak{p})$ posee $(\mathcal{N}_K(\mathfrak{p}) - 1)$ levantados a $\mathbb{A}^{M+1}(\mathcal{O}_K/\mathfrak{p})$. Luego, la cantidad de puntos en $[\overline{S}]_{\mathfrak{p}}$

que verifican la segunda condición esta acotada por $(\mathcal{N}_K(\mathfrak{p})-1)|[S]_{\mathfrak{p}}| \leq \alpha\mathcal{N}_K(\mathfrak{p})^{k+1}$. Mientras tanto, en el primer caso, solo tenemos que los puntos se reducen a la clase 0 en $(\mathcal{O}_K/\mathfrak{p})^{M+1}$. Se concluye que $|[\overline{S}]_{\mathfrak{p}}| \leq \alpha\mathcal{N}_K(\mathfrak{p})^{k+1}+1 \leq \max\{\alpha,1\}\mathcal{N}_K(\mathfrak{p})^{k+1} = \alpha'\mathcal{N}_K(\mathfrak{p})^{k+1}$. Por lo tanto, $\overline{S}$ satisface las hipótesis del Teorema 3.1 (con $k := k+1$ y $\alpha := \alpha'$) y al menos uno de los siguientes situaciones se cumple:

- $|S| = |\overline{S}| \lesssim_{d,k,\varepsilon,K,D,M} (cN)^{(k+1)-1+\varepsilon} \lesssim_{d,k,\varepsilon,K,D,M} N^{k+\varepsilon}$;
- existe un polinomio homogéneo $f \in \mathcal{O}_K[X_0,\ldots,X_M]$ de grado como mucho $C = O_{d,k,\varepsilon,K,D,M,\eta}(1)$ y coeficientes de altura acotada por N^C que se anula en al menos $(1-\eta)|\overline{S}| = (1-\eta)|S|$ puntos de $\overline{S}$, que no se anula sobre $C(Z)$.

A partir de lo cual, se deduce el Teorema 0.5. □

2. Una normalización de Noether efectiva

Hasta el momento, se redujo el Teorema 0.5 a un problema sobre variedades afines. Para continuar con el segundo paso discutido en la introducción de este capítulo, aquí se demuestra la siguiente versión del teorema de normalización de Noether.

Teorema 3.3 (Normalización de Noether efectiva). *Sea $V \subseteq \mathbb{P}^m$ una variedad proyectiva irreducible definida sobre un cuerpo global K. Entonces existe un mapa finito $\varphi : V \to \mathbb{P}^{\dim(V)}$, definido sobre $\mathbb{k}$, tal que*

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

con $L_0(\mathbf{x}),\ldots,L_{\dim(V)}(\mathbf{x})$ formas lineales con coeficientes en $\mathbb{k}$ de altura acotada por $\lesssim_{\mathbb{k},m} (\deg(V))^{m-\dim(V)}$ donde las constantes implícitas son efectivamente computables. Además, cada fibra de φ tiene como mucho $\deg(V)$ elementos. En particular, la misma afirmación se cumple para una variedad afín $Z \subseteq \mathbb{A}^m$.

Demostración. Sea V una variedad irreducible como en el enunciado del teorema. Si $V = \mathbb{P}^m$, tomamos φ el mapa identidad y concluimos. Si $V \subsetneq \mathbb{P}^m$, entonces existe $\mathbf{x} \in \mathbb{P}^m(\overline{\mathbb{k}})\backslash V(\overline{\mathbb{k}})$. Además, veamos que se puede elegir $\mathbf{x}$ con coordenadas en K, y de altura pequeña. Si $\dim(V) = m-1$, V es una hipersuperficie. Si no, lo reducimos al caso de la hipersuperficie por medio de una idea geométrica estándar (ver, por ejemplo, el Teorema 1 en [**Mum70**], o su reimpresión en [**Mar10**]). De hecho, para eso, eligir un subespacio proyectivo genérico W de $\mathbb{P}^m(\overline{\mathbb{k}})$ de dimensión $m-\dim(V)-2$, y considerar el cono $C(W,V)$ formado por la unión de todas las rectas que unen un punto en W con un punto en V. Es genéricamente una subvariedad proyectiva de dimensión $m-1$, es decir, una hipersuperficie. Además, tiene grado $\deg(V)$, por lo que $C(W,V)$ está definido por un polinomio con coeficientes en $\overline{\mathbb{k}}$, de grado $\deg(V)$. En cualquier caso, se tiene que V está contenido en una hipersuperficie $\mathcal{Z}(f) \subseteq \mathbb{P}^m(\overline{\mathbb{k}})$, donde $f \in \overline{\mathbb{k}}[T_0,\ldots,T_m]$ es un polinomio homogéneo distinto de cero, de grado $\deg(V)$.

Supongamos que f tiene un coeficiente distinto de cero en $T_0^{d_0}\cdots T_m^{d_m}$. Consideremos el conjunto $[\deg(V)]_{\mathcal{O}_{\mathbb{k}}} = \{x \in \mathcal{O}_{\mathbb{k}} : H(x) \leq \deg(V)\}$ (notar que aquí se esta

usando la altura absoluta en lugar de la altura relativa a K). Este tiene estrictamente más de $\deg(V) \geq d_i$ elementos. Por el Nullstellensatz Combinatorio, Teorema 9.2 en [**TV10**], existe $x_0, \ldots, x_n \in [\deg(V)]_{\mathcal{O}_{\Bbbk}}$ tal que $f(x_0, \ldots, x_m) \neq 0$. En particular $(x_0, \ldots, x_m) \neq 0$. Sea $\mathbf{x}_1 \in \mathbb{P}^m$ el punto con coordenadas proyectivas $(x_0 : \ldots : x_m)$. Por construcción, $\mathbf{x}_1 \in \mathbb{P}^m(\Bbbk) \backslash V(\Bbbk)$. Ahora, construyamos formas lineales $L_{1,1}(T_0, \ldots, T_m), \ldots, L_{1,m}(T_0, \ldots, T_m) \in \Bbbk[T_0, \ldots, T_m]$ tal que $\mathcal{Z}(L_{1,1}, \ldots, L_{1,m})$ es igual a $\{\mathbf{x}_1\}$. Notar que los coeficientes de tales formas lineales son una base del espacio vectorial $V_1 := \langle (x_0, \ldots, x_m) \rangle^{\perp}$ definido sobre $\Bbbk$. Así, si queremos construir las formas lineales $L_{1,i}$'s con coeficientes de altura pequeña, basta con encontrar una base de altura pequeña de V_1. Para esto, usamos las generalizaciones del lema de Siegel para cuerpos de números y cuerpos funcional en [**BV83, Thu95, Fuk10**] para encontrar una base $\mathbf{y}_1, \ldots, \mathbf{y}_m \in K^{m+1}$ de V_1 tal que

$$\prod_{i=1}^{m} H(1 : \mathbf{y}_i) \lesssim_{\Bbbk,m} H(V_1), \tag{32}$$

donde $H(V_1)$ es la altura de V_1. Por dualidad (ver, por ejemplo, el Teorema de la Dualidad en [**Thu93**]), se tiene que $H(V_1)$ coincide con la altura del subespacio lineal generado por el $\Bbbk$-vector $(x_0, \ldots, x_m)$. Además esta altura coincide con la altura proyectiva $H(x_0 : \ldots : x_m)$. De este modo

$$\prod_{i=1}^{m} H(1 : \mathbf{y}_i) \lesssim_{\Bbbk,m} H(x_0 : \ldots : x_m) \lesssim_{\Bbbk,m} \deg(V). \tag{33}$$

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

$$\varphi_1(\mathbf{x}) = (L_{1,1}(\mathbf{x}) : \ldots : L_{1,m}(\mathbf{x})). \tag{34}$$

Luego φ_1 es un morfismo finito (ver Teorema 7 de la Sección 5.3 del Capítulo 1 de [**Sha74**]), con $L_{1,1}, \ldots, L_{1,m}$ formas lineales con coeficientes de altura acotada por $\lesssim_{\Bbbk,m} \deg(V)$. Si $\varphi_1(V) = \mathbb{P}^{m-1}$, obtenemos lo deseado. Ahora, supongamos lo contrario. Entonces para un espacio lineal genérico $L \subseteq \mathbb{P}^{m-1}$ de codimensión $\dim(V)$, se cumple que $L \cap \varphi_1(V)$ es finito. Además, la preimagen de $L \cap \varphi_1(V)$ por φ_1 es finita (al ser φ_1 un morfismo finito, este tiene fibras finitas), y esta intersección es igual a la intersección de V por algún subespacio lineal $L' \subseteq \mathbb{P}^m$ de codimensión $\dim(V)$ (un morfismo finito conserva la dimensión). Así $|L \cap \varphi_1(V)| \leq |L' \cap V| \leq \deg(V)$, de donde concluimos que el grado de $\varphi_1(V)$ es como mucho $\deg(V)$.

En conclusión, la variedad proyecitva irreducible $\varphi_1(V)$ tiene dimensión $\dim(V)$ y $\deg(\varphi_1(V)) \leq \deg(V)$. Por lo tanto, podemos repetir el argumento anterior y obtener una sucesión de mapas finitos $\varphi_{i+1} : \varphi_i(V) \to \mathbb{P}^{m-i+1}$, definida por

$$\varphi_{i+1}(\mathbf{x}) = (L_{i+1,1}(\mathbf{x}) : \ldots : L_{i+1,m-i+1}(\mathbf{x})), \tag{35}$$

con $L_{i+1,1}, \ldots, L_{i+1,m-i+1}$ formas lineales con coeficientes en $\Bbbk$ de altura acotada por $\lesssim_{\Bbbk,m} \deg(V)$. Dado que la sucesión $\varphi_1, \varphi_2, \ldots$ termina con $i = m - \dim(V)$, concluimos

que existe un morfismo finito $\varphi : V \to \mathbb{P}^{\dim(V)}$ tal que

$$\varphi(\mathbf{x}) = (L_0(\mathbf{x}) : \ldots : L_{\dim(V)}(\mathbf{x})), \tag{36}$$

con $L_0, \ldots, L_m$ formas lineales con coeficientes en $\Bbbk$ cuya altura está acotada por $\lesssim_{\Bbbk,m} \deg(V)^{m-\dim(V)}$.

Finalmente, tenga en cuenta que el morfismo $\varphi : V \to \mathbb{P}^{\dim(V)}$ que construimos puede interpretarse geométricamente como la proyección fuera de un subespacio lineal genérico $L \subseteq \mathbb{P}^m$ de codimensión $\dim(V)+1$. Así, dado $\mathbf{z} \in \mathbb{P}^{\dim(V)}$ los puntos en la fibra $\varphi^{-1}(\mathbf{z})$ corresponden a los puntos que se encuentra en la intersección del cono afín $C(V) \subseteq \mathbb{A}^{m+1}$ de V con respecto a un subespacio lineal afín $L' \subseteq \mathbb{A}^{m+1}$. Como el cono afín $C(V)$ tiene el mismo grado de V, concluimos que $|\varphi^{-1}(\mathbf{z})| \leq |C(Z) \cap L'| \leq \deg(V)$. □

3. Reducción al caso del plano afín

Ahora estamos en condiciones de hacer la última reducción del Teorema 0.5. En concreto, mediante un cambio efectivo de variables, reduciremos la prueba del Teorema 3.1 para probar el siguiente enunciado.

Teorema 3.4 (Caso $Z = \mathbb{A}^{d+1}$). *Sean $0 \leq k < d$ enteros, y sean $\varepsilon, \alpha, \kappa, \eta > 0$ números reales positivos. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2(d+1)}}$ y sea $P \subseteq \mathcal{P}(Q)$ un subconjunto que cumple $w(P) \geq \kappa w(\mathcal{P}(Q))$. Entonces, existe una constante $C = C(d, k, \varepsilon, \alpha, \eta, K)$, tal que para cualquier conjunto $S \subseteq [N]^{d+1}_{\mathcal{O}_K}$ que ocupa menos de $\alpha \mathcal{N}_K(\mathfrak{p})^k$ clases residuales para cada primo $\mathfrak{p}$, al menos una de las siguientes situaciones sucede:*

- *(S es pequeño) $|S| \lesssim_{d,k,\varepsilon,K} N^{k-1+\varepsilon}$;*
- *(S es fuertemente algebraico) existe un polinomio homogéneo no nulo, de grado a lo sumo C y coeficientes de altura acotada por N^C en $\mathcal{O}_K[X_0, \ldots, X_d]$ que se anula en al menos $(1-\eta)|S|$ puntos de S,*

Demostración de que Teorema 3.4 implica Teorema 3.1. Sea $S \subseteq Z \subseteq \mathbb{A}^{M+1}$ como en el Teorema 3.1. Por Teorema 3.3 existe un mapa finito $\mathbf{F} = (F_1, \ldots, F_{d+1}) : Z \to \mathbb{A}^{d+1}$ tal que para todo i, $F_i \in \mathcal{O}_{\Bbbk}[X_0, \ldots, X_M]$ es una forma lineal con coeficientes de altura acotada por $\lesssim_{\Bbbk,M,d,D} 1$. Observar que por (5) y (11) se tiene que $\mathbf{F}(S) \subseteq [cN]_{\mathbb{A}^{d+1}(\mathcal{O}_K)} \subseteq [cN]^{d+1}_{\mathcal{O}_K}$ para algún $c = O_{K,M,d,D}(1)$. Dado que $\mathbf{F}$ preservar congruencias, para cada primo $\mathfrak{p} \in P$ se tiene que $|[\mathbf{F}(S)]_{\mathfrak{p}}| \leq |[S]_{\mathfrak{p}}| \leq \alpha \mathcal{N}_K(\mathfrak{p})^k$ con $k < d+1$. Luego, $\mathbf{F}(S)$ satisface las condiciones del Teorema 3.4, entonces aplicando el a $\mathbf{F}(S)$ con $\eta = \frac{1}{2}$ se concluye que

- $|\mathbf{F}(S)| \lesssim_{d,k,\varepsilon,K} N^{k-1+\varepsilon}$; o
- existe un polinomio homogéneo $g \in \mathcal{O}_K[Y_0, \ldots, Y_d]$ de grado como mucho C con coeficientes de altura acotada por N^C, que se anula en al menos $\frac{1}{2}|\mathbf{F}(S)|$ puntos de $\mathbf{F}(S)$.

Supongamos que ocurre la primera posibilidad. Como $\mathbf{F}$ tiene grado como máximo $\deg(Z) = D$, tenemos $|\mathbf{F}(S)| \geq \frac{|S|}{\deg(Z)}$, entonces deducimos que $|S| \lesssim_{d,k,\varepsilon,K,D} N^{k-1+\varepsilon}$. Si ocurre la segunda posibilidad, usando nuevamente que $\mathbf{F}$ tiene grado a lo sumo $\deg(Z) = D$, concluimos que $g \in \mathcal{O}_K[Y_0, \ldots, Y_d]$ es un polinomio homogéneo de grado como mucho C que se anula en al menos $\frac{1}{2}|\mathbf{F}(S)| \geq \frac{1}{2D}|S| := \eta_0|S|$ puntos de $\mathbf{F}(S)$. Sea $f(X_0, \ldots, X_M) := g(\mathbf{F}(X_0, \ldots, X_M))$. Como $g \neq 0$ y $\mathbf{F}$ es sobreyectiva, concluimos que f es un polinomio homogéneo de grado a lo sumo C, nulo en al menos $\eta_0|S|$ puntos de S, que no se anula en Z. Además, dado que f es la composición de las funciones polinómicas $\mathbf{F}$ y g, y sus coeficientes están acotados por $\lesssim_{\mathbb{k},M,d,D} 1$ y N^C respectivamente, vemos que existe una constante $C' = C'(d, k, \varepsilon, \alpha, \eta_0, K, D, M)$, tal que f tiene grado acotado por C', y coeficientes de altura acotados por $N^{C'}$. Por lo tanto, concluimos el Teorema 3.1 para $\eta_0 = \frac{1}{2D}$. El Teorema 3.1 se concluye para cualquier η mediante un argumento de partición. $\square$

Capítulo 4

Caracterización de conjuntos mal distribuidos sobre clases residuales en el espacio afín sobre cuerpos globales

1. El problema inverso de criba en el espacio afín sobre cuerpos globales

En esta sección vamos a deducir el Teorema 3.4 del Capítulo 3 como una consecuencia de la siguiente versión más fuerte.

TEOREMA 4.1. *Sea $d \in \mathbb{N}$ y $h > 1$ y sea $\varepsilon, \eta > 0$ un número real positivo. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2d}}$ y sea $P \subseteq \mathcal{P}(Q)$ un subconjunto que cumple $w(P) \geq \kappa w(\mathcal{P}(Q))$ para algún $\kappa > 0$. Supongamos que $S \subseteq [N]^d_{\mathcal{O}_K}$ es un subconjunto de tamaño al menos $|S| \geq cN^{d-h-1+\varepsilon}$ ocupando como mucho $\alpha \mathcal{N}_K(\mathfrak{p})^{d-h}$ clases residuales módulo $\mathfrak{p}$ para todo primo $\mathfrak{p} \in P$ y algún $\alpha > 0$. Entonces si N es suficientemente grande, existe un polinomio homogéneo no nulo $f \in \mathcal{O}_K[X_1, \ldots, X_d]$ de grado $O_{d,h,\varepsilon,\eta,\kappa,K}(1)$ y coeficientes de altura acotada por $N^{O_{d,h,\varepsilon,\eta,\kappa,K}(1)}$ que se anula en al menos $(1-\eta)|S|$ puntos de S.*

Observar que el Teorema 3.4 del Capítulo 3 ha sido enunciado para $S \subseteq [N]^{d+1}_{\mathcal{O}_K}$ en lugar de $S \subseteq [N]^d_{\mathcal{O}_K}$. El motivo para hacer esto se ha explicado en la Observación **??**. Teniendo esto en cuenta, el cambio de variables $k := d - h$ (observar que debemos tomar $h > 1$ para que $k < d - 1$ asi como está en el enunciado del Teorema 3.4), muestra que el Teorema 4.1 implica el Teorema 3.4.

Para demostrar el Teorema 4.1, seguimos la demostración del Teorema 2.4 en [**Wal12**]. La idea de la prueba es construir un "subconjunto característico" pequeño $A \subseteq S$ con la propiedad de que cualquier polinomio "pequeño" que se anule en A también se anule en una proporción positiva de S. Esto se hará en la Proposición 4.10, que es una adaptación de la Proposición 2.2 en [**Wal12**]. Para lograr esto, vamos a hacer inducción en d, con h fijo. Para ello, primero mostraremos que una proporción grande de las fibras de S son grandes y están mal distribuidas. Según la hipótesis inductiva, cada una de estas fibras contiene un subconjunto característico pequeño. El siguiente paso técnico será pegar algunos de estos subconjuntos características para obtener el subconjunto característico pequeño A de S. Entonces, al ser A pequeño podremos utilizar una variante del lema de Siegel para construir un polinomio homogéneo pequeño que se anule en A.

En la mayor parte de la demostración del Teorema 4.1, h puede tomarse como cualquier número entero positivo. Es solo en la sección §2 de este capítulo, donde construimos un polinomio homogéneo pequeño, cuando necesitamos usar que $h > 1$.

1.1. Genericidad. Primero extendemos la noción de "conjunto genérico" dada en [**Wal12**], y luego demostramos que cualquier conjunto que satisfaga las condiciones del Teorema 4.1 contiene subconjuntos genéricos grandes. Para ello, introducimos la siguiente notación. Dado $S \subseteq [N]^d_{\mathcal{O}_K}$, $\mathbf{a} \in (\mathcal{O}_K/\mathfrak{p})^d$, $a \in \mathcal{O}_K/\mathfrak{p}$ y $x \in [N]_{\mathcal{O}_K}$,

$$\begin{aligned} S(\mathbf{a}, \mathfrak{p}) &:= \{\mathbf{x} = (x_1, \dots, x_d) \in S : \pi_{\mathfrak{p}}(\mathbf{x}) = \mathbf{a}\}, \\ S(a, \mathfrak{p}) &:= \{\mathbf{x} = (x_1, \dots, x_d) \in S : x_1 \equiv a (\mathrm{mod}\ \mathfrak{p})\}, \\ S_x &:= S \cap \pi_1^{-1}(x). \end{aligned}$$

Definición 4.2 (Genericidad). Dado un número real $B > 0$ y un entero $l \geq 0$ decimos que un conjunto $S \subseteq [N]^d_{\mathcal{O}_K}$ es (B, l)-genérico módulo $\mathfrak{p}$ si

$$\frac{|S(\mathbf{a}, \mathfrak{p})|}{|S|} < \frac{B}{\mathcal{N}_K(\mathfrak{p})^l},$$

para cada clase residual $\mathbf{a}$ modulo $\mathfrak{p}$.

La noción de genericidad captará el hecho de que las secciones de S, en promedio, comparten muchas clases residuales módulo $\mathfrak{p}$ para muchos primos $\mathfrak{p}$.

Lema 4.3. *Sea $d, h \geq 1$ enteros arbitrarios y sea $\varepsilon > 0$ un número real positivo. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2d}}$ y sea $P \subseteq \mathcal{P}(Q)$ un subconjunto que cumple $w(P) \geq \kappa w(\mathcal{P}(Q))$ para algún $\kappa > 0$. Supongamos que $S \subseteq [N]^d_{\mathcal{O}_K}$ es un subconjunto de tamaño al menos $cN^{d-h-1+\varepsilon}$ ocupando como mucho $\alpha \mathcal{N}(\mathfrak{p})^{d-h}$ clases residuales módulo $\mathfrak{p}$ para todo primo $\mathfrak{p} \in P$ y algún $\alpha > 0$. Entonces para N suficientemente grande, existen constantes $B = B(d, h, \varepsilon, \kappa, \alpha, c, K)$, $\kappa_1 = \kappa_1(d, h, \varepsilon, \kappa, \alpha, c, K)$, $c_1 = c_1(d, h, \varepsilon, \kappa, \alpha, c, K)$ tales que existe un subconjunto de primos $P' \subseteq P$ con $w(P') \geq \kappa_1 w(P)$ tal que para cada $\mathfrak{p} \in P'$ existe un subconjunto $\mathcal{G}_{\mathfrak{p}}(S) \subseteq S$ con $|\mathcal{G}_{\mathfrak{p}}(S)| \geq c_1|S|$, el cual es $(B, d-h)$-genérico módulo $\mathfrak{p}$.*

Demostración. De ahora en adelante, fijemos un número entero $h \geq 1$. Si $d \leq h$, entonces podemos tomar $B = 2$, $\mathcal{G}_{\mathfrak{p}}(S) = S$ y $P' = P$. Luego

$$B = B(d, h, \varepsilon, \kappa, \alpha, c, K) = 2, \tag{37}$$

$$\kappa_1 = \kappa_1(d, h, \varepsilon, \kappa, \alpha, c, K) = 1, \tag{38}$$

$$c_1 = c_1(d, h, \varepsilon, \kappa, \alpha, c, K) = 1. \tag{39}$$

Ahora procedemos por inducción sobre d. Supongamos que $d \geq h+1$ es un número entero y supongamos que el Lema 4.3 es válido para cada dimensión más pequeña. Sean S y P como en el enunciado. Para cada $1 \leq i \leq d$, definimos $\pi_i : K^d \to K$ como la proyección sobre la i-ésima coordenada.

Afirmación 4.4. *Existe una constante $C_3 = C_3(d, h, \varepsilon, \kappa, \alpha, c)$ tal que si $N \geq C_3$ entonces existe $1 \leq i \leq d$ y un subconjunto $\tilde{S} \subseteq S$ con $|\tilde{S}| \geq \frac{|S|}{2^d}$ tal que para cada $A \subseteq \tilde{S}$ con $|A| \geq \frac{|\tilde{S}|}{2}$ se tiene que $|\pi_i(A)| \geq Q$.*

Demostración de la Afirmación 4.4. Supongamos que la afirmacion es falsa para $\tilde{S} = S$ and $i = 1$. Entonces existe $A_1 \subseteq S$ con $|A_1| \geq \frac{|S|}{2}$ y $|\pi_1(A_1)| < Q$. Luego, si la afirmación es falsa para $\tilde{S} = A_1$ e $i = 2$, existe $A_2 \subseteq A_1$ con $|A_2| \geq \frac{|A_1|}{2} \geq \frac{|S|}{2^2}$ y $|\pi_1(A_2)|, |\pi_2(A_2)| < Q$. Iterando este proceso d veces, o bien concluimos la afirmación o bien terminamos con un subconjunto $A_d \subseteq S$ con $|A_d| \geq \frac{|S|}{2^d}$. Luego,

$$cN^{d-h-1+\varepsilon} \leq |S| \leq 2^d |A_d| \leq 2^d \prod_{i=1}^{d} |\pi_i(A_d)| < 2^d Q^d = 2^d N^{\frac{\varepsilon}{2}}. \tag{40}$$

Ahora, (40) es absurdo si $N \geq \left(\frac{2^d}{c}\right)^{\frac{1}{d-h-1+\frac{\varepsilon}{2}}}$. □

Por la Afirmación 4.4, a costa de pasar a un subconjunto de S de densidad al menos igual a $\frac{1}{2^d}$ y permutando las variables, de ahora en mas podemos asumir que S satisface

$$|\pi_1(A)| \geq Q \text{ para todo } A \subseteq S \text{ con } |A| \geq \frac{|S|}{2}. \tag{41}$$

El objetivo ahora es encontrar un subconjunto denso de S que esté en condiciones de aplicar la hipótesis inductiva sobre las fibras. Posteriormente se pegarán entre sí los conjuntos genéricos de las fibras de este subconjunto denso para obtener el conjunto genérico deseado. Para ello primero eliminaremos algunas fibras problemáticas. Sea $\mathfrak{p}$ un primo de P. Recordar que para cada $a \in \mathcal{O}_K/\mathfrak{p}$, $S(a, \mathfrak{p})$ denota el elemento $\mathbf{x}$ de S para el cual $\pi_1(\mathbf{x}) \equiv a \pmod{\mathfrak{p}}$. Sea B_1 una constante suficientemente grande, a elegir luego. Dado que $|[S]_{\mathfrak{p}}| \leq \alpha \mathcal{N}_K(\mathfrak{p})^{d-h}$, está claro que hay como mucho $\frac{\alpha}{B_1}\mathcal{N}_K(\mathfrak{p})$ clases residuales $a \in [\pi_1(S)]_{\mathfrak{p}} \subseteq \mathcal{O}_K/\mathfrak{p}$ para las cuales $|[S(a, \mathfrak{p})]_{\mathfrak{p}}| \geq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}$. Notemos

$$\mathcal{E}_1(\mathfrak{p}) := \left\{ a \in [\pi_1(S)]_{\mathfrak{p}} : |[S(a, \mathfrak{p})]_{\mathfrak{p}}| \geq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1} \right\}. \tag{42}$$

También escribiremos

$$\mathcal{E}_2(\mathfrak{p}) := \left\{ a \in [\pi_1(S)]_{\mathfrak{p}} : |S(a, \mathfrak{p})| \geq \frac{B_1}{\alpha \mathcal{N}_K(\mathfrak{p})} |S| \right\}. \tag{43}$$

A partir de la identidad $\sum_{a \in \mathcal{O}_K/\mathfrak{p}} |S(a, \mathfrak{p})| = |S|$ se sigue que $|\mathcal{E}_2(\mathfrak{p})| \leq \frac{\alpha}{B_1}\mathcal{N}_K(\mathfrak{p})$, por lo tanto si $\mathcal{E}(\mathfrak{p}) := \mathcal{E}_1(\mathfrak{p}) \cup \mathcal{E}_2(\mathfrak{p})$ es el conjunto de clases residuales excepcionales, se tiene que $|\mathcal{E}(\mathfrak{p})| \leq \frac{2\alpha}{B_1}\mathcal{N}_K(\mathfrak{p})$. Usaremos la criba más grande (Lema 2.2) para probar que pocos $x \in [N]_{\mathcal{O}_K}$ verifican que $x \pmod{\mathfrak{p}}$ pertenece a $\mathcal{E}(\mathfrak{p})$ para muchos $\mathfrak{p} \in P$. En efecto, consideremos el conjunto

$$X := \left\{ x \in [N]_{\mathcal{O}_K} : \sum_{\mathfrak{p} \in P} 1_{x \pmod{\mathfrak{p}} \in \mathcal{E}(\mathfrak{p})} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \geq \frac{1}{2} w(P) \right\}. \tag{44}$$

Sea $P_1 \subseteq P$ el conjunto de primos tales que al menos $\frac{1}{4}|X|$ elementos de X se encuentran en el conjunto excepcional de clases residuales $\mathcal{E}(\mathfrak{p})$, es decir,

$$P_1 := \left\{ \mathfrak{p} \in P : \left| \bigcup_{a \in \mathcal{E}(\mathfrak{p})} X(a, \mathfrak{p}) \right| \geq \frac{1}{4}|X| \right\}.$$

Afirmación 4.5. $w(P_1) \geq \frac{1}{4} w(P)$.

Demostración de la Afirmación 4.5. Observar que

$$\sum_{a \in \mathcal{E}(\mathfrak{p})} |X(a, \mathfrak{p})| = \left| \bigcup_{a \in \mathcal{E}(\mathfrak{p})} X(a, \mathfrak{p}) \right| = \sum_{x \in X} 1_{x \pmod{\mathfrak{p}} \in \mathcal{E}(\mathfrak{p})}.$$

Por un lado se tiene que

$$\begin{aligned} \sum_{\mathfrak{p} \in P} \sum_{x \in X} 1_{x \pmod{\mathfrak{p}} \in \mathcal{E}(\mathfrak{p})} \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} &= \sum_{x \in X} \left(\sum_{\mathfrak{p} \in P} 1_{x \pmod{\mathfrak{p}} \in \mathcal{E}(\mathfrak{p})} \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} \right) \\ &\geq \sum_{x \in X} \frac{1}{2} w(P) \\ &= \frac{1}{2} w(P)|X|. \end{aligned} \tag{45}$$

Por otro lado,

$$\begin{aligned} &\sum_{\mathfrak{p} \in P} \sum_{x \in X} 1_{x \pmod{\mathfrak{p}} \in \mathcal{E}(\mathfrak{p})} \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} \\ &= \sum_{\mathfrak{p} \notin P_1} \left(\sum_{a \in \mathcal{E}(\mathfrak{p})} |X(a, \mathfrak{p})| \right) \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} + \sum_{\mathfrak{p} \in P_1} \left(\sum_{a \in \mathcal{E}(\mathfrak{p})} |X(a, \mathfrak{p})| \right) \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} \\ &< \sum_{\mathfrak{p} \notin P_1} \frac{1}{4}|X| \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} + \sum_{\mathfrak{p} \in P_1} |X| \frac{\log(\mathcal{N}(\mathfrak{p}))}{\mathcal{N}(\mathfrak{p})} \\ &= \frac{1}{4}|X| w(P \backslash P_1) + |X| w(P_1) \\ &= \frac{1}{4}|X| w(P) - \frac{1}{4}|X| w(P_1) + |X| w(P_1). \end{aligned} \tag{46}$$

Comparando (45) y (46), concluimos que $w(P_1) \geq \frac{1}{4} w(P)$. □

En Lema 2.2, tomando las constantes $\gamma := \frac{\varepsilon}{2d}$, $\kappa := \frac{\kappa}{4}$, $\mu := \frac{1}{4}$, $\alpha := \frac{2\alpha}{B_1}$, se sigue que si tomamos

$$B_1 := \frac{2\alpha}{C_1\left(\frac{\kappa}{4}, \frac{1}{4}, \frac{\varepsilon}{2d}, K\right)} = \frac{2^8 \alpha c_{5,K} d}{\kappa \varepsilon} \tag{47}$$

entonces $|X| < Q$. A partir de (41) se deduce que $|S\backslash\pi_1^{-1}(X)| \geq \frac{1}{2}|S|$.

La siguiente afirmación muestra que existe un subconjunto denso de S cuyas secciones están en condiciones de aplicar la hipótesis inductiva.

Afirmación 4.6. *Sea $0 < \nu < 1$. Existe un subconjunto $S' \subseteq S$ con $|S'| \geq \frac{1}{4}|S|$ que no interseca a $\pi_1^{-1}(X)$ y tal que para todo $x \in \pi_1(S')$, $S'_x := \pi_1^{-1}(x) \cap S'$ satisface $|S'_x| \geq c'(K,\nu)N^{d-h-2+\nu\varepsilon}$, donde $c'(K,\nu)$ es una constante positiva que depende de K, ν.*

Demostración de la Afirmación 4.6. La prueba será por contradicción. Supongamos que para todo $S' \subseteq S\backslash\pi_1^{-1}(X)$ con $|S'| \geq \frac{1}{4}|S|$ se tiene que $|S'_x| < c'(K,\nu)N^{d-h-2+\nu\varepsilon}$ para algún $x \in \pi_1(S')$. Sea

$$\overline{S} := \left\{ s \in S\backslash\pi_1^{-1}(X) : |(S\backslash\pi_1^{-1}(X))_{\pi_1(s)}| < c'(K,\nu)N^{d-h-2+\nu\varepsilon} \right\}.$$

Notar que $\overline{S}$ y $S\backslash\pi_1^{-1}(X)$ poseen las mismas secciones (siempre que la sección de $\overline{S}$ sea no vacía). Así, del supuesto deducimos que $|\overline{S}| \geq \frac{1}{2}|S\backslash\pi_1^{-1}(X)|$ y además $|\overline{S}_x| \leq c'(K,\nu)N^{d-h-2+\nu\varepsilon}$ para todo $x \in \pi_1(\overline{S})$. Luego,

$$\begin{aligned} \frac{1}{4}cN^{d-h-1+\varepsilon} \leq \frac{1}{4}|S| \leq |\overline{S}| &= \left| \bigcup_{x\in\pi_1(\overline{S})} \overline{S}_x \right| \\ &< c'(K,\nu)N^{d-h-2+\nu\varepsilon}|\pi_1(\overline{S})| \\ &\leq c'(K,\nu)N^{d-h-2+\nu\varepsilon}|[N]_{\mathcal{O}_K}|. \end{aligned} \tag{48}$$

Usando la Proposición 1.3 en (48), y utilizando la cota $\log(N) \leq \frac{|M_{K,\infty}|}{(1-\nu)\varepsilon} N^{\frac{(1-\nu)\varepsilon}{|M_{K,\infty}|}}$, obtenemos la inecuación

$$\begin{aligned} \frac{1}{4}cN^{d-h-1+\varepsilon} &\leq c'(K,\nu)N^{d-h-1+\nu\varepsilon}c''(K)(\log(N))^{|M_{K,\infty}|} \\ &\leq c'(K,\nu)c''(K)\left(\frac{d_K}{(1-\nu)\varepsilon}\right)^{d_K} N^{d-h-1+\varepsilon}. \end{aligned}$$

Sin embargo, esta inecuación es falsa tomando

$$c'(K,\nu) := \frac{c}{8c''(K)}\left(\frac{(1-\nu)\varepsilon}{d_K}\right)^{d_K}. \tag{49}$$

□

Tomemos S' como en la Afirmación 4.6. Cada $x \in \pi_1(S')$ cae afuera de X, por lo tanto, por la definición X dada en (44), cada $x \in \pi_1(S')$ tiene asociado el subconjunto de primos

$$P_x := \{\mathfrak{p} \in P : x(\mathrm{mod}\ \mathfrak{p}) \notin \mathcal{E}(\mathfrak{p})\} \tag{50}$$

que verifica $w(P_x) \geq \frac{1}{2}w(P) \geq \frac{1}{2}\kappa w(\mathcal{P}(Q))$. Dado que $\mathcal{E}_1(\mathfrak{p}) \subseteq \mathcal{E}(\mathfrak{p})$, tenemos que para cada $x \in \pi_1(S')$ y para cada $\mathfrak{p} \in P_x$, $|[S'_x]_\mathfrak{p}| \leq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}$. Además, por la definición de S' en la Afirmación 4.6, $|S'_x| \geq c'(K,\nu)N^{d-h-2+\nu\varepsilon}$. Como estamos haciendo inducción en d, en el paso $d-1$, el parámetro Q debe cambiarse a $N^{\frac{\nu\varepsilon}{2(d-1)}}$. Luego, si tomamos $\nu := \frac{d-1}{d} < 1$, el parámetro Q permanece sin cambios a lo largo de la prueba.

Estamos en condiciones de aplicar la hipótesis inductiva a cada S'_x con $x \in \pi_1(S')$, para concluir que existe un subconjunto $P'_x \subseteq P_x$ con $w(P'_x) \geq \kappa_1 w(P_x)$, y constantes c_1, B independientes de x, tal que para cada $\mathfrak{p} \in P'_x$ hay un conjunto $(B, d-h-1)$-genérico módulo $\mathfrak{p}$, $\mathcal{G}_\mathfrak{p}(S'_x) \subseteq S'_x$, que contiene al menos $c_1|S'_x|$ elementos. Aquí, la dependencia de las constantes es:

$$B = B\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, c'(K,\nu), K\right), \tag{51}$$

$$\kappa_1 = \kappa_1\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, c'(K,\nu), K\right), \tag{52}$$

$$c_1 = c_1\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, c'(K,\nu), K\right), \tag{53}$$

$$\nu = \frac{d-1}{d}, \tag{54}$$

donde B_1 y $c'(K,\nu)$ se determinaron en las ecuaciones (47) y (49) respectivamente.

Cada fibra S'_x tiene su propio conjunto de primos P'_x, con densidad $w(P'_x) \geq \kappa_1 w(P_x)$. El hecho de que κ_1 sea independiente de x, nos permitirá hallar un conjunto de primos $P' \subseteq P$ con $w(P') \gtrsim w(P)$ tal que para cada $\mathfrak{p} \in P'$ existirá un conjunto genérico módulo $\mathfrak{p}$, $\mathcal{G}_\mathfrak{p}(S)$, construido pegando los conjuntos genéricos módulo $\mathfrak{p}$ de las fibras S'_x. Comenzamos construyendo el conjunto P' en la siguiente afirmación.

Afirmación 4.7. *Existe una constante positiva $\beta > 0$ dependiendo del κ_1 dado por (52), y un conjunto de primos $P' \subseteq P$ con $w(P') \geq \frac{\kappa_1}{4}w(P)$ tal que para cada $\mathfrak{p} \in P'$ hay por lo menos $\beta|S'|$ elementos $s \in S'$ para los cuales $\mathfrak{p} \in P'_{\pi_1(s)}$.*

Demostración de la Afirmación 4.7. Sea $\beta > 0$ y consideremos el conjunto

$$P' := \left\{\mathfrak{p} \in P : \sum_{s \in S'} 1_{\mathfrak{p} \in P'_{\pi_1(s)}} \geq \beta|S'|\right\}.$$

Entonces,

$$\begin{aligned}\sum_{s\in S'}\sum_{\mathfrak{p}\in P} 1_{\mathfrak{p}\in P'_{\pi_1(s)}}\frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} &= \sum_{\mathfrak{p}\in P}\left(\sum_{s\in S'} 1_{\mathfrak{p}\in P'_{\pi_1(s)}}\right)\frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})}\\ &\le \sum_{\mathfrak{p}\notin P'}\beta|S'|\frac{\log(\mathcal{N}_K(p))}{\mathcal{N}_K(\mathfrak{p})} + \sum_{\mathfrak{p}\in P'}|S'|\frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})}\\ &= \beta|S'|w(P\backslash P') + |S'|w(P')\\ &= \beta|S'|w(P) - \beta|S'|w(P') + |S'|w(P').\end{aligned}$$

Por otro lado, recordando que $w(P'_x) \ge \kappa_1 w(P_x) \ge \frac{\kappa_1}{2}w(P)$, tenemos que

$$\sum_{s\in S'}\sum_{\mathfrak{p}\in P} 1_{\mathfrak{p}\in P'_{\pi_1(s)}}\frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} = \sum_{s\in S'} w(P'_{\pi_1(s)}) \ge \sum_{s\in S'}\frac{\kappa_1}{2}w(P) = \frac{\kappa_1}{2}w(P)|S'|.$$

Concluimos que $\left(\frac{\kappa_1}{2} - \beta\right)w(P) \le (1-\beta)\,w(P') < w(P')$. Basta con tomar

$$\beta = \frac{\kappa_1}{4}. \tag{55}$$

□

Para finalizar la prueba del Lema 4.3, para cada $\mathfrak{p} \in P'$ construimos un conjunto grande, genérico módulo $\mathfrak{p}$, $\mathcal{G}_{\mathfrak{p}}(S)$. Para ello, tomemos

$$\mathcal{G}_{\mathfrak{p}}(S) := \bigcup_{x:\mathfrak{p}\in P'_x}^{\bullet} \mathcal{G}_{\mathfrak{p}}(S'_x). \tag{56}$$

Observar que $\mathcal{G}_{\mathfrak{p}}(S) \cap \pi_1^{-1}(x) = \mathcal{G}_{\mathfrak{p}}(S'_x)$ es un conjunto $(B, d-h-1)$-genérico módulo $\mathfrak{p}$ para todo $x \in \pi_1(\mathcal{G}_{\mathfrak{p}}(S))$. La inecuación

$$\begin{aligned}|\mathcal{G}_{\mathfrak{p}}(S)| &= \left|\bigcup_{x:\mathfrak{p}\in P'_x}^{\bullet}\mathcal{G}_{\mathfrak{p}}(S'_x)\right| = \sum_{x:\mathfrak{p}\in P'_x}|\mathcal{G}_{\mathfrak{p}}(S'_x)| \ge c_1\sum_{x:\mathfrak{p}\in P'_x}|S'_x| \\ &= c_1\left|\left\{s\in S' : \mathfrak{p}\in P'_{\pi_1(s)}\right\}\right| > c_1\beta|S'| \ge \frac{c_1\beta}{2^2}|S|\end{aligned} \tag{57}$$

muestra que $\mathcal{G}_{\mathfrak{p}}(S)$ es grande en S.

Veamos ahora que $\mathcal{G}_{\mathfrak{p}}(S)$ es de hecho un conjunto genérico módulo $\mathfrak{p}$. Primero, observar que por construcción, las clases residuales módulo $\mathfrak{p}$ de $\pi_1(\mathcal{G}_{\mathfrak{p}}(S))$ no se encuentran en $\mathcal{E}(\mathfrak{p})$. Luego, recordando la definición de $\mathcal{E}_2(\mathfrak{p}) \subseteq \mathcal{E}(\mathfrak{p})$ dada en (43), se sigue que

$$|\mathcal{G}_{\mathfrak{p}}(S)(a,\mathfrak{p})| \le \frac{B_1}{\alpha\mathcal{N}_K(\mathfrak{p})}|S| \le \frac{2^2B_1}{c_1\beta\alpha}\frac{|\mathcal{G}_{\mathfrak{p}}(S)|}{\mathcal{N}_K(\mathfrak{p})}, \tag{58}$$

donde la segunda inecuación se debe a (57). Sea $\mathbf{a}$ una clase residual módulo $\mathfrak{p}$. Observar que

$$\begin{aligned}\mathcal{G}_{\mathfrak{p}}(S)(\mathbf{a},\mathfrak{p}) &= \left(\bigcup_{x:\mathfrak{p}\in P'_x}{}^{\cdot}\ \mathcal{G}_{\mathfrak{p}}(S'_x)\right)(\mathbf{a},\mathfrak{p}) \\ &= \bigcup_{x:\mathfrak{p}\in P'_x}{}^{\cdot}\ \mathcal{G}_{\mathfrak{p}}(S'_x)(\mathbf{a},\mathfrak{p}) \\ &= \bigcup_{\substack{x:\mathfrak{p}\in P'_x \\ x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}}{}^{\cdot}\ \mathcal{G}_{\mathfrak{p}}(S'_x)(\mathbf{a},\mathfrak{p}).\end{aligned} \tag{59}$$

Entonces, el hecho de que $\mathcal{G}_{\mathfrak{p}}(S'_x)$ es $(B, d-h-1)$-genérico módulo $\mathfrak{p}$ implica

$$\begin{aligned}|\mathcal{G}_{\mathfrak{p}}(S)(\mathbf{a},\mathfrak{p})| &= \left|\bigcup_{\substack{x:\mathfrak{p}\in P'_x \\ x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}}{}^{\cdot}\ \mathcal{G}_{\mathfrak{p}}(S'_x)(\mathbf{a},\mathfrak{p})\right| \\ &= \sum_{\substack{x:\mathfrak{p}\in P'_x \\ x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}} |\mathcal{G}_{\mathfrak{p}}(S'_x)(\mathbf{a},\mathfrak{p})| \\ &\le \sum_{\substack{x:\mathfrak{p}\in P'_x \\ x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}} |\mathcal{G}_{\mathfrak{p}}(S'_x)| \frac{B}{\mathcal{N}_K(\mathfrak{p})^{d-h-1}} \\ &= \frac{B}{\mathcal{N}_K(\mathfrak{p})^{d-h-1}} \sum_{\substack{x:\mathfrak{p}\in P'_x \\ x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}} |\mathcal{G}_{\mathfrak{p}}(S'_x)| \\ &= \frac{B}{\mathcal{N}_K(\mathfrak{p})^{d-h-1}} \left|\bigcup_{\substack{x:\mathfrak{p}\in P'_x \\ x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}}{}^{\cdot}\ \mathcal{G}_{\mathfrak{p}}(S'_x)\right|.\end{aligned} \tag{60}$$

El hecho de que $\bigcup_{x:x\equiv\pi_1(\mathbf{a})(\mathrm{mod}\ \mathfrak{p})}{}^{\cdot}\ \mathcal{G}_{\mathfrak{p}}(S'_x) \subseteq \mathcal{G}_{\mathfrak{p}}(S)(\pi_1(\mathbf{a}),\mathfrak{p})$, junto con (60) y (58) nos da que

$$\begin{aligned}|\mathcal{G}_{\mathfrak{p}}(S)(\mathbf{a},\mathfrak{p})| &\le \frac{B}{\mathcal{N}_K(\mathfrak{p})^{d-h-1}} |\mathcal{G}_{\mathfrak{p}}(S)(\pi_1(\mathbf{a}),\mathfrak{p})| \\ &\le \frac{B}{\mathcal{N}_K(\mathfrak{p})^{d-h-1}} 2^2 \frac{B_1}{c_1\beta\alpha} \frac{1}{\mathcal{N}_K(\mathfrak{p})} |\mathcal{G}_{\mathfrak{p}}(S)| \\ &= 2^2 \frac{BB_1}{c_1\beta\alpha} \frac{1}{\mathcal{N}_K(\mathfrak{p})^{d-h}} |\mathcal{G}_{\mathfrak{p}}(S)|.\end{aligned} \tag{61}$$

□

La prueba también muestra que las constantes en Lema 4.3 se pueden computar inductivamente de la siguiente forma: a partir de la Afirmación 4.7,

$$\kappa_1(d,h,\varepsilon,\kappa,\alpha,c,K) = \frac{1}{4}\kappa_1\left(d-1,h,\nu\varepsilon,\frac{\kappa}{2},\frac{2\alpha}{C_1},\frac{c'(K,\nu)}{2^d},K\right) \tag{62}$$

donde 2^d se debe a la suposición hecha en (41); a partir de (55) y (57) se tiene que $c_1(d,h,\varepsilon,\kappa,\alpha,c,K)$ es igual a

$$\frac{\kappa_1\left(d-1,h,\nu\varepsilon,\frac{\kappa}{2},\frac{2\alpha}{C_1},\frac{c'(K,\nu)}{2^d},K\right)c_1\left(d-1,h,\nu\varepsilon,\frac{\kappa}{2},\frac{2\alpha}{C_1},\frac{c'(K,\nu)}{2^d},K\right)}{2^{d+4}} \tag{63}$$

donde 2^d se debe a la suposición hecha en (41); y de (47) y (61) se tiene que $B(d,h,\varepsilon,\kappa,\alpha,c,K)$ es igual a

$$\frac{2^{12}dc_{5,K}B\left(d-1,h,\nu\varepsilon,\frac{\kappa}{2},\frac{2\alpha}{C_1},\frac{c'(K,\nu)}{2^d},K\right)}{\kappa\varepsilon\kappa_1\left(d-1,h,\nu\varepsilon,\frac{\kappa}{2},\frac{2\alpha}{C_1},\frac{c'(K,\nu)}{2^d},K\right)c_1\left(d-1,h,\nu\varepsilon,\frac{\kappa}{2},\frac{2\alpha}{C_1},\frac{c'(K,\nu)}{2^d},K\right)} \tag{64}$$

donde, por (47) y (29)

$$C_1 = C_1\left(\frac{\kappa}{4},\frac{1}{4},\frac{\varepsilon}{2d},K\right) = \frac{\kappa\varepsilon}{2^7c_{5,K}d}. \tag{65}$$

1.2. Conjuntos característicos. Habiendo demostrado la existencia de subconjuntos genéricos, ahora demostramos que existen "subconjuntos característicos pequeños". Para precisar la noción de subconjunto característico, primero definimos qué entendemos por un polinomio "pequeño".

Definición 4.8 (r-polinomio). Sea K un cuerpo global de grado d_K. Dado un parámetro N y un entero $d > 0$, por un r-polinomio nos referimos a un polinomio no nulo $f \in \mathcal{O}_K[X_1,\ldots,X_d]$ que cumple que para todo $\mathbf{x} \in [N]^d_{\mathcal{O}_K}$ se tiene que $H_K(f(\mathbf{x})) < N^{3rd_K}$.

Observamos que la razón del exponente $3rd_K$ en la definición es porque para cualquier $f \in \mathcal{O}_K[X_1,\ldots,X_d]$ con grado acotado por r y coeficientes de altura acotados por N^{rd_K} satisface que para N lo suficientemente grande, $H_K(f(\mathbf{x})) < N^{3rd_K}$ para todo $[N]^d_{\mathcal{O}_K}$.

Definición 4.9 (Subconjunto característico). Sea $0 < \delta \leq 1$ un número real y $r > 0$ un entero positivo. Se dice que $A \subseteq S$ es (r,δ)-característico para S si existe $A \subseteq L \subseteq S$ de tamaño $|L| \geq \delta|S|$ tal que para cualquier r-polinomio que se anula en A, también se anula L.

El resultado principal de esta sección es que existe una constante positiva $\delta > 0$ tal que para cualquier S como en el enunciado del Teorema 4.1, existe un subconjuntos (r,δ)-característico pequeño, siempre que N sea lo suficientemente grande.

PROPOSITION 4.10. *Sean $d, h \geq 0$ enteros arbitrarios y $\varepsilon > 0$ un número real positivo. Sean $Q = N^{\frac{\varepsilon}{2d}}$ y $P \subseteq \mathcal{P}(Q)$ tal que $w(P) \geq \kappa w(\mathcal{P}(Q))$ para algún $\kappa > 0$. Sea $r > 0$ un entero. Supongamos que $S \subseteq [N]^d_{\mathcal{O}_K}$ es un subconjunto de tamaño $|S| \geq cN^{d-h-1+\varepsilon}$ que ocupa a lo sumo $\alpha \mathcal{N}_K(\mathfrak{p})^{d-h}$ clases residuales módulo $\mathfrak{p}$ para todo $\mathfrak{p} \in P$ y algún $\alpha > 0$. Luego, si N es suficientemente grande, existe un conjunto $A \subseteq S$ de tamaño $|A| \leq c_2 r^{d-h}$ el cual es (r, δ)-característico para S, para cierto $\delta = \delta(d, h, \varepsilon, \kappa, \alpha, c, K)$ y $c_2 = c_2(d, h, \varepsilon, \kappa, \alpha, c, K)$.*

DEMOSTRACIÓN DE LA PROPOSICIÓN 4.10. Fijemos h y procedamos por inducción en d. Si $d < h$, tomando N suficientemente grande, existe $\mathfrak{p} \in P$ tal que $\alpha \mathcal{N}_K(\mathfrak{p})^{d-h} < 1$, luego S es vacío. Cuando $d = h$, el resultado se sigue del Lema 2.3. De hecho, en este caso cualquier subconjunto $S \subseteq [N]^d_{\mathcal{O}_K}$ que satisfaga la hipótesis de la Proposición 4.10 ocupa como mucho α clases residuales módulo $\mathfrak{p}$ para todo $\mathfrak{p} \in P$ y algún $\alpha > 0$. Luego, Lema 2.3 implica que $|S| \leq C_2 = C_2(\alpha, \kappa, \frac{\varepsilon}{2d}, K)$. Tomando $A = B = S$ tenemos que A es $(r, 1)$-característico para S. En particular, tenemos que

$$c_2(d, h, \varepsilon, \kappa, \alpha, c, K) = C_2, \tag{66}$$

$$\delta(d, h, \varepsilon, \kappa, \alpha, c, K) = 1. \tag{67}$$

Por lo tanto, supongamos que $d \geq h + 1$ y que el resultado es válido para dimensiones más pequeñas. Primero encontraremos subconjuntos genéricos dentro de las secciones de S para muchos primos $\mathfrak{p}$, como hicimos en el Lema 4.3. Similarmente a como se hizo en la Afirmación 4.4, pasamos a un conjunto $S_1 \subseteq S$ de tamaño $|S_1| \geq \frac{1}{8^d}|S|$ tal que

$$|\pi_1(A)| \geq Q \text{ para todo } A \subseteq S_1 \text{ con } |A| \geq \frac{|S_1|}{8}. \tag{68}$$

Podemos refinar aún más el conjunto S_1 para tener control en el tamaño de las secciones:

AFIRMACIÓN 4.11. *Existe un subconjunto $S_2 \subseteq S_1$ de tamaño $|S_2| \geq \frac{3}{4}|S_1|$, tal que*

$$|(S_2)_x| \leq \frac{|S|}{Q} \text{ para todo } x \in [N]_{\mathcal{O}_K}, \tag{69}$$

donde $(S_2)_x := \pi_1^{-1}(x) \cap S_2$.

DEMOSTRACIÓN DE LA AFIRMACIÓN 4.11. Sea $W := \left\{ s \in S_1 : \left|(S_1)_{\pi_1(s)}\right| > \frac{|S_1|}{Q} \right\}$. Notar que $|W| \leq \frac{1}{4}|S_1|$, de lo contrario $|W| > \frac{1}{4}|S_1| > \frac{1}{8}|S_1|$ y (68) implicaría $|\pi_1(W)| \geq Q$. Esto implicaría que

$$|S_1| = \left| \bigcup_{x \in \pi_1(S_1)} (S_1)_x \right| \geq \left| \bigcup_{x \in \pi_1(W)} (S_1)_x \right| > |\pi_1(W)| \frac{|S_1|}{Q} \geq |S_1|,$$

lo cual es una contradicción. Definamos $S_2 \coloneqq S_1 \backslash W$. Entonces $|S_2| \geq \frac{3}{4}|S_1|$ y para cualquier $x \in \pi_1(S_2)$, $(S_2)_x = (S_1)_x$, por lo tanto, para tal x se cumple

$$|(S_2)_x| = |(S_1)_x| \leq \frac{|S_1|}{Q} \leq \frac{|S|}{Q}.$$

□

Ahora, seguimos como en la demostración de la Afirmación 4.6 para obtener un subconjunto $S_3 \subseteq S_2$ de tamaño $|S_3| \geq \frac{1}{2}|S_2|$ tal que

$$|(S_3)_x| \geq c'(K,\nu) N^{d-h-2+\nu\varepsilon} \text{ para todo } x \in \pi_1(S_3) \tag{70}$$

donde $\nu = \frac{d-1}{d}$ y

$$c'(K,\nu) = \frac{3c}{2^{3d+4}c''(K)} \left(\frac{(1-\nu)\varepsilon}{d_K} \right)^{d_K}. \tag{71}$$

Sea B_1 una constante grande. Para cualquier primo $\mathfrak{p}$ denotamos $\mathcal{E}_1(\mathfrak{p})$ al conjunto de clases residuales $a \in \mathcal{O}_K/\mathfrak{p}$ tales que $|[S_3(a,\mathfrak{p})]_\mathfrak{p}| \geq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}$. Dado que $S_3 \subseteq S$ y $|[S]_\mathfrak{p}| \leq \alpha \mathcal{N}_K(\mathfrak{p})^{d-h}$, se sigue que $|\mathcal{E}_1(\mathfrak{p})| \leq \frac{\alpha}{B_1}\mathcal{N}_K(\mathfrak{p})$. Aplicando Lema 2.2 como en la demostración del Lema 4.3 concluimos que si B_1 es suficientemente grande, por ejemplo, si

$$B_1 \coloneqq \frac{\alpha}{C_1\left(\frac{\kappa}{4}, \frac{1}{4}, \frac{\varepsilon}{2d}, K\right)} = \frac{2^7 \alpha c_{5,K} d}{\kappa\varepsilon}, \tag{72}$$

luego el conjunto

$$X \coloneqq \left\{ x \in [N]_{\mathcal{O}_K} : \sum_{\mathfrak{p} \in P} 1_{x(\mathrm{mod}\ \mathfrak{p}) \in \mathcal{E}_1(\mathfrak{p})} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \geq \frac{1}{2} w(P) \right\},$$

posee tamaño $|X| < Q$. Luego, $|\pi_1^{-1}(X) \cap S_3| < \frac{1}{8}|S_1|$, ya que de lo contrario la desigualdad $|\pi_1^{-1}(X) \cap S_3| \geq \frac{1}{8}|S_1|$ y (68) implicaría $|\pi_1(\pi_1^{-1}(X) \cap S_3)| \geq Q$. Pero esto no puede suceder, ya que $|\pi_1(\pi_1^{-1}(X) \cap S_3)| \leq |X| < Q$. Como $|S_3| \geq \frac{1}{2}|S_2| \geq \frac{3}{8}|S_1|$, concluimos que $|S_3 \backslash \pi_1^{-1}(X)| \geq \frac{1}{4}|S_1|$.

Si tomamos $S_4 \coloneqq S_3 \backslash \pi_1^{-1}(X)$, sus secciones no vacías coinciden con las secciones no vacías de S_3, luego por (70), tenemos que

$$|(S_4)_x| = |(S_3)_x| \geq c'(K,\nu) N^{d-h-2+\nu\varepsilon} \text{ para todo } x \in \pi_1(S_4). \tag{73}$$

Más aún, para cada $x \in \pi_1(S_4)$ tenemos un subconjunto de primos

$$P_x \coloneqq \{\mathfrak{p} \in P : x(\mathrm{mod}\ \mathfrak{p}) \notin \mathcal{E}_1(\mathfrak{p})\}$$

el cual satisface $w(P_x) \geq \frac{1}{2}w(P) \geq \frac{1}{2}\kappa w(\mathcal{P}(Q))$, y $|[(S_4)_x]_\mathfrak{p}| \leq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}$, para todo $\mathfrak{p} \in P_x$. Por tanto, estamos en condiciones de aplicar la hipótesis inductiva a las secciones de S_4 con el parámetro $Q' \coloneqq N^{\frac{\nu\varepsilon}{2(d-1)}}$, el cual es igual a Q por nuestra elección de ν. Podemos deducir que para cada sección no vacía $(S_4)_x$ existe δ_0 y c_2,

independiente de x, tal que $(S_4)_x$ admite un subconjunto (r,δ_0)-característico $A(x)$ de tamaño $|A(x)| \leq c_2 r^{d-h-1}$. La dependencia de las constantes es la siguiente,

$$c_2 = c_2\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, c'(K,\nu), K\right), \tag{74}$$

$$\delta_0 = \delta\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, c'(K,\nu), K\right). \tag{75}$$

Dado que cada $A(x)$ es (r,δ_0)-característico para $(S_4)_x$, existe un subconjunto "testigo" $A(x) \subseteq S'_x \subseteq (S_4)_x$ de tamaño $|S'_x| \geq \delta_0|(S_4)_x|$ que satisface las condiciones de la Definición 4.9. Definimos

$$S' \coloneqq \bigcup_{x \in \pi_1(S_4)} S'_x. \tag{76}$$

(Observar que la notación S'_x es consistente con nuestro uso anterior de subíndices para denotar secciones, ya que para cada $x \in \pi_1(S_4)$ la sección de S' sobre x es igual al subconjunto testigo S'_x.). Resumamos las propiedades que satisface S':

$$|S'| \geq \delta_0|S_4| \geq \delta_0\frac{1}{4}|S_1| \geq \frac{\delta_0}{2^{3d+2}}|S|, \tag{77}$$

$$|S'_x| \geq \delta_0|(S_4)_x| \geq \delta_0 c'(K,\nu)N^{d-h-2+\nu\varepsilon}, \text{ para todo } x \in \pi_1(S'), \tag{78}$$

$$\text{para todo } x \in \pi_1(S'), A(x) \text{ is a } (r,1)\text{-characteristic subset for } S'_x \text{ of size } |A(x)| \leq c_2 r^{d-h-1}. \tag{79}$$

Aplicando Lema 4.3 a cada sección S'_x, podemos construir un subconjunto de primos $P'_x \subseteq P_x$ con $w(P'_x) \geq \kappa_1 w(P_x)$ tal que para todo $\mathfrak{p} \in P'_x$ existe un subconjunto $(B, d-h-1)$-genérico $\mathcal{G}_{\mathfrak{p}}(S'_x) \subseteq S'_x$, de tamaño $|\mathcal{G}_{\mathfrak{p}}(S'_x)| \geq c_1|S'_x|$, donde las constantes son independientes de $\mathfrak{p}$ y x. Específicamente,

$$B = B\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, \delta_0 c'(K,\nu), K\right), \tag{80}$$

$$\kappa_1 = \kappa_1\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, \delta_0 c'(K,\nu), K\right), \tag{81}$$

$$c_1 = c_1\left(d-1, h, \nu\varepsilon, \frac{\kappa}{2}, B_1, \delta_0 c'(K,\nu), K\right). \tag{82}$$

Procediendo como en la Afirmación 4.7, existe $\beta > 0$ y un subconjunto de primos $P' \subseteq P$ tal que

$$w(P') \geq \frac{\kappa_1}{4} w(P), \tag{83}$$

y para todo $\mathfrak{p} \in P'$ hay al menos $\beta|S'|$ elementos $s \in S'$ para los cuales $\mathfrak{p} \in P'_{\pi_1(s)}$. Luego, para $\mathfrak{p} \in P'$

$$\mathcal{G}_{\mathfrak{p}} \coloneqq \bigcup_{x : \mathfrak{p} \in P'_x}^{\cdot} \mathcal{G}_{\mathfrak{p}}(S'_x)$$

es un subconjunto de S de tamaño

$$|\mathcal{G}_{\mathfrak{p}}| \geq \beta c_1 |S'| \geq \beta c_1 \frac{\delta_0}{2^{3d+2}} |S|. \tag{84}$$

Por construcción, cada sección no vacía $(\mathcal{G}_{\mathfrak{p}})_x$ es igual a $\mathcal{G}_{\mathfrak{p}}(S'_x)$, que es $(B, d-h-1)$-genérico módulo $\mathfrak{p}$.

Para probar la Proposicińn 4.10, vamos a pegar algunos de los subconjuntos características que encontramos en cada sección de S'. Para obtener un subconjunto característico pequeño de S' mediante este procedimiento, necesitamos localizar secciones de S' que contengan la clase residual de muchos elementos de S' para muchos primos $\mathfrak{p}$. Este es el contenido del siguiente lema.

LEMA 4.12. *Existe un subconjunto $\mathcal{B} \subseteq S'$ con $|\mathcal{B}| \geq c_3|S'|$, tal que cada sección no vacía $\mathcal{B}_x$ de $\mathcal{B}$ es igual a S'_x y existe un subconjunto de primos $P''_x \subseteq P'$ con $w(P''_x) \geq \kappa_3 w(P')$, tal que para cada $\mathfrak{p} \in P''_x$*

$$|\{s \in S' : [s]_{\mathfrak{p}} \in [\mathcal{B}_x]_{\mathfrak{p}}\}| \geq c_4 \frac{|S'|}{\mathcal{N}_K(\mathfrak{p})}.$$

DEMOSTRACIÓN DEL LEMA 4.12. Empezamos fijando un primo $\mathfrak{p} \in P'$ y considerando una clase residual $a \in [\pi_1(\mathcal{G}_{\mathfrak{p}})]_{\mathfrak{p}} \subseteq \mathcal{O}_K/\mathfrak{p}$. Dado que $\mathfrak{p}$ está fijo, vamos a denotar por $\mathcal{G}_{\mathfrak{p}}(a)$ a aquellos elementos en $\mathcal{G}_{\mathfrak{p}}$ con primera coordenada congruente a a módulo $\mathfrak{p}$. Más aún, dada una clase $\mathbf{b} \in (\mathcal{O}_K/\mathfrak{p})^d$ notamos $\mathcal{G}_{\mathfrak{p}}(\mathbf{b})$ a aquellos elementos de $\mathcal{G}_{\mathfrak{p}}$ congruentes a $\mathbf{b}$ módulo $\mathfrak{p}$. Por el principio del palomar, y el hecho de que por la construcción de P' y $\mathcal{G}_{\mathfrak{p}}$, se tiene que $|[\mathcal{G}_{\mathfrak{p}}(a)]_{\mathfrak{p}}| \leq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}$ se sigue que podemos hallar $\mathbf{b}_1 \in [\mathcal{G}_{\mathfrak{p}}(a)]_{\mathfrak{p}} \subseteq (\mathcal{O}_K/\mathfrak{p})^d$ con

$$|\mathcal{G}_{\mathfrak{p}}(\mathbf{b}_1)| \geq \frac{|\mathcal{G}_{\mathfrak{p}}(a)|}{B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}}.$$

Consideremos ahora $\mathcal{B}_1 \subseteq \mathcal{G}_{\mathfrak{p}}(a)$ definido por

$$\mathcal{B}_1 := \bigcup_{s:[s]_{\mathfrak{p}}=\mathbf{b}_1} (\mathcal{G}_{\mathfrak{p}})_{\pi_1(s)}, \tag{85}$$

es decir, $\mathcal{B}_1$ es la unión de aquellas secciones de $\mathcal{G}_{\mathfrak{p}}$ que contienen un representante de $\mathbf{b}_1$.

Dado que cada $(\mathcal{G}_{\mathfrak{p}})_x$ es $(B, d-h-1)$-genérico módulo $\mathfrak{p}$, tenemos que

$$|(\mathcal{G}_{\mathfrak{p}})_x| \geq \frac{\mathcal{N}_K(\mathfrak{p})^{d-h-1}}{B} |(\mathcal{G}_{\mathfrak{p}})_x(\mathbf{b}_1)|,$$

luego

$$|\mathcal{B}_1| \geq \frac{\mathcal{N}_K(\mathfrak{p})^{d-h-1}}{B} |\mathcal{G}_{\mathfrak{p}}(\mathbf{b}_1)| \geq \frac{1}{B_1 B} |\mathcal{G}_{\mathfrak{p}}(a)|. \tag{86}$$

Notar que como $|\mathcal{G}_{\mathfrak{p}}(a)| \geq |\mathcal{B}_1|$ y $|[\mathcal{G}_{\mathfrak{p}}(a)]_{\mathfrak{p}}| \leq B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}$, por la primera inecuación de (86) y el principio del palomar podemos encontrar otra clase residual $\mathbf{b}_2 \in [\mathcal{G}_{\mathfrak{p}}(a)]_{\mathfrak{p}}$ con

$$\begin{aligned} |\mathcal{G}_{\mathfrak{p}}(\mathbf{b}_2)| &\geq \frac{1}{B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}} |\mathcal{G}_{\mathfrak{p}}(a) \backslash \mathcal{G}_{\mathfrak{p}}(\mathbf{b}_1)| \\ &\geq \frac{1}{B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}} \left(1 - \frac{B}{\mathcal{N}_K(\mathfrak{p})^{d-h-1}}\right) |\mathcal{G}_{\mathfrak{p}}(a)|, \end{aligned}$$

que es al menos $\frac{|\mathcal{G}_{\mathfrak{p}}(a)|}{2B_1 \mathcal{N}_K(\mathfrak{p})^{d-h-1}}$ si $\mathcal{N}_K(\mathfrak{p})^{d-h-1} > 2B$. En tal caso, si definimos $\mathcal{B}_2$ como en (85), el mismo razonamiento por el que llegamos a (86) implica que $|\mathcal{B}_2| \geq \frac{1}{2B_1 B} |\mathcal{G}_{\mathfrak{p}}(a)|$. Iterando este proceso obtenemos una sucesión $\mathbf{b} := \{\mathbf{b}_1, \dots, \mathbf{b}_q\}$ de clases residuales, con $q = \left\lceil \frac{\mathcal{N}_K(\mathfrak{p})^{d-h-1}}{2B} \right\rceil$, la cual satisface

$$\begin{aligned} |\mathcal{G}_p(\mathbf{b}_j)| &\geq \frac{1}{B_1 \mathcal{N}(p)^{d-h-1}} \left| \mathcal{G}_p(a) \backslash \bigcup_{i=1}^{j-1} \mathcal{G}_p(\mathbf{b}_i) \right| \\ &\geq \frac{1}{B_1 \mathcal{N}(p)^{d-h-1}} \left(1 - \frac{(q-1)B}{\mathcal{N}(p)^{d-h-1}}\right) |\mathcal{G}_p(a)|, \end{aligned}$$

y $|\mathcal{B}_j| \geq \frac{1}{2B_1 B} |\mathcal{G}_{\mathfrak{p}}(a)|$. En particular,

$$\sum_{j=1}^{q} |\mathcal{B}_j| \geq \frac{q}{2B_1 B} |\mathcal{G}_{\mathfrak{p}}(a)|. \tag{87}$$

Ahora, consideremos el conjunto

$$\mathcal{B}[a] := \left\{ s \in \mathcal{G}_{\mathfrak{p}}(a) : \sum_{j=1}^{q} 1_{s \in \mathcal{B}_j} \geq \frac{q}{4B_1 B} \right\}.$$

Observar que $\mathcal{B}[a]_x = \mathcal{B}[a] \cap \pi_1^{-1}(x)$ es igual a $(\mathcal{G}_{\mathfrak{p}})_x$ siempre y cuando esta intersección sea no vacía. Además, (87) implica

$$\begin{aligned} \frac{q}{2B_1 B} |\mathcal{G}_p(a)| &\leq \sum_{j=1}^{q} |\mathcal{B}_j| = \sum_{j=1}^{q} \sum_{s} 1_{s \in \mathcal{B}_j} \\ &= \sum_{s \in \mathcal{B}[a]} \sum_{j=1}^{q} 1_{s \in \mathcal{B}_j} + \sum_{s \notin \mathcal{B}[a]} \sum_{j=1}^{q} 1_{s \in \mathcal{B}_j} \\ &\leq \sum_{s \in \mathcal{B}[a]} q + \sum_{s \notin \mathcal{B}[a]} \frac{q}{4B_1 B} \\ &\leq q \left(|\mathcal{B}[a]| + \frac{1}{4B_1 B} |\mathcal{G}_p(a)| \right), \end{aligned} \tag{88}$$

de lo que deducimos

$$|\mathcal{B}[a]| \geq \frac{1}{4B_1 B} |\mathcal{G}_{\mathfrak{p}}(a)|. \tag{89}$$

Afirmación 4.13. *Para cada x tal que $\mathcal{B}[a]_x \neq \varnothing$, existen al menos $\frac{|\mathcal{G}_\mathfrak{p}(a)|}{(4B_1B)^2}$ elementos $s \in \mathcal{G}_\mathfrak{p}(a)$ tales que $s \equiv \mathbf{y} (mod\ \mathfrak{p})$ para algún $\mathbf{y} \in \mathcal{B}[a]_x$.*

Demostración de la Afirmación 4.13. Sea x tal que $\mathcal{B}[a]_x \neq \varnothing$. Entonces, $\mathcal{B}[a]_x = (\mathcal{G}_\mathfrak{p})_x$ y por definición de $\mathcal{B}[a]$, se tiene que $(\mathcal{G}_\mathfrak{p})_x \subseteq \mathcal{B}_j$ para al menos $\frac{q}{4B_1B}$ valores de j. Ahora, fijemos cualquier j. Luego, por definición de $\mathcal{B}_j$, existen $s_j \in \mathcal{G}_\mathfrak{p}(a)$ tal que $(\mathcal{G}_\mathfrak{p})_x = (\mathcal{G}_\mathfrak{p})_{\pi_1(s_j)}$ y $s_j \equiv \mathbf{b}_j (\mathrm{mod}\ \mathfrak{p})$. Notar que $s_j \in (\mathcal{G}_\mathfrak{p})_x$. Luego, para cualquier $s \in \mathcal{G}_\mathfrak{p}(\mathbf{b}_j)$, se tiene que $s \equiv \mathbf{b}_j \equiv s_j (\mathrm{mod}\ \mathfrak{p})$. Deducimos que hay $|\mathcal{G}_\mathfrak{p}(\mathbf{b}_j)| \geq \frac{|\mathcal{G}_\mathfrak{p}(a)|}{2B_1\mathcal{N}_K(\mathfrak{p})^{d-h-1}}$ elementos $s \in \mathcal{G}_\mathfrak{p}(a)$ tales que $s \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ para algún $\mathbf{y} \in \mathcal{G}_\mathfrak{p}(a)$. Ahora, los elementos construidos poseen clase residual igual a $\mathbf{b}_j$ módulo $\mathfrak{p}$. Dado que las clases residuales $\mathbf{b}_j$ son todas diferentes, concluimos que hay al menos $\frac{q}{4B_1B} \frac{|\mathcal{G}_\mathfrak{p}(a)|}{2B_1\mathcal{N}_K(\mathfrak{p})^{d-h-1}} \geq \frac{|\mathcal{G}_\mathfrak{p}(a)|}{(4B_1B)^2}$ elementos $s \in \mathcal{G}_\mathfrak{p}(a)$ tales que $s \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ para algún $\mathbf{y} \in \mathcal{B}[a]_x$. □

Ahora, sea

$$\mathcal{R} := \left\{ a \in [\pi_1(S')]_\mathfrak{p} \subseteq \mathcal{O}_K/\mathfrak{p} : |\mathcal{G}_\mathfrak{p}(a)| \geq \frac{1}{2\mathcal{N}_K(\mathfrak{p})} |\mathcal{G}_\mathfrak{p}| \right\} \tag{90}$$

y notemos

$$\mathcal{B}[\mathfrak{p}] := \left\{ s \in S' : (S')_{\pi_1(s)} \cap \mathcal{B}[a] \neq \varnothing \text{ para algún } a \in \mathcal{R} \right\}.$$

En otras palabras, $\mathcal{B}[\mathfrak{p}]$ consiste de aquellas secciones de S' con inteserción no trivial con $\bigcup_{a\in\mathcal{R}} \mathcal{B}[a]$. En particular, como $\mathcal{B}[\mathfrak{p}]$ contiene la unión disjunta $\bigcup_{a\in\mathcal{R}} \mathcal{B}[a]$, de la definición de $\mathcal{R}$ deducimos:

Afirmación 4.14. *Se cumple la siguiente cota*

$$|\mathcal{B}[\mathfrak{p}]| \geq \frac{\beta c_1}{8B_1B} |S'|.$$

Demostración de la Afirmación 4.14. Primero notemos que por el principio del palomar, $\mathcal{R} \neq \varnothing$. Ahora, si $\mathcal{R} = \{a_1, \ldots, a_h\}$,

$$|\mathcal{G}_\mathfrak{p}| = \sum_a |\mathcal{G}_\mathfrak{p}(a)| = \sum_{a\in\mathcal{R}} |\mathcal{G}_\mathfrak{p}(a)| + \sum_{a\notin\mathcal{R}} |\mathcal{G}_\mathfrak{p}(a)| < \sum_{a\in\mathcal{R}} |\mathcal{G}_\mathfrak{p}(a)| + \frac{\mathcal{N}_K(\mathfrak{p}) - h}{2\mathcal{N}_K(\mathfrak{p})} |\mathcal{G}_\mathfrak{p}|,$$

entonces

$$\sum_{a\in\mathcal{R}} |\mathcal{G}_\mathfrak{p}(a)| > \left(1 - \frac{\mathcal{N}_K(\mathfrak{p}) - h}{2\mathcal{N}_K(\mathfrak{p})}\right) |\mathcal{G}_\mathfrak{p}| = \frac{\mathcal{N}_K(\mathfrak{p}) + h}{2\mathcal{N}_K(\mathfrak{p})} |\mathcal{G}_\mathfrak{p}| > \frac{|\mathcal{G}_\mathfrak{p}|}{2}.$$

Combinando esto con (84) y (89) obtenemos que

$$|\mathcal{B}[\mathfrak{p}]| \geq \left| \bigcup_{a\in\mathcal{R}} \mathcal{B}[a] \right| = \sum_{a\in\mathcal{R}} |\mathcal{B}[a]| \geq \sum_{a\in\mathcal{R}} \frac{1}{4B_1B} |\mathcal{G}_\mathfrak{p}(a)| > \frac{1}{8B_1B} |\mathcal{G}_\mathfrak{p}| > \frac{\beta c_1}{8B_1B} |S'|.$$

□

Para un elemento $s \in S'$ notamos P''_s al conjunto de primos $\mathfrak{p} \in P'$ para los cuales $s \in \mathcal{B}[\mathfrak{p}]$.

Afirmación 4.15. *Existen constantes κ_3 y c_3 tales que el conjunto*

$$\mathcal{B} := \{s \in S' : w(P''_s) \geq \kappa_3 w(P')\}$$

satisface $|\mathcal{B}| \geq c_3|S'|$.

Demostración de la Afirmación 4.15. Por un lado, tenemos que

$$\sum_{\mathfrak{p}\in P'} \sum_{s\in S'} 1_{s\in\mathcal{B}[\mathfrak{p}]} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} = \sum_{\mathfrak{p}\in P'} |\mathcal{B}[\mathfrak{p}]| \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \geq \frac{\beta c_1}{8B_1B}|S'|w(P').$$

Por otro lado,

$$\begin{aligned}
\sum_{s\in S'} \sum_{\mathfrak{p}\in P'} 1_{s\in\mathcal{B}[\mathfrak{p}]} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} &= \sum_{s\in S'} \sum_{\mathfrak{p}\in P''_s} \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \\
&= \sum_{s\in S'} w(P''_s) \\
&= \sum_{s\in\mathcal{B}} w(P''_s) + \sum_{s\notin\mathcal{B}} w(P''_s) \\
&\leq |\mathcal{B}|w(P') + \kappa_3|S'|w(P'),
\end{aligned}$$

puesto que $P''_s \subseteq P'$. Luego $\left(\frac{\beta c_1}{8B_1B} - \kappa_3\right)|S'| \leq |\mathcal{B}|$. Entonces, es suficiente con tomar

$$\kappa_3 = c_3 := \frac{\beta c_1}{16B_1B}. \tag{91}$$

□

Ahora, comprobemos que $\mathcal{B}$ satisface la condición del Lema 4.12. Sea x tal que $\mathcal{B}_x \neq \varnothing$. Observar que si $s_1, s_2 \in \pi_1^{-1}(x)$, entonces $P''_{s_1} = P''_{s_2}$. Se sigue que $P''_x := P''_s$ con $s \in \pi_1^{-1}(x)$ está bien definido. De esto concluimos que cada sección $\mathcal{B}_x$ no vacía de $\mathcal{B}$ es igual a S'_x. Sea $\mathfrak{p} \in P''_x$, por construcción, $\mathcal{B}[a]_x \subseteq \mathcal{B}_x$ para algún $a \in \mathcal{R}$, donde $\mathcal{R}$ fue definido en (90). Puesto que hay al menos $\frac{|\mathcal{G}_{\mathfrak{p}}(a)|}{(4B_1B)^2}$ elementos $s \in \mathcal{G}_{\mathfrak{p}}(a)$ tales que

$s \equiv \mathbf{y} (\mathrm{mod}\ \mathfrak{p})$ para algún $\mathbf{y} \in \mathcal{B}[a]_x$, concluimos que

$$\begin{aligned} |\{s \in S' : [s]_{\mathfrak{p}} \in [\mathcal{B}_x]_{\mathfrak{p}}\}| &\geq \frac{|\mathcal{G}_{\mathfrak{p}}(a)|}{(4B_1B)^2} \\ &\geq \frac{1}{2^5(B_1B)^2} \frac{1}{\mathcal{N}_K(\mathfrak{p})} |\mathcal{G}_{\mathfrak{p}}| \\ &\geq \frac{\beta c_1}{2^5(B_1B)^2} \frac{|S'|}{\mathcal{N}_K(\mathfrak{p})} \\ &= c_4 \frac{|S'|}{\mathcal{N}_K(\mathfrak{p})}, \end{aligned}$$

donde la segunda inecuación es verdadera ya que $a \in \mathcal{R}$, la tercera inecuación se debe a (84), y

$$c_4 := \frac{\beta c_1}{2^5(B_1B)^2}. \tag{92}$$

Esto termina la demostración del Lema 4.12. □

Para concluir la prueba de la Proposiciń 4.10 vamos a demostrar que si un r-polinomio se anula en las secciones $\mathcal{B}_x$ para $\gtrsim_{r,d,h,\varepsilon,\kappa,K} 1$ valores de x, entonces debería anularse en una proporción positiva de S. Para ello, primero encontraremos $m = O_{r,d,h,\varepsilon,\kappa,K}(1)$ lo suficientemente grande y $S'_{x_1}, \ldots, S'_{x_m}$, m secciones diferentes de S' que tienen intersección no trivial con $\mathcal{B}$, y tales que para muchos $s \in S'$ hay muchos primos $\mathfrak{p} \in \mathcal{P}(Q)$ para los cuales existe $s_j \in S'_{x_j}$ para algún $1 \leq j \leq m$ tal que $s_j \equiv s (\mathrm{mod}\ \mathfrak{p})$.

Recordar que cualquier sección no vacía $\mathcal{B}_x$ de $\mathcal{B}$ es igual a S'_x. Puesto que $S' \subseteq S_4 \subseteq S_3 \subseteq S_2$, se sigue de (69) que $|\mathcal{B}_x| = |S'_x| \leq \frac{|S|}{Q}$, para todo $x \in \pi_1(\mathcal{B})$. Por otro lado, por Lema 4.12 y la inecuación (77), tenemos que $|\mathcal{B}| \geq c_3 \frac{\delta_0}{2^{3d+2}} |S|$. Se sigue que existen al menos $\frac{c_3\delta_0}{2^{3d+2}} Q$ secciones no vacías de $\mathcal{B}$.

Notemos por $\mathcal{L} := \{S'_{x_1}, \ldots, S'_{x_m}\}$ una elección de m secciones de S' tales que $S'_{x_i} \cap \mathcal{B} \neq \varnothing$ para todo i. Sea $P_{\mathcal{L}}$ un conjunto de primos $\mathfrak{p}$ en $\mathcal{P}(Q)$ para los cuales existe un par de secciones $S'_{x_i} \neq S'_{x_j}$ en $\mathcal{L}$ tales que $[S'_{x_i}]_{\mathfrak{p}} \cap [S'_{x_j}]_{\mathfrak{p}} \neq \varnothing$. Dado un tal par de secciones, el hecho de que $[S'_{x_i}]_{\mathfrak{p}} \cap [S'_{x_j}]_{\mathfrak{p}} \neq \varnothing$ implica $x_i \equiv x_j (\mathrm{mod}\ \mathfrak{p})$. Dado que $x_i \neq x_j$ y que ambos

están en $[N]_{\mathcal{O}_K}$, por (3) y (7), se sigue que $\mathcal{N}_K(x_i - x_j) \leq N^3$ cuando $N \geq 2^{d_K}$. Luego

$$\begin{aligned}\sum_{\mathfrak{p}\in P_{\mathcal{L}}} \log(\mathcal{N}_K(\mathfrak{p})) &\leq \sum_{\{i,j\},i\neq j} \sum_{\mathfrak{p}|x_i-x_j} \log(\mathcal{N}_K(\mathfrak{p})) \\ &\leq \sum_{\{i,j\},i\neq j} \log(\mathcal{N}_K(x_i - x_j)) \\ &\leq \binom{m}{2} 3\log(N).\end{aligned}$$

Mediante una aplicación estándar de sumación por partes, esto implica que

$$w(P_{\mathcal{L}}) \lesssim_{r,d,h,\varepsilon,\kappa,K} \log(\log(N)). \tag{93}$$

Ahora, consideramos en S' la función

$$\Psi_{\mathcal{L}}(s) := \sum_{\mathfrak{p}\in\mathcal{P}(Q)} 1_{\exists \mathbf{x}\in\mathcal{L}: s\equiv\mathbf{x} (\mathrm{mod}\ \mathfrak{p})} \log(\mathcal{N}_K(\mathfrak{p})).$$

Notar que $\Psi_{\mathcal{L}}(s)$ mide cuánto contiene, una clase de residuo ocupada por s, un representante en $\mathcal{L}$. Teniendo en cuenta que las secciones no vacías de $\mathcal{B}$ son secciones no vacías de S', del Lema 4.12 deducimos que

$$\begin{aligned}\sum_{s\in S'} \Psi_{\mathcal{L}}(s) &\geq \sum_{i=1}^{m} \sum_{\mathfrak{p}\in P_{x_i}\setminus P_{\mathcal{L}}} \sum_{s\in S'} 1_{\exists \mathbf{x}\in S'_{x_i}: s\equiv\mathbf{x} (\mathrm{mod}\ \mathfrak{p})} \log(\mathcal{N}_K(\mathfrak{p})) \\ &\geq \sum_{i=1}^{m} \sum_{\mathfrak{p}\in P_{x_i}\setminus P_{\mathcal{L}}} c_4|S'| \frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})} \\ &= c_4|S'| \sum_{i=1}^{m} \left(w(P_{x_i}) - w(P_{\mathcal{L}})\right),\end{aligned}$$

donde la primera desigualdad es porque para cualquier primo $\mathfrak{p} \in \bigcup_i P_{x_i}\setminus P_{\mathcal{L}}$ tenemos $[S'_{x_i}]_{\mathfrak{p}} \cap [S'_{x_j}]_{\mathfrak{p}} = \varnothing$ para cualquier $i \neq j$, así las condiciones $\exists \mathbf{x} \in S'_{x_i} : s \equiv \mathbf{x} (\mathrm{mod}\ \mathfrak{p})$ son disjuntas dos a dos. Puesto que $w(P_{x_i}) \geq \kappa_3 w(P') \geq \frac{\kappa_3\kappa_1}{4} w(P) \geq \frac{\kappa_3\kappa_1\kappa}{4} w(\mathcal{P}(Q))$, la inecuación (93) implica que

$$\begin{aligned}\sum_{s\in S'} \Psi_{\mathcal{L}}(s) &\geq mc_4|S'| \left(\frac{\kappa_3\kappa_1\kappa}{4} w(\mathcal{P}(Q)) + O_{r,d,h,\varepsilon,\kappa,K}(\log(\log(N))) \right) \qquad (94) \\ &\geq \frac{1}{2} mc_4|S'| \frac{\kappa_3\kappa_1\kappa}{4} w(\mathcal{P}(Q)) \\ &\geq mc_4 \frac{\delta_0}{2^{3d+2}} |S| \frac{\kappa_3\kappa_1\kappa}{8} w(\mathcal{P}(Q)) \\ &\geq c_5 m|S| \log(N),\end{aligned}$$

para N suficientemente grande. Aquí,

$$c_5 = \frac{\kappa}{2^{3d+6}} c_{2,K} \frac{\varepsilon}{d} c_4\kappa_1\kappa_3\delta_0. \tag{95}$$

Ahora acotaremos $\sum_{s\in S'}\Psi_{\mathcal{L}}(s)$ inferiormente. Para esto, primero notar que para s en $\mathcal{L}$, (69) implica que

$$\begin{aligned}\sum_{s\in\mathcal{L}}\Psi_{\mathcal{L}}(s) &= \sum_{s\in\mathcal{L}}\sum_{\mathfrak{p}\in\mathcal{P}(Q)} 1_{\exists \mathbf{x}\in\mathcal{L}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}\log(\mathcal{N}_K(\mathfrak{p})) \\ &= \sum_{s\in\mathcal{L}}\sum_{\mathfrak{p}\in\mathcal{P}(Q)}\log(\mathcal{N}_K(\mathfrak{p})) \\ &\leq c_{4,K}Q|\mathcal{L}| \\ &\leq c_{4,K}m|S|.\end{aligned} \tag{96}$$

Notar también que si $s\notin\mathcal{L}$, entonces

$$\begin{aligned}\Psi_{\mathcal{L}}(s) &= \sum_{\mathfrak{p}\in\mathcal{P}(Q)} 1_{\exists \mathbf{x}\in\mathcal{L}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}\log(\mathcal{N}_K(\mathfrak{p})) \\ &\leq \sum_{\mathfrak{p}\in\mathcal{P}(Q)}\sum_{i=1}^{m} 1_{\exists \mathbf{x}\in S'_{x_i}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}\log(\mathcal{N}_K(\mathfrak{p})) \\ &= \sum_{i=1}^{m}\sum_{\mathfrak{p}\in\mathcal{P}(Q)} 1_{\exists \mathbf{x}\in S'_{x_i}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}\log(\mathcal{N}_K(\mathfrak{p})) \\ &\leq \sum_{i=1}^{m}\sum_{\mathfrak{p}|\pi_1(s)-x_i}\log(\mathcal{N}_K(\mathfrak{p})) \\ &\leq \sum_{i=1}^{m}\log(\mathcal{N}_K(\pi_1(s)-x_i)).\end{aligned} \tag{97}$$

Por (3), (7) y el hecho de que $\pi_1(s), x_i \in [N]_{\mathcal{O}_K}$, tenemos que $\mathcal{N}_K(\pi_1(s)-x_i)\leq N^3$ cuando $N\geq 2^{d_K}$, por lo tanto de (97) deducimos que para $s\notin\mathcal{L}$ se tiene que

$$\Psi_{\mathcal{L}}(s)\leq 3m\log(N). \tag{98}$$

Sea $\delta_1 := \dfrac{c_5}{4}$, y supongamos que el conjunto

$$L := \{s\in S' : \Psi_{\mathcal{L}}(s)\geq\gamma\}$$

posee tamaño como mucho $\delta_1|S|$. Entonces

$$\begin{aligned}\sum_{s\in S'}\Psi_{\mathcal{L}}(s) &= \sum_{\substack{s\in S'\\ \Psi_{\mathcal{L}}(s)<\gamma}}\Psi_{\mathcal{L}}(s) + \sum_{\substack{s\in\mathcal{L}\\ \Psi_{\mathcal{L}}(s)\geq\gamma}}\Psi_{\mathcal{L}}(s) + \sum_{\substack{s\notin\mathcal{L}\\ \Psi_{\mathcal{L}}(s)\geq\gamma}}\Psi_{\mathcal{L}}(s) \\ &\leq \sum_{\substack{s\in S'\\ \Psi_{\mathcal{L}}(s)<\gamma}}\Psi_{\mathcal{L}}(s) + \sum_{s\in\mathcal{L}}\Psi_{\mathcal{L}}(s) + \sum_{\substack{s\in S'\\ \gamma\leq\Psi_{\mathcal{L}}(s)\leq 3m\log(N)}}\Psi_{\mathcal{L}}(s) \\ &< \gamma|S| + c_{4,K}m|S| + \delta_1|S|3m\log(N).\end{aligned} \tag{99}$$

Si ahora fijamos $\gamma := 3rd_K\log(N)$, combinando (94) con (99) tenemos que

$$4\delta_1 m\log(N) < 3rd_K\log(N) + c_{4,K}m + 3\delta_1 m\log(N),$$

y entonces

$$m\left(\delta_1 - \frac{c_{4,K}}{\log N}\right) < 3rd_K.$$

Luego, si tomamos $m := \dfrac{4rd_K}{\delta_1}$ tenemos una contradicción cuando $N > \exp\left(\dfrac{4c_{4,K}}{\delta_1}\right)$. Concluimos que para N suficientemente grande, el conjunto

$$L := \{s \in S' : \Psi_{\mathcal{L}}(s) \geq 3rd_K \log(N)\}$$

posee tamaño $|L| \geq \delta_1 |S|$ para nuestra elección de m y δ_1. Dado que

$$\Psi_{\mathcal{L}}(s) = \log\left(\prod_{\substack{\mathfrak{p}\in\mathcal{P}(Q)\\ \exists \mathbf{x}\in\mathcal{L}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}} \mathcal{N}_K(\mathfrak{p})\right),$$

se sigue que si $s \in L$ entonces

$$\prod_{\substack{\mathfrak{p}\in\mathcal{P}(Q)\\ \exists \mathbf{x}\in\mathcal{L}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}} \mathcal{N}_K(\mathfrak{p}) \geq N^{3rd_K}.$$

Ahora, veamos que si un r-polinomio se anula en $\mathcal{L}$, entonces se debe anular en L. En efecto, sea f un tal polinomio y sea $s \in L$. Si $\mathfrak{p} \in \mathcal{P}(Q)$ es un primo para el cual existe $\mathbf{x} \in \mathcal{L}$ con $s \equiv \mathbf{x}(\mathrm{mod}\ \mathfrak{p})$, el hecho de que $f(\mathbf{x}) = 0$ implica que $\mathfrak{p} | f(s)$. Por definición 4.8, $H_K(f(\mathbf{y})) < N^{3rd_K}$ para todo $\mathbf{y} \in [N]^d_{\mathcal{O}_K}$. Por lo tanto, si $f(s) \neq 0$ se tiene que

$$N^{3rd_K} \leq \prod_{\substack{\mathfrak{p}\in\mathcal{P}(Q)\\ \exists \mathbf{x}\in\mathcal{L}: s\equiv\mathbf{x}(\mathrm{mod}\ \mathfrak{p})}} \mathcal{N}(\mathfrak{p}) \leq \prod_{\mathfrak{p}|f(s)} \mathcal{N}_K(\mathfrak{p}) \leq \mathcal{N}_K(f(s)) \leq H_K(f(s)) < N^{3rd_K},$$

lo cual es absurdo. Luego $f(s) = 0$.

Por la construcción de S' dada en (76) y por (79), sabemos que cada sección $S'_{x_i} \in \mathcal{L}$ contiene un conjunto $(r,1)$-característico $A(x_i)$, de tamaño a lo sumo $c_2 r^{d-h-1}$. Tomando A como la union de estos m subconjuntos obtenemos un conjunto (r,δ_1)-característico para S, de tamaño a lo sumo $\frac{m}{r} c_2 r^{d-h} = \frac{4d_K}{\delta_1} c_2 r^{d-h}$. □

2. Construcción de un polinomio de baja complejidad y conclusión de la prueba

Habiendo construido un subconjunto característico $A \subseteq S$, el último paso para demostrar el Teorema 4.1 es construir un polinomio pequeño que se anule sobre A. Esto se hará utilizando la siguiente variante del lema de Siegel.

LEMA 4.16 (Lema 3.6 en [**Par21**]). *Sea K un cuerpo global de grado d_K. Sean $(a_{ij})_{i,j}$, $1 \leq i \leq s$, $1 \leq j \leq t$ elementos de $\mathcal{O}_K$ con $H(a_{ij}) \leq C$ para todo i, j. Supongamos*

que $t > 2d_K^2 s$. *Entonces, existe* $\mathbf{c} = (c_1, \ldots, c_t) \in \mathcal{O}_K^t \backslash \{0\}$, *tal que*

$$H_K(1 : \mathbf{c}) \leq c_{6,K} \, (tC)^{\frac{8d_K^2 s}{t - 2d_K s}}$$

y

$$\sum_{j=1}^{t} c_j a_{ij} = 0 \text{ para todo } 1 \leq i \leq s.$$

Demostración del Teorema 4.1. La prueba es como la del Teorema 2.4 en [**Wal12**], reemplazando el lema clásico de Siegel y la Proposición 2.2 en [**Wal12**] por el Lema 4.16 y la Proposición 4.10. Primero, basta con demostrar el Teorema 4.1 para $\eta = 1 - \delta$; el caso general sigue por un simple argumento de partición. Así, tenemos $S \subseteq [N]_{\mathcal{O}_K}^d$ de tamaño $|S| \geq cN^{d-h-1+\varepsilon}$ ocupando a lo sumo $\alpha \mathcal{N}_K(\mathfrak{p})^{d-h}$ clases residuales módulo $\mathfrak{p}$ para todo primo $\mathfrak{p} \in P$. Por la Proposición 4.10 existe un subconjunto $A \subseteq S$ de tamaño $|A| \leq c_2 r^{d-h}$ el cual es (r, δ)-característico para S, si N es suficientemente grande. Recordar que el número de monomios en d variables de grado r es igual a $\binom{r+d-1}{d-1}$. Consideremos el sistema de $|A|$-ecuaciones lineales en $\binom{r+d-1}{d-1}$ variables dado por

$$\sum_{\mathbf{i}=(i_1,\ldots,i_d)} \beta_{\mathbf{i}} \mathbf{a}^{\mathbf{i}} = 0 \text{ para todo } \mathbf{a} \in A,$$

donde estamos usando la notación multi-índice $\mathbf{a}^{\mathbf{i}} = a_1^{i_1} \ldots a_d^{i_d}$ para $\mathbf{a} = (a_1, \ldots, a_d)$ y estamos sumando sobre los $\mathbf{i}$'s con $i_1 + \ldots + i_d = r$. Notar que $H_K(\mathbf{a}^{\mathbf{i}}) \leq N^r$. Ahora, eligiendo r suficientemente grande tal que

$$\binom{r + d - 1}{d - 1} > 18 d_K^2 |A|, \tag{100}$$

es decir, como $\binom{r+d-1}{d-1} \geq \frac{r^{d-1}}{(d-1)!}$ y $|A| \leq c_2 r^{d-h}$ es suficiente con elegir

$$\frac{r^{d-1}}{(d-1)!} > 18 d_K^2 c_2 r^{d-h}, \text{ i.e. } r > \left(18 d_K^2 c_2 (d-1)!\right)^{\frac{1}{h-1}}. \tag{101}$$

Observación. En esta etapa es el único lugar en el que requerimos que $h > 1$.

Notar que (100) implica

$$\frac{16 d_K |A|}{\binom{r+d-1}{d-1} - 2 d_K |A|} < 1. \tag{102}$$

Por Lema 4.16 y (102) existe una solución $(\beta_{\mathbf{i}}) \in \mathcal{O}_K^{\binom{r+d-1}{d-1}} \backslash \{0\}$ que cumple

$$H_K(1 : (\beta_{\mathbf{i}})) \leq c_{6,K} \left[\binom{r + d - 1}{d - 1} N^r \right]^{\frac{8d_K^2 |A|}{\binom{r+d-1}{d-1} - 2 d_K |A|}} \leq c_{6,K} \binom{r + d - 1}{d - 1}^{\frac{d_K}{2}} N^{\frac{r d_K}{2}} \leq N^{r d_K}$$

tomando N suficientemente grande de forma que $\binom{r+d-1}{d-1} \leq N^r$. Consideremos ahora el polinomio homogéneo no nulo $f = \sum_{\mathbf{i}} \beta_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ de grado r. Para cualquier $\mathbf{x} \in [N]^d_{\mathcal{O}_K}$ (5) y (6) implican que

$$H_K(f(\mathbf{x})) \leq \binom{r+d-1}{d-1}^{d_K} H_K(1:(\beta_{\mathbf{i}}))H_K(1:\mathbf{x})^r < \binom{r+d-1}{d-1}^{d_K} N^{2rd_K} < N^{3rd_K}$$

para N suficientemente grande. Luego, por definición 4.8, f es un r-polinomio homogéneo no nulo de grado r que se anula sobre A. Esto concluye la prueba. En particular, podemos tomar $r = \left\lceil (18c_2 d_K^2 (d-1)!)^{\frac{1}{h-1}} \right\rceil$. □

Observación 4.17. Notemos que si bien el Teorema 4.1 implica el Teorema 3.4, y por tanto al Teorema 0.5, no implica el Teorema 0.4. Una razón es que el Teorema 4.1 es válido para $0 \leq k < d-1$, mientras que el Teorema 0.4 es válido para $0 \leq k < d$. Otra razón es que el enunciado del Teorema 0.4 está en términos de conjuntos S que se encuentran en $[N]^d_{\mathcal{O}_K}$. En cambio, si en el Teorema 0.4 el conjunto S se encuentra en $[N]_{\mathbb{A}^d(\mathcal{O}_K)}$ y ocupa como máximo $\alpha \mathcal{N}_K(\mathfrak{p})^k$ clases residuales para cada primo $\mathfrak{p}$, con $0 \leq k < d-1$, entonces la conclusión del teorema se sigue inmediatamente del Teorema 3.4. Para demostrar el Teorema 0.4 tal como se establece en la introducción, observemos el hecho de que el número de monomios de grado como máximo r en d variables es igual a $\binom{r+d}{d}$. Teniendo en cuenta que el Lema 4.3 y la Proposición 4.10 son válidos para cualquier $h \geq 1$, una modificación sencilla en la construcción del polinomio auxiliar presentado en esta sección da el siguiente resultado.

Teorema 4.18. *Sean d, h enteros positivos y sea $\varepsilon, \eta > 0$ un número real positivo. Sea K un cuerpo global de grado d_K y $\mathcal{O}_K$ su anillo de enteros. Tomemos $Q = N^{\frac{\varepsilon}{2d}}$ y sea $P \subseteq \mathcal{P}(Q)$ tal que $w(P) \geq \kappa \log(Q)$ para algún $\kappa > 0$. Supongamos que $S \subseteq [N]^d_{\mathcal{O}_K}$ es un conjunto de tamaño $|S| \geq cN^{d-h-1+\varepsilon}$ ocupando a lo sumo $\alpha \mathcal{N}_K(\mathfrak{p})^{d-h}$ clases residuales módulo $\mathfrak{p}$ para cada primo $\mathfrak{p} \in P$ y algún $\alpha > 0$. Luego, si N es suficientemente grande, existe un polinomio no nulo $f \in \mathcal{O}_K[X_1, \ldots, X_d]$ de grado $O_{d,h,\varepsilon,\eta,\kappa,K}(1)$ y coeficientes de altura acotada por $N^{O_{d,h,\varepsilon,\eta,\kappa,K}(1)}$ que se anula en más de $(1-\eta)|S|$ puntos de S.*

Ahora, es inmediato que el Teorema 4.18 implica una versión adecuada del Teorema 3.4, a partir de la cual se deduce el Teorema 0.4.

Como se puede ver de la construcción del polinomio homogéneo mediante el lema de Siegel, para poder tomar r grande es necesario que $h > 1$, esto deja sin considerar el caso $k = d-1$ en el enunciado del Teorema 0.5. Esto se debe a que el subconjunto característico tiene tamaño $\lesssim r^{d-h}$ mientras que la dimensión del espacio de polinomios homogéneos de grado r en d variables es $\sim r^{d-1}$, por lo tanto la matriz del sistema es de tamaño $c_1 r^{d-h} \times c_2 r^{d-1}$. Es tentador pensar que este problema puede evitarse si en lugar de reducir el Teorema 0.5 al Teorema 3.1 se intenta demostrar una versión proyectiva de la Proposición 4.10. En este caso un obstáculo para llevar a cabo la inducción es que

un conjunto mal distribuido de tamaño $N^{d-h+\varepsilon}$ en $\mathbb{P}^d(K)$ puede tener muchas secciones y, por lo tanto, el tamaño de cada sección es menor que el tamaño deseado. Específicamente, en la ecuación (48) de la Afirmación 4.6, $|\pi_1(\overline{S})|$ puede ser de tamaño $\sim N^2$ en lugar de tamaño $\sim N^{1+\varepsilon}$, y por lo tanto las secciones tendrían un tamaño de al menos $\gtrsim N^{d-h-2+\varepsilon}$ en lugar de un tamaño de al menos $\gtrsim N^{d-h-1+\varepsilon}$. Si S tiene proyecciones pequeñas, es decir, que $|\pi_j(\overline{S})|$ es de tamaño $\lesssim N^{1+\varepsilon}$ para todo $1 \le j \le d$, entonces la misma prueba funcionaría reemplazando la criba más grande por una versión proyectiva de la misma, como la presentada en [**Zyw10**].

Como comentario final, mencionamos que el Teorema 0.3, el Teorema 0.4, el Teorema 4.1 y el Teorema 4.18 también son válidos cuando $S \subseteq [N]^d_{\mathcal{O}_{K,S}}$ donde, como en el Capítulo 1, $\mathcal{O}_{K,S}$ denota los anillos de S-enteros, para S un subconjunto finito de lugares que contienen $M_{K,\infty}$ cuando K es cuerpo de números y que contiene el lugar distinguido v en el caso de que K sea un cuerpo funcional sobre $\mathbb{F}_q$.

Bibliografía

[Bar15] F. Barroero. Algebraic S-integers of fixed degree and bounded height. *Acta Arith.*, 167(1):67–90, 2015.

[BG06] E. Bombieri and W. Gubler. *Heights in Diophantine geometry (New Mathematical Monographs 4)*. Cambridge University Press, Cambridge, 2006.

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

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

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

[EG15] J. Evertse and K. Győry. *Unit equations in Diophantine number theory (Cambridge Studies in Advanced Mathematics 146)*. Cambridge University Press, Cambridge, 2015.

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

[Gal71] P. X. Gallagher. A larger sieve. *Acta Arith.*, 18:77–81, 1971.

[Gre08] B. Green. On a variant of the large sieve. *arXiv e-prints, page arXiv:0807.5037*, Jul 2008.

[HS00] M. Hindry and J. Silverman. *Diophantine geometry: An Introduction (Graduate Texts in Mathematics 201)*. Springer-Verlag, New York, 2000.

[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.

[Lan83] S. Lang. *Fundamentals of Diophantine geometry (Graduate Texts in Mathematics)*. Springer-Verlag, New York, 1983.

[LM04] T. Loher and D. Masser. Uniformly counting points of bounded height. *Acta Arith.*, 111(3), 2004.

[Lor96] D. Lorenzini. *An invitation to arithmetic geometry (Graduate Studies in Mathematics 9)*. American Mathematical Society, Providence, RI, 1996.

[Mar10] E. (Ed.) Marchionna. Questions on algebraic varieties. Centro Internazionale Matematico Estivo (C.I.M.E.) Summer Schools 51, 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].

[Mon68] H. L. Montgomery. A note on the large sieve. *J. London Math. Soc.*, 43:93–98, 1968.

[MPS21] J. M. Menconi, M. Paredes, and R. Sasyk. The inverse sieve problem for algebraic varieties over global fields. *Rev. Mat. Iberoam.*, 37(6):2245–2284, 2021.

[Mum70] D. Mumford. Varieties defined by quadratic equations. In *Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969)*, pages 29–100. Edizioni Cremonese, Rome, 1970.

[Nar04] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[Par21] M. Paredes. Ill-distributed sets over global fields and exceptional sets in diophantine geometry. *Acta Arith.*, 199(4):361–382, 2021.

[Ros02] M. Rosen. *Number theory in function fields (Graduate Texts in Mathematics 210)*. Springer-Verlag, New York, 2002.

[Sed17] A. Sedunova. On the Bombieri-Pila method over function fields. *Acta Arith.*, 181(4):321–331, 2017.

[Ser89] J. P. Serre. *Lectures on the Mordell-Weil theorem (Aspects of Mathematics, E15)*. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

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

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

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

[TV91] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes (Mathematics and its Applications (Soviet Series) 58)*. Kluwer Academic Publishers Group, Dordrecht, 1991. Translated from the Russian by the authors.

[TV10] T. Tao and V. H. Vu. *Additive combinatorics (Cambridge Studies in Advanced Mathematics 105)*. Cambridge University Press, Cambridge, 2010.

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

[Zyw10] D. Zywina. Hilbert's irreducibility theorem and the larger sieve. *arXiv e-prints, page arXiv:1011.6465*, Nov 2010.