UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Tesis de Licenciatura

Teorema de Bombieri-Vaaler sobre el lema de Siegel

Álvaro Daniel Garimberti

Director: Román Sasyk

Junio 2019

Índice general

Introducción

La construcción de polinomios auxiliares es una técnica básica en aproximación diofántica y teoría de la trascendencia. Este tipo de ideas también ha sido de gran utilidad en otras áreas de las matemáticas, particularmente en problemas de naturaleza combinatoria. Su importancia radica en el hecho de que sirven para evidenciar una estructura algebraica subyacente del problema.

En términos generales, la estrategia del método polinomial es capturar el conjunto de objetos de interés dentro del conjunto de ceros de un polinomio de grado "pequeño". Más precisamente, el método polinomial consiste de dos pasos. Supongamos que tenemos un conjunto de interés S. El primer paso es encontrar un *subconjunto característico* $A \subset S$ tal que todo polinomio (con ciertas propiedades deseadas) que se anule en A con multiplicidad suficientemente grande tenga que anularse en todos o en la mayoría de los puntos de S también. El segundo paso es encontrar uno de esos polinomios. Las propiedades que pedimos al polinomio dependen de la naturaleza del problema en cuestión, sin embargo, siempre queremos que su grado sea (en cierto sentido) pequeño. También es muy común exigir que los coeficientes pertenezcan a algún anillo adecuado. En esta tesis sólo nos ocuparemos del segundo paso. Para un tratamiento más detallado del método polinomial, el lector puede consultar [10], [17] y [20].

El problema que estudiaremos es el siguiente. Sea K un cuerpo y sea S un subconjunto finito de K^d. Queremos encontrar un polinomio $P \in K[X_1, \ldots, X_d]$ que se anula en cada punto de S. Quizás el enfoque más simple es considerar el sistema de ecuaciones lineales dado por

$$P(s) = 0, \quad s \in S\,,$$

donde las incógnitas son los coeficientes del polinomio. El problema de encontrar el polinomio P es, por lo tanto, equivalente a resolver un sistema lineal.

Siguiendo este enfoque, se puede probar, utilizando un argumento de contar dimensio-

nal elemental, que para cualquier cuerpo K y cualquier subconjunto finito S de K^d, existe un polinomio de grado $\lesssim |S|^{1/d}$ que se anula en todo punto de S. Esta es la versión más simple del lema de Siegel. Observar que esto no nos da ningún control sobre los coeficientes del polinomio; sin embargo, tiene el beneficio de ser aplicable a cualquier cuerpo K. Este resultado es elemental, pero es increíblemente útil. Por ejemplo, es una herramienta crucial en la prueba de Dvir de la conjetura de Kakeya sobre cuerpos finitos (ver [5]).

En casos más específicos, argumentos de contar similares dan propiedades adicionales sobre los coeficientes del polinomio. Si $K = \mathbb{Q}$ y $S \subset \{1, \dots, N\}^d$, el lema de Siegel también afirma que el polinomio tiene coeficientes enteros de módulo $\lesssim (dN)^{1/d}$. Este resultado puede extenderse fácilmente a cuerpos de números; en este caso se debe trabajar con alturas, en lugar del valor absoluto habitual.

Para la mayoría de las aplicaciones, una de estas dos versiones del lema de Siegel es suficiente. A veces, sin embargo, uno necesita mejores cotas para los coeficientes (ver, por ejemplo, [19]). En [3], Bombieri y Vaaler obtuvieron varias mejoras del lema de Siegel. Sus argumentos se basan en las poderosas técnicas de Geometry of Number en lugar de los argumentos de contar, más simples pero menos precisos, utilizados por Thue y Siegel. Sin embargo, aparece una dificultad cuando se trabaja sobre cuerpos de números arbitrarios, lo que proporciona una motivación para trabajar en el contexto de adeles.

Consideremos primero la situación más simple. Queremos resolver el sistema $Ax = 0$ en los enteros, donde A es una matriz $M \times N$ con entradas en $\mathbb{Z}$. Además, queremos probar que existe una base de soluciones "pequeñas" en $\mathbb{Z}^N$. Esto requiere del segundo teorema de Minkowski, que habla sobre puntos linealmente independientes en el lattice. El punto crucial es que todas las pruebas conocidas del segundo teorema de Minkowski en $\mathbb{R}^N$ consideran un lattice $\Lambda = \mathbb{Z}^N$ y un sublattice M y proporcionan bases de M y Λ de modo que la base de M se pueda expresar en forma triangular en términos de la base de Λ.

En el caso de un cuerpo de números arbitrario K, reemplazamos $\mathbb{Z}^N$ por $(\mathcal{O}_K)^N$, donde $\mathcal{O}_K$ es el anillo de enteros de K. En este caso, el resultado anterior relativo a las bases de un sublattice es válido solo si $\mathcal{O}_K$ es un ideal principal, y de lo contrario, la prueba del segundo teorema de Minkowski no se puede completar de manera obvia. Dado que un dominio de Dedekind es un dominio de ideales principales si y solo si es un dominio de factorización única, una forma de resolver esta dificultad es restaurar la factorización única mediante la localización en un conjunto suficientemente grande de primos (es decir,

reemplazar $\mathcal{O}_K$ por $S^{-1}\mathcal{O}_K$ para un conjunto multiplicativo S apropiado) y luego ver a K como subconjunto de un espacio "más grande", en donde la localización $S^{-1}\mathcal{O}_K$ sea discreta. De hecho, podemos localizar con respecto a todos los primos, y así el espacio "más grande" adecuado es el anillo de adeles de K. En particular, esto significa que necesitamos geometría de números en adeles.

El objetivo de esta tesis es estudiar los argumentos utilizados por Bombieri y Vaaler para obtener mejoras del lema de Siegel. Estructuralmente, hacemos esto de la siguiente manera.

El primer capítulo está dedicado al desarrollo de resultados preliminares. Primero, revisamos los conceptos básicos de la teoría de valuaciones y cuerpos locales, de modo que podamos definir el anillo de adeles de un cuerpo de números. Luego, damos algunas propiedades del discriminante, con el único propósito de llegar a un tipo de fórmula del producto. Después de eso, recordamos algunos hechos básicos de la medida de Haar, y definimos la medida de Haar adélica y la medida en el espacio cociente. Finalmente, definimos la altura de un vector y de una matriz. Nuestras referencias principales para este capítulo son [2] y [15]; para la sección sobre discriminantes, seguimos [13].

En el segundo y tercer capítulo se tratan los dos resultados principales de geometría de números involucrados en la prueba de Bombieri y Vaaler: el segundo teorema de Minkowski y la desigualdad de rebanado de cubos (*cube slicing inequality*). En ambos casos, primero estudiamos el caso real y luego extendemos los argumentos al contexto adélico. Nuestras referencias principales para estos dos capítulos son [2], [3] y [18].

En el último capítulo, estudiamos las mejoras por Bombieri y Vaaler del lema de Siegel. Comenzamos recordando el lema de Siegel y su extensión a cuerpos de números. Luego, enunciamos el lema de Bombieri-Vaaler y lo comparamos con el resultado de Siegel. Finalmente, siguiendo [3], damos una prueba del lema de Bombieri-Vaaler, junto con varias generalizaciones.

Capítulo 1

Preliminares

1.1. Valores absolutos

Definición 1.1.1. Un **valor absoluto** en un cuerpo K es una función a valores reales $|\cdot|$ en K tal que, para todo $x, y \in K$:

(a) $|x| \geq 0$ y $|x| = 0$ si y solo si $x = 0$.

(b) $|xy| = |x||y|$.

(c) $|x + y| \leq |x| + |y|$ (*desigualdad triangular*).

Un valor absoluto se llama **no arquimediano** si en lugar de la desigualdad triangular (c), satisface la condición más fuerte

(c ') $|x + y| \leq \text{máx}\{|x|, |y|\}$ (*desigualdad ultramétrica)*

Un valor absoluto para el cual (c') no se satisface para algún par $x, y \in K$ se dice **arquimediano**.

El valor absoluto **trivial** es el que es igual a uno para todo elemento no nulo de K.

La siguiente caracterización de valores absolutos no arquimedianos es bastante útil:

Proposición 1.1.2. *Sea $|\cdot|$ un valor absoluto en K. Las siguientes afirmaciones son equivalentes:*

1. $|\cdot|$ *satisface la desigualdad ultramétrica*

2. *El conjunto* $\{|n| : n \in \mathbb{N}\}$ *es acotado.*

En cualquier caso, la sucesión $(|n|)_{n\in\mathbb{N}}$ *está acotada por* 1.

Demostración. Ver, por ejemplo, [15, 4-28]. □

Está claro que un valor absoluto $|\cdot|$ define una métrica en K dada por $d(x, y) = |x-y|$. Esto induce una topología en K. Si dos valores absolutos definen la misma topología, se denominan **equivalentes**.

Proposición 1.1.3. *Sean* $|\cdot|_1$ *y* $|\cdot|_2$ *dos valores absolutos de* K*. Las siguientes afirmaciones son equivalentes:*

(a) $|\cdot|_1$ *y* $|\cdot|_2$ *son equivalentes.*

(b) Existe un número real positivo s *tal que*

$$|x|_1 = |x|_2^s$$

para todo $x \in K$*.*

(c) Para cualquier $x \in K$*,* $|x|_1 < 1$ *si y solo si* $|x|_2 < 1$*.*

Demostración. Ver [8, Th. 9.1] y [9, Ch. XII, Prop. 1.1]. □

Definición 1.1.4. Un **lugar** v es una clase de equivalencia de valor absoluto no trivial. Por $|\cdot|_v$ denotamos a un valor absoluto en la clase de equivalencia v.

Si L/K es una extensión de cuerpos, v es un lugar de K y w un lugar de L, decimos que w **está arriba de** (o **sobre**) v si la restricción a K de cualquier representante de w es un representante de v. En este caso, escribimos $w|v$.

La **completación** de K con respecto al lugar v es un cuerpo K_v con un lugar w tal que:

- $w|v$
- K_v es completo con la topología inducida por w.

- K es un subconjunto denso de K_v en la topología inducida por w.

La completación existe y es única salvo isomorfismo isométrico. Esto se puede probar utilizando la familiar construcción de clases de equivalencia de las sucesiones de Cauchy.

Ejemplo. En $\mathbb{Q}$, claramente tenemos el valor absoluto euclidiano $|\cdot| = |\cdot|_\infty$, que es arquimediano. La completación de $\mathbb{Q}$ con respecto a este valor absoluto es claramente $\mathbb{R}$.

Para cada primo p, también tenemos el valor absoluto p-ádico $|\cdot|_p$, determinado de la siguiente manera. Sea $m/n \in \mathbb{Q}$ un número racional, podemos escribirlo en la forma

$$\frac{m}{n} = p^a \frac{m'}{n'},$$

donde m', n' son números primos coprimos con p. Luego definimos

$$\left|\frac{m}{n}\right|_p := p^{-a}.$$

La completación de $\mathbb{Q}$ con respecto al valor absoluto p-ádico se denomina cuerpo de números p-ádicos y se denota $\mathbb{Q}_p$.

El siguiente teorema de Ostrowski nos dice que, de hecho, estos son todos los lugares en $\mathbb{Q}$.

Teorema 1.1.5 (Ostrowski)**.** *Cada lugar no trivial de $\mathbb{Q}$ se puede representar con el valor absoluto habitual o con el valor absoluto p-ádico correspondiente a algún primo p.*

Demostración. Ver, por ejemplo, [7, Th. 3.1.3], o [15, 4-30]. □

Sea K un cuerpo con un lugar no arquimediano v. Definimos el **anillo de valuación** de v como

$$\mathcal{O}_v := \{x \in K : |x|_v \leq 1\}.$$

No es difícil probar que $\mathcal{O}_v$ es un anillo local con único ideal máximal

$$\mathfrak{m}_v := \{x \in K : |x|_v < 1\}.$$

El cociente $\mathcal{O}_v/\mathfrak{m}_v$ es entonces un cuerpo, denominado **cuerpo residual**.

Sea L una extensión de cuerpos de dimensión finita de K y w un lugar de L sobre v. Entonces $\mathcal{O}_w/\mathfrak{m}_w$ es una extensión de cuerpos de dimensión finita de $\mathcal{O}_v/\mathfrak{m}_v$. Su grado se denomina **grado residual**; lo denotamos $f_{w/v}$. Por otro lado, es claro que $|K^\times|_v$ es un

subgrupo multiplicativo de $|L^\times|_w$. Su índice se denomina **índice de ramificación** de w en v; lo denotamos $e_{w/v}$.

Un lugar v se dice **discreto** si el grupo $|K^\times|_v$ es cíclico. En este caso, $\mathfrak{m}_v$ es un ideal principal y cualquier generador principal se denomina **parámetro local**; además, cada ideal de $\mathcal{O}_v$ es de la forma $(\mathfrak{m}_v)^n$ para algún entero positivo n (ver [13, (3.9)]).

Ejemplo. Supongamos $K = \mathbb{Q}$ y consideremos un lugar no arquimediano p. El anillo de valuación de p se denota $\mathbb{Z}_p$, y su ideal máximal es $p\mathbb{Z}_p$, es decir, el ideal principal generado por el primo p. Estudiando el núcleo de la composición

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/p\mathbb{Z}_p$$

uno prueba fácilmente que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. Por lo tanto, el cuerpo residual es $\mathbb{F}_p$, el cuerpo finito de p elementos.

Proposición 1.1.6. *$\mathcal{O}_v$ es un subconjunto abierto y cerrado de K con respecto a la topología dada por v. Además, es compacto si y solo si el cuerpo residual $\mathcal{O}_v/\mathfrak{m}_v$ es finito.*

Demostración. Ver [7, Prop. 2.3.6], y [16, Lemma 9.5, Prop. 9.7]. □

Sea K un cuerpo de números (es decir, una extensión finita de $\mathbb{Q}$). Para cada lugar no arquimediano v de K, sea $\mathcal{O}_v$ el anillo de valuación de K_v (continuaremos usando esta notación a lo largo de toda la tesis). Cada lugar no arquimediano de K está sobre algún primo, con lo cual el cuerpo residual $\mathcal{O}_v/\mathfrak{m}_v$ correspondiente a K_v es una extensión finita del cuerpo residual $\mathbb{F}_p$ correspondiente a $\mathbb{Q}_p$, y por lo tanto es un cuerpo finito. Entonces, Proposición 1.1.6 implica:

Corolario 1.1.7. *Si K es un cuerpo de números, entonces, para cada lugar no arquimediano v, el anillo de valuación $\mathcal{O}_v$ de la completación K_v es compacto.*

Ahora, supongamos que tenemos una extensión separable finita L/K. Para lugares no arquimedianos, existe una relación entre el grado local, el índice de ramificación y el grado residual.

Lema 1.1.8. *Sea L/K una extensión separable finita. Sea v un lugar no arquimediano de K y w un lugar de L sobre v. Sean K_v y L_w las completaciones correspondientes, y sean e_v y f_v el índice de ramificación y el grado residual, respectivamente. Entonces,*

$$[L_w : K_v] = e_v f_v.$$

Demostración. Ver, por ejemplo, [15, 4-33], o [9, Ch. XII, Prop. 6.1]. □

1.1.1. Extensión de valores absolutos

En esta tesis, trabajaremos con cuerpos de números; es decir, extensiones algebraicas finitas de $\mathbb{Q}$. Ya que hemos enumerado todos los lugares de $\mathbb{Q}$, será de gran utilidad para nosotros entender cómo se extienden los valores absolutos en extensiones algebraicas finitas.

Primero, recordamos un resultado sobre extensiones finitas de cuerpos completos.

Proposición 1.1.9. *Sea K un cuerpo completo con valor absoluto $|\cdot|_v$ y sea L una extensión finita de K. Luego hay una única extensión de $|\cdot|_v$ a un valor absoluto $|\cdot|_w$ de L, que se define explícitamente por la ecuación*

$$|x|_w = |N_{L/K}(x)|_v^{1/[L:K]},$$

donde $N_{L/K}$ es la norma de la extensión L/K. Además, el cuerpo L es completo con respecto a $|\cdot|_w$.

Demostración. Ver, por ejemplo, [8, Th.s 9.8, 9.9, 9.12]. □

Observación. La proposición anterior implica que, si K es completo, su valor absoluto se extiende de manera única a la clausura algebraica de K. Sin embargo, la clausura algebraica no es necesariamente completa con respecto a ese valor absoluto.

Sea K un cuerpo con un valor absoluto no trivial fijo $|\cdot|_v$.

Teorema 1.1.10. *Sea L una extensión de cuerpos finita de K generada por un único elemento ξ. Sea f el polinomio minimal de ξ sobre K y sea*

$$f = f_1^{k_1} \cdots f_r^{k_r}$$

su descomposición en factores mónicos irreducibles sobre $K_v[t]$. Luego, se satisfacen las siguientes afirmaciones:

(a) Para cada j hay un homomorfismo inyectivo $\iota_j : L \to K_j := K_v[t]/(f_j)$ de extensiones de cuerpos sobre K, dado por $\xi \mapsto t$.

(b) Existe una extensión única $|\cdot|_j$ del valor absoluto de K_v a K_j. Además, los valores absolutos $|\cdot|_j$ no son equivalentes dos a dos.

(c) K_j *es la completación de* L *con respecto al valor absoluto* $|\cdot|_j$ *y el morfismo* ι_j*.*

(d) Para cualquier valor absoluto $|\cdot|_w$ *que extiende a* $|\cdot|_v$ *a* L*, hay un único* $j \in \{1, \ldots, r\}$ *tal que la restricción de* $|\cdot|_j$ *a* L *es igual a* $|\cdot|_w$*.*

Demostración. Proposición 1.1.9 prueba que existe una extensión única $|\cdot|_j$ del valor absoluto de K_v a K_j. Es fácil ver que ι_j es un homomorfismo inyectivo bien definido. Además, dado que K es denso en K_v y la clase de t en K_j está contenida en la imagen de ι_j, tenemos que la imagen de ι_j es densa en K_j. Utilizando una vez más Proposición 1.1.9, se deduce que K_j es la completación de L con respecto a $|\cdot|_j$.

Si las restricciones de $|\cdot|_j$ y $|\cdot|_k$ a L son equivalentes, entonces tenemos un isomorfismo isométrico de K_j en K_k que deja K_v fijo. Por lo tanto, las imágenes de ξ de los respectivos embeddings ι_j y ι_k deben ser raíces del mismo factor irreducible de $f(t)$ en $K_v[t]$. Por lo tanto, $j = k$.

Hasta ahora hemos demostrado (a), (b) y (c). Sólo queda (d). Sea $|\cdot|_w$ un valor absoluto de L que extiende a $|\cdot|_v$. La clausura (topológica) de K en L_w se puede identificar con K_v, por lo que $L_w = K_v(\xi)$ (aquí asumimos $L \subset L_w$). De hecho, $K_v(\xi) \subset L_w$, L es denso en $K_v(\xi)$ y, por Proposición 1.1.9, $K_v(\xi)$ es completo. Al deshacer las identificaciones realizadas, hemos demostrado que L_w es isomorfo a algún K_j, porque ξ es una raíz de algún f_j. Además, $L = K(\xi)$ queda fijo bajo este isomorfismo. Por la parte de unicidad de la Proposición 1.1.9, $|\cdot|_w$ es igual a la restricción de $|\cdot|_j$ a L. □

Observación. El teorema anterior nos dice que existe una correspondencia biyectiva entre los lugares de $L = K(\xi)$ sobre v y los factores irreducibles del polinomio minimal de ξ sobre K. Más aún, si fijamos una clausura algebraica $\overline{K}_v$ de K_v, entonces la completación de L con respecto al lugar w_j correspondiente al factor f_j es isomorfa a $K_v(\beta)$, donde $\beta \in \overline{K}_v$ es cualquier raíz de f_j.

Si L es una extensión finita separable de K, podemos deducir dos corolarios.

Corolario 1.1.11. *Sea* L *una extensión separable finita de* K *y sea* v *un lugar de* K*. Entonces, tenemos un isomorfismo de espacios vectoriales sobre* K_v

$$L \otimes_K K_v \cong \prod_{w|v} L_w,$$

donde el producto es sobre todos los lugares w *de* L *que se encuentran sobre* v*.*

Más específicamente, si L, K, ξ, f *y* $f_1, \ldots, f_r$ *se definen como en Teorema 1.1.10, entonces*

$$\psi : K(\xi) \otimes_K K_v \longrightarrow \prod_{j=1}^{r} K_v[X]/(f_j(X)), \quad \psi\left(\sum_i p_i(\xi) \otimes \lambda_i\right) = \left(\sum_i \lambda_i \overline{p_i(X)}^j\right)_{j=1,\ldots,r}$$

es un isomorfismo de espacios vectoriales sobre K_v*, donde, para cada* i*,* p_i *es un polinomio con coeficientes en* K *y* $\overline{p_i(X)}^j$ *denota la clase de* p_i *en* $K_v[X]/(f_j(X))$*.*

Demostración. Por el teorema chino del resto,

$$\prod_{j=1}^{r} K_v[X]/(f_j(X)) \cong K_v[X]/(f(X)).$$

Luego,

$$L \otimes_K K_v \cong K[X]/(f) \otimes_K K_v \cong K_v[X]/(f) \cong K_v[X]/(f(X)).$$

El corolario sigue escribiendo explícitamente la cadena de morfismos. □

Corolario 1.1.12. *Si* L *es una extensión separable finita de* K*, entonces*

$$\sum_{w|v} [L_w : K_v] = [L : K],$$

donde la suma es sobre todos los lugares w *de* L *sobre* v*.*

Demostración. Por el teorema del elemento primitivo, $L = K(\xi)$ para algún $\xi \in L$, y por lo tanto, estamos en la hipótesis del Teorema 1.1.10. En este caso, el polinomio minimal f es separable (es decir, todas sus raíces tienen multiplicidad uno) y por lo tanto $k_1 = k_2 = \cdots = k_r = 1$. Por el teorema, cada factor f_j de f sobre K_v corresponde a un lugar w de L, y la extensión L_w/K_v tiene un grado $[L_w : K_v] = \deg f_j$. El resultado se sigue de forma inmediata. □

Definición 1.1.13. El número $[L_w : K_v]$ es el **grado local** de L/K en w. Por lo general, denotaremos $d = [L : K]$ y $d_w = [L_w : K_v]$.

Si, además, la extensión L/K es Galois, entonces todas las completaciones de L con respecto a lugares arriba de v son isomorfas.

Corolario 1.1.14. *Si* L/K *es una extensión de Galois del grado* d*, entonces el grado local* d_v *es constante para todo* $w|v$*.*

Demostración. Sea ξ un elemento de L con $L = K(\xi)$, y sea f su polinomio minimal sobre K. Sea $\overline{K}_v$ una clausura algebraica de K_v. Como L/K es Galois, L contiene todas las raíces de f, y por lo tanto, para cada lugar $w|v$, la completación L_w contiene todas las raíces de f. Por Teorema 1.1.10, todas las completaciones son iguales (vistas como subcuerpos de $\overline{K}_v$). Por lo tanto, d_v es constante para todo $w|v$. □

Normalización de extensiones de lugares

Sea K un cuerpo con un valor absoluto no trivial fijo $|\cdot|_v$. Sea L una extensión separable finita de K, y sea w un lugar de L con $w|v$. Para cualquier $x \in L$, definimos

$$\|x\|_w := |N_{L_w/K_v}(x)|_v$$

y

$$|x|_w := |N_{L_w/K_v}(x)|_v^{1/[L:K]}.$$

Observación. $|\cdot|_w$ siempre es un valor absoluto, y $\|\cdot\|_w$ es un valor absoluto si y solo si v es no arquimediano o $[L_w : K_v] = 1$.

Para un valor absoluto fijo $|\cdot|_v$, siempre nos referiremos a $|\cdot|_w$ y $\|\cdot\|_w$ como los **valores absolutos normalizados** correspondientes al lugar $w|v$. Claramente, para $\|\cdot\|_w$, esta nomenclatura se usará únicamente si v es no arquimediano o si $[L_w : K_v] = 1$.

El siguiente lema establece una relación entre el valor absoluto $|\cdot|_v$ y los valores absolutos normalizados correspondientes a lugares sobre v.

Lema 1.1.15. *Sean K y L como arriba. Sean $x \in K \setminus \{0\}$ y $y \in L \setminus \{0\}$. Manteniendo la notación anterior, tenemos que*

$$\prod_{w|v} |x|_w = |x|_v,$$

$$\prod_{w|v} \|y\|_w = |N_{L/K}(y)|_v.$$

Demostración. La primera igualdad es una consecuencia directa del Corolario 1.1.12, y de que $K \subset K_v$, lo que significa $N_{L_w/K_v}(x) = x^{[L_w:K_v]}$.

La segunda afirmación se reduce a probar que, para cualquier $y \in L$,

$$N_{L/K}(y) = \prod_{w|v} N_{L_w/K_v}(y). \tag{1.1}$$

Primero asumimos que $L = K(y)$. Sea f el polinomio minimal de y sobre K, y sea $f = f_1 \cdots f_r$ su factorización en polinomios irreducibles sobre K_v. Por Teorema 1.1.10, hay exactamente r lugares de L sobre v. Sean $w_1, \ldots, w_r$ dichos lugares y $L_1, \ldots L_r$ sus respectivas completaciones. Sabemos que $L_j = K_v(y_j)$ para alguna raíz y_j del polinomio irreducible f_j. Explícitamente, y_j es la imagen de y por el correspondiente embedding $\iota_j : L \hookrightarrow L_j$. La norma $N_{L/K}(y)$ es igual a $(-1)^{\deg f}$ por el término constante de f. Lo mismo ocurre para cada $N_{L_j/K_v}(y_j)$ y f_j. Como el término constante de f es igual al producto de los términos constantes de f_j, finalmente obtenemos (1.1).

Ahora, si L no es igual a $K(y)$, necesitaremos usar la transitividad de la norma, es decir

$$N_{L/K} = N_{K(y)/K} \circ N_{L/K(y)},$$

y lo mismo para las torres locales $K_v \subset K_v(y_j) \subset L_j$, con y_j como en el párrafo anterior. Si $d = [L : K]$ y $s = \deg f = [K(y) : K]$, tenemos

$$\begin{aligned} N_{L/K}(y) &= N_{K(y)/K}(N_{L/K(y)}(y)) \\ &= N_{K(y)/K}(y^{\frac{d}{s}}) \\ &= \prod_{j=1}^{r} N_{K_v(y_j)/K_v}(y_j^{\frac{d}{s}}) \end{aligned}$$

Observar que $d/s = [L : K(y)]$, entonces si $w_1, \ldots, w_r$ son los lugares de $K(y)$ sobre v, por Corolario 1.1.12 tenemos

$$\frac{d}{s} = \sum_{u|w_j} [L_u : K_v(y_j)]$$

para cada $j = 1, \ldots, r$. Además, sabemos que

$$N_{L_u/K_v(y_j)}(y_j) = y_j^{[L_u:K_v(y_j)]}.$$

Entonces,

$$\begin{aligned} N_{K_v(y_j)/K_v}(y_j^{\frac{d}{s}}) &= \prod_{u|w_j} N_{K_v(y_j)/K_v}(N_{L_u/K_v(y_j)}(y_j)) \\ &= \prod_{u|w_j} N_{L_u/K_v}(y_j). \end{aligned}$$

El lema se sigue del hecho de que cada lugar de L sobre K está sobre exactamente un lugar w_j de $K(y)$. □

Supongamos ahora que L/K es una extensión finita de Galois. Sea v un lugar de K y sea $\sigma \in \mathrm{Gal}(L/K)$. Para w un lugar de L sobre v, consideremos la aplicación $|\cdot|_{\sigma(w)}$ definida por

$$x \in L \longmapsto |\sigma(x)|_w \in \mathbb{R}_{\geq 0}\,,$$

donde $|\cdot|_w$ es el valor absoluto normalizado. Dado que σ es un automorfismo que fija K, está claro que $|\cdot|_{\sigma(w)}$ es un valor absoluto que está arriba de v. Por lo tanto, por la Proposición 1.1.3, hay un número real $s > 0$, y un lugar w' sobre v tal que

$$|\sigma(x)|_w = |x|_{w'}^s \tag{1.2}$$

para todo $x \in L$, donde $|\cdot|_{w'}$ es el valor absoluto normalizado correspondiente a w'. Si tomamos $x \in K$ entonces (1.2) da

$$|x|_v^{\frac{d_w}{d}} = |x|_v^{\frac{d_{w'}}{d}s}\,,$$

donde $d = [L : K]$, $d_w = [L_w : K_v]$ y $d_{w'} = [L_{w'} : K_v]$. Pero, por el Corolario 1.1.14, $d_w = d_{w'}$, entonces $s = 1$. Por lo tanto, $|\cdot|_{\sigma(w)}$ es el absoluto normalizado correspondiente a un lugar sobre v.

Hemos probado la siguiente proposición.

Proposición 1.1.16. *Sea L/K una extensión finita de Galois, sea v un lugar de K y sea $\sigma \in Gal(L/K)$. Para cualquier lugar w de L sobre v, defina $|\cdot|_{\sigma(w)}$ para que sea la aplicación*

$$x \in L \longmapsto |\sigma(x)|_w \in \mathbb{R}_{\geq 0}\,,$$

donde $|\cdot|_w$ denota el valor absoluto normalizado. Luego, hay otro lugar w' de L sobre v, de manera que $|\cdot|_{\sigma(w)}$ es el valor absoluto normalizado correspondiente a w'. Además, para dos lugares distintos w_1, w_2 de L, los valores absolutos $|\cdot|_{\sigma(w_1)}$ y $|\cdot|_{\sigma(w_2)}$ son no equivalentes.

Concretamente, cada $\sigma \in Gal(L/K)$ define una bijection $|\cdot|_w \mapsto |\cdot|_{\sigma(w)}$ en el conjunto de valores absolutos normalizados de L sobre v.

1.1.2. Cuerpos de números y anillo de enteros

Si K es un cuerpo de números, los lugares no arquimedianos también se llaman **lugares finitos** y los arquimedianos se llaman **lugares infinitos**. En otras palabras, los lugares finitos son aquellos que se encuentran sobre los lugares p-ádicos, y los lugares infinitos son aquellos que se encuentran sobre el lugar euclidiano habitual.

Observación. En el contexto más general de los cuerpos globales, la distinción entre finito e infinito no corresponde a la dicotomía de lo arquimediano frente a lo no arquimediano. Los lugares finitos son en realidad aquellos que corresponden a los ideales primos del anillo de números enteros, de una manera que se precisará más adelante.

Sea K un cuerpo de números. Usando Teorema 1.1.10 podemos ver que si v es un lugar infinito, entonces la completación K_v es una extensión finita de $\mathbb{R}$. De ello se deduce que $K_v = \mathbb{R}$, en cuyo caso v se denomina **lugar real**, o $K_v = \mathbb{C}$, en cuyo caso decimos que v es un **lugar complejo**.

Definición 1.1.17. Sea K un cuerpo de números. Definimos el **anillo de enteros** de K como

$$\mathcal{O}_K = \bigcap_{v\, finito} \{x \in K : |x|_v \leq 1\}.$$

Proposición 1.1.18. *$\mathcal{O}_K$ es igual al clausura íntegra de $\mathbb{Z}$ en K.*

Demostración. Ver, por ejemplo, [11, Th.s 10.3, 10.4]. □

1.1.3. Lugares finitos e ideales primos

En esta sección, veremos que hay una correspondencia entre lugares finitos e ideales primos de $\mathcal{O}_K$.

Recordar que un ideal fraccionario de $\mathcal{O}_K$ tiene una factorización única en ideales primos. Luego, dado $x \in K$ podemos escribir

$$x\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

con $e_i \in \mathbb{Z}$ para todo $i = 1, \ldots, r$. Dado un ideal primo $\mathfrak{p}$ en $\mathcal{O}_K$ y $x \in K$, definimos el **orden de x en $\mathfrak{p}$** como el exponente de $\mathfrak{p}$ en la factorización del ideal fraccionario principal $x\mathcal{O}_K$. Lo denotamos $ord_{\mathfrak{p}}(x)$. Luego,

$$x\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{ord_{\mathfrak{p}}(x)},$$

donde el producto es sobre todos los ideales primos de $\mathcal{O}_K$.

Ahora podemos definir el lugar en K asociado al primo $\mathfrak{p}$ de la siguiente manera. Si $\mathfrak{p}$ se encuentra sobre el primo $p \in \mathbb{Z}$, entonces

$$|x|_{\mathfrak{p}} := p^{-ord_{\mathfrak{p}}(x)} \tag{1.3}$$

Claramente, cambiando p por cualquier otro número real positivo obtenemos otro representante del mismo lugar.

Concluimos que cada ideal principal de $\mathcal{O}_K$ define un valor absoluto de K. De hecho, cada valor absoluto es equivalente a uno de la forma (1.3). En efecto, sea v un lugar finito en K y sea

$$\mathfrak{p}_v := \{x \in \mathcal{O}_K : |x|_v < 1\}.$$

un ideal primo de $\mathcal{O}_K$. Usando Proposición 1.1.3, es fácil ver que $|\cdot|_v$ es equivalente a $|\cdot|_{\mathfrak{p}_v}$.

Hemos probado la siguiente proposición.

Proposición 1.1.19. *Sea K un cuerpo de números. La aplicación*

$$v \mapsto \mathfrak{p}_v = \{x \in \mathcal{O}_K : |x|_v < 1\}$$

es una correspondencia biyectiva entre los lugares v de K y los ideales primos $\mathfrak{p}$ de $\mathcal{O}_K$. Su inversa es

$$\mathfrak{p} \mapsto |\cdot|_{\mathfrak{p}},$$

donde $|x|_{\mathfrak{p}} := p^{-ord_{\mathfrak{p}}(x)}$.

Corolario 1.1.20. *Cada lugar finito de un cuerpo de números es discreto.*

1.1.4. La fórmula del producto

Consideremos el cuerpo de los números racionales $\mathbb{Q}$. Sea

$$M_{\mathbb{Q}} := \{|\cdot|_p : p \text{ primo o } p = \infty\},$$

donde $|\cdot|_p$ es el valor absoluto p-ádico en $\mathbb{Q}$ si p es primo, y el valor absoluto usual en $\mathbb{Q}$ si $p = \infty$. Es fácil ver que

$$\prod_{p \in M_{\mathbb{Q}}} |x|_p = 1.$$

Esta fórmula puede generalizarse fácilmente a cuerpos de números arbitrarios. Sea K un cuerpo de números y sea M_K el conjunto de valores absolutos normalizados $|\cdot|_v$ correspondientes a lugares sobre elementos de $M_{\mathbb{Q}}$. Por la correspondencia entre lugares finitos e ideales primos de $\mathcal{O}_K$ se puede deducir que, dado $x \in K$, $|x|_v = 1$ para casi todo $|\cdot|_v \in M_K$. Esto significa que el producto infinito $\prod_{v \in M_K} |x|_v$ está bien definido.

Proposición 1.1.21 (La fórmula del producto)**.** *Si K es un cuerpo de números, entonces*

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

Demostración. Ya sabemos que la proposición es cierta para $K = \mathbb{Q}$. Una sencilla aplicación del Lema 1.1.15 da el resultado para un cuerpo de número arbitrario K. □

1.2. Adeles

Sea K un cuerpo de números y sea K_v la completación de K en un lugar v.

Definición 1.2.1. El **anillo de adeles** de K, que denotamos $K_{\mathbb{A}}$, es el subanillo

$$K_{\mathbb{A}} = \{(x_v) : x_v \in K_v \text{ con } x_v \in \mathcal{O}_v \text{ para todo } v, \text{ salvo finitas excepciones}\}$$

del producto $\prod_v K_v$.

Observación. $K_{\mathbb{A}}$ no es localmente compacto con la topología producto. La existencia de una medida de Haar para grupos localmente compactos motiva la construcción de una topología alternativa.

Definimos la **topología adélica** en $K_{\mathbb{A}}$ especificando una base de entornos del elemento neutro aditivo $(0_v)_v$. Esta base consiste en conjuntos de la forma $\prod_v N_v$, donde N_v es un entorno de $0_v \in K_v$ y $N_v = \mathcal{O}_v$ para casi todo lugar v de K.

Para ver que $K_{\mathbb{A}}$ es localmente compacto con esta topología, consideramos la siguiente construcción. Sea S un subconjunto de lugares de K que contiene todos los lugares infinitos, y sea $(K_{\mathbb{A}})_S$ el subanillo

$$(K_{\mathbb{A}})_S = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v.$$

Dado que $(K_{\mathbb{A}})_S$ es el producto de una familia finita de grupos localmente compactos con un grupo compacto, se deduce que $(K_{\mathbb{A}})_S$ es localmente compacto en la topología producto. La observación clave es que la topología producto y la topología adélica coinciden en $(K_{\mathbb{A}})_S$, con lo cual este conjunto es localmente compacto en la topología adélica. Ahora, observemos que

$$K_{\mathbb{A}} = \bigcup_S (K_{\mathbb{A}})_S,$$

donde la unión es sobre todos los conjuntos S de lugares de K que contienen todos los lugares infinitos. Por lo tanto, el anillo de adeles es una unión de anillos localmente compactos, lo que significa que es localmente compacto.

Identificamos K con un subgrupo de $K_{\mathbb{A}}$ por medio de la aplicación diagonal

$$\begin{aligned} K &\longrightarrow K_{\mathbb{A}} \\ x &\longmapsto (x)_v = (x, x, x, \dots). \end{aligned}$$

El siguiente teorema afirma que podemos dar aproximaciones razonablemente buenas de elementos de $K_{\mathbb{A}}$ por elementos de K.

Teorema 1.2.2 (Teorema de aproximación fuerte)**.** *Sea S un conjunto finito de valores absolutos no arquimedianos y no equivalentes $|\cdot|_v$ del cuerpo de números K. Para cada $v \in S$, sea $x_v \in K_v$. Entonces, dado $\epsilon > 0$, existe $\alpha \in K$ con $|\alpha - x_v|_v < \epsilon$ para todo $v \in S$ y $|\alpha|_v \leq 1$ para todo lugar no arquimediano $v \notin S$.*

Demostración. Ver, por ejemplo, [2, Th. 1.4.5]. □

Para finalizar esta sección, probaremos un importante teorema sobre las propiedades topológicas de K como un subespacio de $K_{\mathbb{A}}$, y del cociente $K_{\mathbb{A}}/K$. Antes de eso, necesitamos un lema, que también será importante en sí mismo.

Primero, vamos a fijar notación. Ya que K es un cuerpo de números, por Corolario 1.1.11 tenemos que $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v|\infty} K_v$. En lo que sigue, identificaremos estos dos espacios. Sea $d = [K : \mathbb{Q}]$. Sea $\omega_1, \dots, \omega_d$ una $\mathbb{Z}$-base de $\mathcal{O}_K$, y sea

$$\Omega_\infty := \{x \in \prod_{v|\infty} K_v : \exists\, a_1, \dots, a_d \in [0, 1) \text{ tal que } x = \sum_{j=1}^{d} w_j \otimes a_j\}.$$

Lema 1.2.3. *El subconjunto $\Omega = \Omega_\infty \times \prod_{v \text{ finito}} \mathcal{O}_v$ de $K_{\mathbb{A}}$ es un dominio fundamental de $K_{\mathbb{A}}/K$; es decir, cada clase de $K_{\mathbb{A}}/K$ tiene exactamente un representante en Ω.*

Demostración. El lema tiene dos partes. Por un lado, necesitamos demostrar que cada elemento de $K_{\mathbb{A}}/K$ tiene un representante en Ω, y, por el otro, que dicho representante es único.

Comenzamos con la unicidad. Tomemos $x, y \in \Omega$ de manera que $\alpha = x - y \in K$, con proyecciones a Ω_∞ respectivamente dadas por $\sum_{j=1}^{d} w_j \otimes a_j$ y $\sum_{j=1}^{d} w_j \otimes b_j$. Para

cada lugar finito v, tenemos que $x_v, y_v \in \mathcal{O}_v$; por lo tanto, $\alpha \in \mathcal{O}_K$. Si ahora miramos los lugares infinitos, tenemos

$$\alpha = \sum_{j=1}^{d} w_j \otimes (a_j - b_j)$$

con $a_j - b_j \in (-1, 1)$. Como $\alpha \in \mathcal{O}_K$, podemos escribir

$$\alpha = \left(\sum_{j=1}^{d} c_j w_j \right) \otimes 1,$$

para ciertos $c_1, \ldots, c_d \in \mathbb{Z}$. Usando que $\{\omega_1 \otimes 1, \ldots, \omega_d \otimes 1\}$ es una base de $K \otimes_{\mathbb{Q}} \mathbb{R}$ como espacio vectorial sobre $\mathbb{R}$, podemos deducir que $a_j - b_j \in \mathbb{Z}$. Concluimos que $a_j = b_j$ para todo j, y por lo tanto $x = y$.

Probemos ahora la existencia de un representante en Ω. Sea $\overline{x} \in K_{\mathbb{A}}/K$. Sea S el conjunto de lugares no arquimedianos con $|x|_v > 1$. Por el teorema de aproximación fuerte, existe $\alpha \in K$ tal que $|x_v - \alpha|_v < 1$ para todo $v \in S$ y $|\alpha|_v \leq 1$ para todos los lugares no archimedeanos $v \notin S$. Por lo tanto, reemplazando x por $x - \alpha$, podemos asumir $x_v \in \mathcal{O}_v$ para cada lugar finito v. En el caso de los lugares infinitos, tenemos

$$(x_v)_{v|\infty} = \sum_{j=1}^{d} w_j \otimes a_j$$

para ciertos $a_j \in \mathbb{R}$. Existen $b_1, \ldots, b_d \in \mathbb{Z}$, de modo que $0 \leq a_j - b_j < 1$ para cada j. Entonces $x - \left(\sum_{j=1}^{d} w_j \otimes b_j, 0 \right)$ es un representante de $\overline{x}$ en Ω. □

Ahora, estamos en condiciones de probar el siguiente teorema.

Teorema 1.2.4. *Sea K un cuerpo de números. Entonces, K es un subgrupo discreto de $K_{\mathbb{A}}$, y el grupo cociente $K_{\mathbb{A}}/K$ es compacto en la topología cociente.*

Demostración. Primero veamos que $K \subset K_{\mathbb{A}}$ es discreto. Basta con probar que hay un entorno abierto $U \subset K_{\mathbb{A}}$ de 0 tal que $K \cap U = \{0\}$. Fijemos w un lugar finito de K, y tomemos

$$U := \{x \in K_w : |x|_w < 1\} \times \prod_{v|\infty} \{x \in K_v : |x|_v < 1\} \times \prod_{v \text{ finito}, v \neq w} \mathcal{O}_v.$$

Claramente, U es abierto y contiene 0. Supongamos que existe $x \in U \cap K \setminus \{0\}$. Luego, por la fórmula del producto, deberíamos tener $\prod_v |x|_v = 1$, lo cual es imposible por definición de U.

Ahora, probemos que $K_{\mathbb{A}}/K$ es compacto. Sea Ω el dominio fundamental de $K_{\mathbb{A}}/K$ el lema anterior, y sea

$$\Omega' = \Omega'_\infty \times \prod_{v \text{ finito}} \mathcal{O}_v,$$

donde

$$\Omega'_\infty := \{x \in \prod_{v|\infty} K_v : \exists\, a_1, \ldots, a_d \in [0,1] \text{ tal que } x = \sum_{j=1}^{d} w_j \otimes a_j\}.$$

Sea $\pi : K_{\mathbb{A}} \to K_{\mathbb{A}}/K$ el morfismo cociente. Por el Lema 1.2.3, $\pi(\Omega) = K_{\mathbb{A}}/K$ y, por consiguiente, $\pi(\Omega') = K_{\mathbb{A}}/K$. La topología de Ω' como subespacio del anillo de adeles es igual a la topología producto; por lo tanto, por el teorema de Tychonoff, Ω' es compacto. Como π es continuo, concluimos que $K_{\mathbb{A}}/K$ es compacto. □

1.3. Diferente y discriminante

El objetivo de esta sección es obtener un tipo de fórmula del producto para el discriminante de una extensión finita de $\mathbb{Q}$. Para ello, necesitaremos algunos resultados relativos al ideal diferente y al ideal discriminante. Solamente mencionaremos las definiciones y los resultados que conducen a la fórmula del producto, a fin de proporcionar una idea de la conceptos involucrados en la prueba. Para una descripción más detallada de estos temas, consultar [13, Ch. III, §2].

Sea L/K una extensión separable finita, sea $A \subset K$ un dominio de Dedekind con cuerpo de fracciones $\mathrm{Frac}(A) = K$ y sea que $B \subset L$ su clausura íntegra en L.

Definición 1.3.1. Sea I un ideal fraccionario de L. El **módulo dual** B de I es

$$I^* := \{x \in L : \mathrm{Tr}_{L/K}(xI) \subset A\}.$$

Observación. La noción de dualidad está justificada por el isomorfismo

$$I^* \longrightarrow \hom_A(I, A), \quad x \longmapsto \left(y \mapsto \mathrm{Tr}_{L/K}(xy)\right).$$

Proposición 1.3.2. *Si I es un ideal fraccionario de L, entonces I^* también es un ideal fraccionario.*

Definición 1.3.3. El ideal fraccionario $\mathfrak{C}_{B/A} := B^* = \{x \in L : \mathrm{Tr}(xB) \subset A\}$ se denomina **diferente inverso**. Su inverso $\mathfrak{D}_{B/A} = \mathfrak{C}_{B/A}^{-1}$ es el **diferente** de B/A.

Observación. $B \subset \mathfrak{C}_{B/A}$, y entonces $\mathfrak{D}_{B/A}$ es de hecho un ideal integral de L (es decir, $\mathfrak{D}_{B/A} \subset B$).

Por lo general, cuando los dominios de Dedekind A y B son evidentes del contexto, denotamos al diferente y a su inverso por $\mathfrak{D}_{L/K}$ y $\mathfrak{C}_{L/K}$, respectivamente.

Proposición 1.3.4. (I) *Si S es un subconjunto multiplicativo de A, entonces $S^{-1}B$ es la clausura íntegra de $S^{-1}A$ en L.*

(II) *Sea $\mathfrak{p}$ un ideal primo en A y sea $\mathfrak{q}|\mathfrak{p}$ un ideal primo en B. Denotamos por $A_\mathfrak{p}$, $K_\mathfrak{p}$, $B_\mathfrak{q}$ y $L_\mathfrak{q}$ a las completaciones correspondientes, respecto a los valores absolutos definidos por*

$$|x|_\mathfrak{p} := \exp(-ord_\mathfrak{p}(x)), \ \ y \ |x|_\mathfrak{q} := \exp(-ord_\mathfrak{q}(X)).$$

Entonces, $B_\mathfrak{q}$ es la clausura íntegra de $A_\mathfrak{p}$ en $L_\mathfrak{q}$.

Proposición 1.3.5. (I) *Para cualquier subconjunto multiplicativo S de A, se tiene que*

$$\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}.$$

(II) *Sea $\mathfrak{p}$ un ideal primo en A y sea $\mathfrak{q}|\mathfrak{p}$ un ideal primo en B. Entonces,*

$$\mathfrak{D}_{B/A}B_\mathfrak{q} = \mathfrak{D}_{B_\mathfrak{q}/A_\mathfrak{p}}.$$

Definición 1.3.6. Sea $d = [L : K]$, y sea $e_1, \ldots, e_d$ una base de L como espacio vectorial sobre K. El **discriminante** de la base $\{e_1, \ldots, e_d\}$ se define como

$$d(e_1, \ldots, e_d) := \det\big(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\big).$$

Recordamos el siguiente resultado básico:

Lema 1.3.7. *Si $\sigma_1, \ldots, \sigma_d$ son los K-embeddings $L \hookrightarrow \overline{K}$ (donde $\overline{K}$ es la clausura algebraica de K), entonces*

$$\det\big(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\big) = (\det(\sigma_i\alpha_j))^2.$$

Definición 1.3.8. El **ideal discriminante** $\mathfrak{d}_{B/A}$ es el ideal de A generado por los discriminantes $d(\alpha_1, \ldots, \alpha_d)$ de todas las bases $\alpha_1, \ldots, \alpha_d$ de L/K que están contenidas en B.

Observación. Si $\alpha_1, \ldots, \alpha_d$ es una base íntegra de B/A, entonces $\mathfrak{d}_{L/K}$ es un ideal principal generado por $d(\alpha_1, \ldots, \alpha_d)$. En efecto, si $\beta_1, \ldots, \beta_d \in B$, existe $c_{ij} \in A$ tal que

$$\beta_j = \sum_{i=1} c_{ij}\alpha_i,$$

para $j = 1, \ldots, d$. Usando el Lema 1.3.7, la fórmula del producto para los determinantes, y el hecho de que los σ_i son monomorfismos, podemos concluir que

$$d(\beta_1, \ldots, \beta_d) = (\det(c_{ij}))^2 d(\alpha_1, \ldots, \alpha_d).$$

Teorema 1.3.9. *$\mathfrak{d}_{L/K} = N_{L/K}(\mathfrak{D}_{L/K})$, donde $N_{L/K}(\mathfrak{D}_{L/K})$ denota el ideal de A generado por $\{N_{L/K}(x) : x \in \mathfrak{D}_{L/K}\}$.*

El Teorema 1.3.9 nos permite deducir el siguiente corolario.

Corolario 1.3.10. *Sea $\mathfrak{p}$ un ideal primo en A y sean $A_\mathfrak{p}$ y $K_\mathfrak{p}$ las completaciones correspondientes de A y K. De manera similar, para cada ideal primo $\mathfrak{q}$ de L, sea $L_\mathfrak{q}$ la completación de L. Entonces, tenemos la siguiente fórmula del producto para el discriminante:*

$$\mathfrak{d}_{L/K} A_\mathfrak{p} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{d}_{L_\mathfrak{q}/K_\mathfrak{p}}.$$

Estamos interesados en aplicar el resultado anterior a una extensión $K/\mathbb{Q}$ de grado d, con $A = \mathbb{Z}$ y $B = \mathcal{O}_K$. Sea $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ una base íntegra de K sobre $\mathbb{Q}$ y sea $D_{K/\mathbb{Q}} = d(\alpha_1, \ldots, \alpha_d)$ un generador de $\mathfrak{d}_{K/\mathbb{Q}}$. Supongamos que $\beta_1, \ldots, \beta_d$ es otra base íntegra, luego para cierta matriz invertible (c_{ij}) con entradas en $\mathbb{Z}$, podemos escribir

$$\beta_j = \sum_{i=1} c_{ij}\alpha_i.$$

Observar que si (f_{ij}) es la inversa de (c_{ij}), entonces también tenemos

$$\alpha_j = \sum_{i=1} f_{ij}\beta_i \ ;$$

por lo tanto, $f_{ij} \in \mathbb{Z}$. Esto significa que $\det(c_{ij})$ es una unidad de $\mathbb{Z}$, es decir, $\det(c_{ij}) = \pm 1$. Concluimos que para cualquier lugar p de $\mathbb{Q}$, el valor absoluto $\left|D_{K/\mathbb{Q}}\right|_p$ no depende de la base íntegra elegida.

De manera similar, podemos probar que para cualquier $p \in \mathbb{Z}$ y cada lugar v de K sobre p, el ideal discriminante $\mathfrak{d}_{K_v/\mathbb{Q}_p}$ es principal y que el valor absoluto $|\cdot|_p$ de cada generador es el mismo. Primero, sin embargo, necesitamos la siguiente proposición.

Proposición 1.3.11. *Sea L/K una extensión separable finita, sea $A \subset K$ un dominio de Dedekind con* $\mathrm{Frac}(A) = K$ *y sea $B \subset L$ su clausura íntegra en L. Si A es un dominio de ideales principales, entonces cada B-submódulo $M \neq 0$ de L es un módulo libre de A de rango $[L : K]$. En particular, B admite una base íntegra sobre A.*

Demostración. Ver, por ejemplo, [13, Ch. I, (2.10)]. □

De la proposición anterior, se deduce que $\mathcal{O}_v$ es un $\mathbb{Z}_p$-módulo libre. Sea d_v el grado local $[K_v : \mathbb{Q}_p]$, sea $e_1, \ldots, e_{d_v}$ una base íntegra, y sea $D_{K_v/\mathbb{Q}_p} := d(e_1, \ldots, e_{d_v})$. Podemos probar exactamente de la misma forma que antes que $\left|D_{K_v/\mathbb{Q}_p}\right|_p$ no depende de la base íntegra elegida.

Como consecuencia directa de Corolario 1.3.10, tenemos el siguiente resultado, que será esencial para el resto de la tesis.

Proposición 1.3.12. *Sea K un cuerpo de números y $p \in \mathbb{Z}$ un número primo. Sea $D_{K/\mathbb{Q}}$ el discriminante de alguna base íntegra de K, y, para cada lugar $v|p$, sea $D_{K_v/\mathbb{Q}_p}$ el discriminante de alguna base íntegra de K_v. Entonces*

$$\left|D_{K/\mathbb{Q}}\right|_p = \prod_{v|p} \left|D_{K_v/\mathbb{Q}_p}\right|. \tag{1.4}$$

Si en (1.4) tomamos el producto sobre todos los números primos, una simple aplicación de la fórmula del producto da:

Corolario 1.3.13. *Sea K un cuerpo de números. Para cada p y v, sean $D_{K/\mathbb{Q}}$ y $D_{K_v/\mathbb{Q}_p}$ como arriba. Entonces*

$$\left|D_{K/\mathbb{Q}}\right|^{-1} = \prod_{v \text{ finito}} \left|D_{K_v/\mathbb{Q}_p}\right|.$$

1.4. Medida de Haar

1.4.1. Definición y propiedades básicas

Antes de dar la definición de la medida de Haar, recordaremos una serie de definiciones fundamentales de teoría de la medida.

Sea μ una medida de Borel en un espacio de Hausdorff localmente compacto X, y sea E un subconjunto boreliano de X.

- Decimos que μ es **regular exterior** en E si

$$\mu(E) = \text{ínf}\{\mu(U) : U \subset E, U \text{ abierto}\}.$$

- Decimos que μ es **regular interior** en E si

$$\mu(E) = \sup\{\mu(K) : K \subset E, K \text{ compacto}\}.$$

- Una **medida de Radón** en X es una medida de Borel que es finita en todo compacto, regular exterior en todo boreliano y regular interior en todo abierto.

- Sea G un grupo y μ una medida de Borel en G. Decimos que μ es **invariante por traslación a izquierda** si para todo los conjuntos de Borel E de G y para todo $s \in G$,

$$\mu(sE) = \mu(E).$$

  Invariancia por traslación a derecha se define de manera similar.

Definición 1.4.1. Sea G un grupo topológico localmente compacto (notar que pedimos también que sea Hausdorff). Luego, una **medida de Haar a izquierda** (respectivamente, **a derecha**) en G es una medida de Radon μ en G, distinta de cero, que es invariante por traslaciones a izquierda (respectivamente, a derecha). Una medida de Haar **bi-invariante** es una medida de Radón distinta de cero que es invariante a izquierda y a derecha.

Ejemplo. Sea K un cuerpo con una medida de Haar fija μ, y V un espacio vectorial sobre K de dimensión n. Si $T : K^n \to V$ es un isomorfismo K-lineal, entonces tenemos una medida de Haar ν en V definida por

$$\nu(\Omega) := \mu^n(T^{-1}(\Omega)), \tag{1.5}$$

donde μ^n denota la medida producto en K^n. Los conjuntos medibles en (V, ν) son los $\Omega \subset V$ tales que $T^{-1}(\Omega)$ es medible en (K^n, μ^n).

Supongamos que $K = \mathbb{R}$ y μ es la medida de Lebesgue. Sea V un espacio vectorial real de dimensión n. Sean $\alpha_1, \ldots, \alpha_n$ y $\beta_1, \ldots, \beta_n$ dos bases ortonormales de V. Consideramos los isomorfismos E_1 y E_2 de $\mathbb{R}^n$ en V, dados por $E_1(e_i) = \alpha_i$ y $E_2(e_i) = \beta_i$ respectivamente, donde $e_1, \ldots, e_n$ es la base estándar de $\mathbb{R}^n$. Cada E_j define una medida de Haar ν_j en V. Por el teorema de cambio de variables y el hecho de que E_1 y E_2 son transformaciones ortogonales, tenemos

$$\nu_2 = \left|\det(E_2^{-1}E_1)\right|\nu_1 = \nu_1.$$

La discusión anterior nos lleva a adoptar la siguiente convención. Cada vez que hablamos de *la* medida ν de un espacio vectorial real V, nos referimos a aquella definida como en (1.5) con $T : \mathbb{R}^n \to V$ una transformación ortogonal.

Teorema 1.4.2. *Todo grupo localmente compacto admite una medida de Haar a izquierda. Además, esta medida es única salvo múltiplos escalares.*

Demostración. Ver, por ejemplo, [15, 1-8]. □

Recordemos algunas propiedades básicas de la medida de Haar.

En primer lugar, vamos a fijar notación. Sea $\mathcal{C}_c(X)$ el conjunto de funciones continuas de soporte compacto de X en $\mathbb{R}$, y sea

$$\mathcal{C}_c^+(X) := \{f \in \mathcal{C}_c(X) \setminus \{0\} : f(x) \geq 0 \; \forall x \in X\}.$$

Si $A \subset X$, χ_A denota la función característica de A.

Proposición 1.4.3. *Sea G un grupo compacto local con una medida de Radón no nula μ Entonces:*

(I) *La medida μ es una medida Haar a izquierda en G si y solo si la medida $\tilde{\mu}$ definida por $\tilde{\mu}(E) = \mu(E^{-1})$ es una medida de Haar a derecha en G.*

(II) *La medida μ es una medida Haar a izquierda en G si y solo si*

$$\int_G L_s f d\mu = \int_G f d\mu$$

para toda $f \in \mathcal{C}_c^+(G)$; donde $L_s : G \to G$, $L_s(g) = sg$.

(III) *Si μ es una medida Haar a izquierda en G, entonces μ es positivo en todo subconjunto abierto no vacío de G y*

$$\int_G f d\mu > 0$$

para toda $f \in \mathcal{C}_c^+(G)$.

(IV) *Si μ es una medida Haar a izquierda en G, entonces $\mu(G)$ es finito y solo si G es compacto.*

Demostración. Ver, por ejemplo, [15, 1-7]. □

1.4.2. Medida de Haar en adeles

La medida de Haar en el anillo de adeles es esencialmente la única medida que se restringe a la medida producto en cada $(K_{\mathbb{A}})_S$. Formalmente, esto es:

Proposición 1.4.4. *Sea $K_{\mathbb{A}}$ el anillo de adeles del cuerpo de números K. Para cada lugar v, sea μ_v la medida de Haar en la completación K_v, normalizada para que*

$$\mu_v(\mathcal{O}_v) = c_v$$

para todo lugar finito v, donde $\{c_v : v \text{ es finito}\}$ es un conjunto de números reales positivos tales que el producto infinito $\prod_{v\nmid\infty} c_v$ converge. Entonces, hay una única medida de Haar μ en $K_{\mathbb{A}}$ que cumple que para cada subconjunto finito S de lugares de K que contienen a todos los lugares infinitos, la restricción μ_S de μ sobre

$$(K_{\mathbb{A}})_S = \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v$$

es precisamente la medida producto.

Demostración. Ver, por ejemplo, [15, 5-5]. □

La siguiente proposición nos dice cómo integrar algunas funciones "buenas" en $K_{\mathbb{A}}$ con respecto a esta medida. Denotamos $\mu = \prod_v \mu_v$ a la medida de Haar del anillo de adeles $K_{\mathbb{A}}$, y $\mu_S = \prod_{v\in S} \mu_v \times \prod_{v\notin S} \mu_v|_{\mathcal{O}_v}$.

Proposición 1.4.5. *Sea $K_{\mathbb{A}}$ el anillo de adeles con medida inducida μ como se indica arriba.*

(a) Sea f una función integrable en $K_{\mathbb{A}}$. Considerar la red

$$\left\{ \int_{(K_{\mathbb{A}})_S} f(g_S) d\mu_S(g_S) \right\}_S$$

indexada en los subconjuntos de lugares que contienen todos los lugares infinitos, equipados con el orden habitual dado por la inclusión. Entonces

$$\int_{K_{\mathbb{A}}} f(g) d\mu(g) = \lim_S \int_{(K_{\mathbb{A}})_S} f(g_S) d\mu_S.$$

Esta igualdad sigue valiendo si sólo se asume que f es continuo, siempre que permitamos que la integral tome valores infinitos.

(b) Sea S_0 un conjunto finito de lugares de K que contiene todos los lugares infinitos. Supongamos que por cada lugar v tenemos una función integrable y continua f_v en K_v, de manera que $f_v|_{\mathcal{O}_v} = 1$ para todo $v \notin S_0$. Para $g = (g_v)_v \in K_{\mathbb{A}}$, definimos la función producto

$$f(g) = \prod_v f_v(g_v)\,.$$

f está bien definido y es continuo en $K_{\mathbb{A}}$. Si S es un subconjunto de lugares que incluye S_0, entonces

$$\int_{(K_{\mathbb{A}})_S} f(g_S)d\mu_S(g_S) = \prod_{v\in S}\left(\int_{K_v} f_v(g_v)d\mu_v(g_v)\right).$$

Además,

$$\int_{K_{\mathbb{A}}} f(g)d\mu(g) = \prod_v \left(\int_{K_v} f_v(g_v)d\mu_v(g_v)\right),$$

y, si el lado derecho es finito, entonces f es integrable.

Demostración. Ver, por ejemplo, [15, 5-6]. □

La siguiente proposición y los subsiguientes corolarios nos dicen que tenemos un teorema de cambio de variables para cualquier completación de un cuerpo de números y, por lo tanto, también para el anillo de adeles.

Proposición 1.4.6. *Sea K un cuerpo de números y K_v su completación con respecto a un lugar finito v sobre el primo p. Sea μ una medida de Haar de K_v. Luego, para cada $x \in K_v$ y cada conjunto medible $U \subset K_v$, tenemos*

$$\mu(xU) = \|x\|_v\,\mu(U).$$

Demostración. La proposición es claramente cierta para $x = 0$, por lo que siempre podemos suponer que $x \neq 0$ si es necesario. Para cada $x \in K_v$, la aplicación

$$\Phi_x : y \in K_v \mapsto xy \in K_v$$

es un automorfismo de K_v, por lo que la composición $\mu_x = \mu \circ \Phi_x$ es una medida de Haar en K_v. Por lo tanto, μ_x es un múltiplo de μ, digamos $\mu_x = \lambda_x\mu$. Definimos la función $\chi : K_v \to \mathbb{R}_{\geq 0}$ como

$$\chi(x) := \lambda_x = \frac{\mu_x(\mathcal{O}_v)}{\mu(\mathcal{O}_v)}.$$

Esta función es multiplicativa. En efecto, para cualquier $x, y \in K_v$ tenemos

$$\chi(xy) = \frac{\mu_{xy}(\mathcal{O}_v)}{\mu(\mathcal{O}_v)} = \frac{\mu_x(y\mathcal{O}_v)}{\mu(\mathcal{O}_v)} = \frac{\chi(x)\mu_y(\mathcal{O}_v)}{\mu(\mathcal{O}_v)} = \frac{\chi(x)\chi(y)\mu(\mathcal{O}_v)}{\mu(\mathcal{O}_v)} = \chi(x)\chi(y).$$

Ahora tenemos que probar que $\chi(x) = \|x\|_v$. Dado que tanto χ como $\|\cdot\|_v$ son multiplicativos, basta con considerar $x \in \mathcal{O}_v$. Como v es finito, $\mathcal{O}_v$ es discreto y, por lo tanto, el ideal principal generado por x se puede escribir como

$$x\mathcal{O}_v = (\mathfrak{m}_v)^{\operatorname{ord}(x)}. \tag{1.6}$$

El cuerpo residual $\mathcal{O}_v/\mathfrak{m}_v$ es finito, por lo tanto, $\mathcal{O}_v/x\mathcal{O}_v$ también es finito. Además, el número de elementos de $\mathcal{O}_v/x\mathcal{O}_v$ es

$$|\mathcal{O}_v/x\mathcal{O}_v| = |\mathcal{O}_v/\mathfrak{m}_v|^{\operatorname{ord}(x)}.$$

Escribiendo $\mathcal{O}_v$ como una unión disjunta finita de cosets de $x\mathcal{O}_v$, tenemos que

$$\mu(\mathcal{O}_v) = |\mathcal{O}_v/x\mathcal{O}_v|\,\mu(x\mathcal{O}_v) = |\mathcal{O}_v/x\mathcal{O}_v|\,\chi(x)\,\mu(\mathcal{O}_v).$$

Entonces,

$$\chi(x) = |\mathcal{O}_v/x\mathcal{O}_v|^{-1} = |\mathcal{O}_v/\mathfrak{m}_v|^{-\operatorname{ord}(x)}.$$

Resta ver que $\|x\|_v = |\mathcal{O}_v/\mathfrak{m}_v|^{-\operatorname{ord}(x)}$ por cada $x \in K_v$. Sea $|\cdot|_1$ la aplicación definida por

$$x \in K_v \mapsto |x|_1 := |\mathcal{O}_v/\mathfrak{m}_v|^{-\operatorname{ord}(x)} = p^{-f_v \operatorname{ord}(x)},$$

donde $f_v = [\mathcal{O}_v/\mathfrak{m}_v : \mathbb{F}_p]$ es el grado residual y $\operatorname{ord}(x)$ es el único exponente r para el cual $x\mathcal{O}_v = \mathfrak{m}_v^r$. Es fácil ver que esta aplicación define un valor absoluto en K_v, y que dado $x \in K_v$, $|x|_1 < 1$ si y solo si $\|x\|_v < 1$. Por Proposición 1.1.3, hay un número real $s > 0$ tal que por cada $x \in K_v$,

$$\|x\|_v = |x|_1^s.$$

Considere el caso $x = p$. Por un lado, tenemos

$$\|p\|_v = \left|p^{d_v}\right|_p = p^{-d_v},$$

donde d_v es el grado local $[K_v : \mathbb{Q}_p]$. Por otra parte,

$$|x|_1 = p^{-f_v \operatorname{ord}(p)} = p^{-f_v e_v},$$

donde e_v es el índice de ramificación de v en p. Pero, por Lema 1.1.8, $f_v e_v = d_v$. Por lo tanto, $s = 1$ y $\|\cdot\|_v = |\cdot|_1$. □

Corolario 1.4.7. *Sea K un cuerpo de números y sea K_v su completación con respecto a un lugar finito v. Sea μ una medida de Haar de K_v y sea μ^n la medida producto de K_v^n. Si $T : K_v^n \to K_v^n$ es un isomorfismo lineal de K_v, entonces para cualquier conjunto medible $\Omega \subset K_v^n$ tenemos*

$$\mu^n(T\Omega) = \|\det T\|_v \, \mu^n(\Omega).$$

Demostración. Solo hay que adaptar la prueba del teorema de cambio de variables en $\mathbb{R}^n$. La observación clave es que basta probar el resultado para matrices elementales, y esto se desprende fácilmente de Proposición 1.4.6 mediante el uso del teorema de Fubini. Para una prueba del caso real, ver, por ejemplo, [1, Th. 15.12]. □

Medida de Haar normalizada en el anillo de adeles de un cuerpo de números

Sea K un cuerpo de números. Para cada completación K_v, sea β_v la única medida de Haar que satisface lo siguiente:

- Si v es no archimedeano, entonces

$$\beta_v(\mathcal{O}_v) = \left|D_{K_v/\mathbb{Q}_p}\right|_p^{1/2},$$

  donde $D_{K_v/\mathbb{Q}_p}$ es el discriminante.

- Si $v|\infty$ y $K_v = \mathbb{R}$, entonces β_v es la medida de Lebesgue en $\mathbb{R}$.

- Si $v|\infty$ y $K_v = \mathbb{C}$, entonces β_v es dos veces la medida de Lebesgue en el plano complejo.

Por Proposición 1.4.4, la medida de Haar β_v induce una única medida de Haar β en $K_{\mathbb{A}}$. Llamamos a β_v y β las **medidas de Haar normalizadas** de K_v y $K_{\mathbb{A}}$ respectivamente.

Como consecuencia del Corolario 1.4.7, obtenemos:

Corolario 1.4.8. *Sea K un cuerpo de números y sea K_v su completación con respecto a un lugar v. Sea $K_{\mathbb{A}}$ el anillo de adeles, y sea n un entero positivo. Si T es una matriz invertible de tamaño $n \times n$ con entradas en $K_{\mathbb{A}}$, entonces para cualquier conjunto medible $\Omega \subset K_{\mathbb{A}}^n$ tenemos*

$$\beta^n(T\Omega) = \left(\prod_{v \in M_K} \|\det T\|_v\right) \beta^n(\Omega). \tag{1.7}$$

Demostración. Claramente, basta demostrar que (1.7) se satisface si $\Omega = \prod_v \mathcal{O}_v^n$. Por Proposición 1.4.5 (b), sólo necesitamos probar que, por cada $v \in M_K$,

$$\beta_v^n(T\mathcal{O}_v^n) = \|\det T\|_v \, \beta_v^n(\mathcal{O}_v^n).$$

Si v es finito, esto es exactamente lo que afirma el Corolario 1.4.7. Si v es infinito, esto es una consecuencia del teorema de cambio de variables clásico. □

1.4.3. Medida de Haar en cocientes

Sea G un grupo localmente compacto y H un subgrupo normal cerrado de G (en particular, es localmente compacto). Sea $\pi : G \to G/H$ el morfismo cociente. Equipamos G/H con la topología de cociente; es decir, un subconjunto $U \subset G/H$ es abierto si y sólo si $\pi^{-1}(U)$ es abierto en G. Recordar que π es entonces una función abierta y continua, por lo que G/H es localmente compacto (y, por lo tanto, admite una medida de Haar).

La siguiente proposición relaciona las medidas de Haar de G, H y G/H.

Proposición 1.4.9. *Si μ_G y μ_H son medidas de Haar en G y H respectivamente, entonces existe una única medida en Haar $\mu_{G/H}$ en G/H tal que*

$$\int_G f(x) d\mu_G(x) = \int_{G/H} \left(\int_H f(xy) d\mu_H(y) \right) d\mu_{G/H}(\pi(x))$$

para toda función compleja continua f con soporte compacto. Además, esta fórmula sigue siendo válida para cualquier función μ_G-integrable en G.

Demostración. Ver, por ejemplo, [12, pp. 86-87]. □

Recordar que K es discreto en $K_{\mathbb{A}}$, por lo que su medida de Haar es la medida de contar. Además, recordar que $K_{\mathbb{A}}/K$ es compacto, lo que significa que tiene medida de Haar finita. Consideremos ahora la medida de Haar $\beta_{K_{\mathbb{A}}/K}$ en $K_{\mathbb{A}}/K$, inducida por la medida de Haar normalizada de $K_{\mathbb{A}}$ y la medida de contar de K. Luego tenemos el siguiente resultado:

Proposición 1.4.10. *El volumen de $K_{\mathbb{A}}/K$ con respecto a la medida de Haar $\beta_{K_{\mathbb{A}}/K}$ es de* 1.

Demostración. Recordar que β denota la medida de Haar normalizada de $K_{\mathbb{A}}$. Por la Proposición 1.4.9 y el Lema 1.2.3, tenemos

$$\begin{aligned}\beta(\Omega) &= \int_{K_{\mathbb{A}}} \chi_\Omega(z) d\beta(z) \\ &= \int_{K_{\mathbb{A}}/K} \left(\sum_{y \in K} \chi_\Omega(x+y) \right) d\beta_{K_{\mathbb{A}}/K}(K+x) \\ &= \beta_{K_{\mathbb{A}}/K}(K_{\mathbb{A}}/K).\end{aligned}$$

Por definición de la medida adélica normalizada, y el Corolario 1.3.13,

$$\beta(\Omega) = \left(\prod_{v|\infty} \beta_v(\Omega_\infty) \right) \left(\prod_{v \text{ finito}} \left| D_{K_v/\mathbb{Q}_p} \right|_p^{1/2} \right) = \left| D_{K/\mathbb{Q}} \right|^{-1/2} \tag{1.8}$$

Sea $d = [K : \mathbb{Q}]$, y denotemos por r y s al número de lugares reales y complejos de K respectivamente. Recordemos que $d = r + 2s$. Para cada lugar infinito v de K, sabemos que $K_v = \mathbb{R}$ o $K_v = \mathbb{C}$. En cualquier caso, por el Teorema 1.1.10, por cada completación K_v tenemos un embedding $K \hookrightarrow K_v$. Sean $\sigma_1, \ldots, \sigma_d$ todos los embeddings de K en $\mathbb{C}$, con $\sigma_1, \ldots, \sigma_r$ siendo los embeddings reales, y el resto los embeddings complejos, enumerados de forma que $\sigma_{r+s+j} = \overline{\sigma_{r+j}}$ para $j = 1, \ldots, s$.

Por Corolario 1.1.11, tenemos $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v|\infty} K_v \cong \mathbb{R}^d$, que es un isomorfismo de espacios vectoriales reales. Además, si $\omega_1, \ldots, \omega_d$ es una base $\mathbb{Z}$ de $\mathcal{O}_K$, podemos dar esta identificación explícitamente asignando cada elemento básico $\omega_j \otimes 1 \in K \otimes_{\mathbb{Q}} \mathbb{R}$ a un vector $\nu(\omega_j) \in \mathbb{R}^d$ definido por

$$\nu(\alpha) := (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}(\sigma_{r+1}(\alpha)),\ \mathrm{Im}(\sigma_{r+1}(\alpha)), \ldots, \mathrm{Re}(\sigma_{r+s}(\alpha)), \mathrm{Im}(\sigma_{r+s}(\alpha)))$$

para cada $\alpha \in K$.

A través de esta identificación, Ω_∞ corresponde al paralelepípedo d-dimensional generado por los $\nu(\omega_j)$, por lo que su volumen con respecto a la medida de Lebesgue en $\mathbb{R}^d$ es

$$\left| \det \left(\nu(\omega_1) \cdots \nu(\omega_d) \right) \right| = 2^{-s} \left| \det \left(\sigma_i(\omega_j) \right) \right|.$$

Recordar que para lugares complejos, la medida β_v es dos veces la medida de Lebesgue, con lo cual

$$\beta(\Omega_\infty) = \left| \det \left(\sigma_i(\omega_j) \right) \right| = \left| D_{K/\mathbb{Q}} \right|^{1/2}. \tag{1.9}$$

Combinando (1.8) y (1.9), obtenemos

$$\beta(\Omega) = 1\,,$$

lo que concluye la prueba. □

Definición 1.4.11. $\beta_{K_{\mathbb{A}}/K}$ es la **medida normalizada en el cociente** $K_{\mathbb{A}}/K$.

1.5. Alturas

1.5.1. Altura de un vector

Sea K un cuerpo de números. Para cada lugar v en K, sean $|\cdot|_v$ y $\|\cdot\|_v$ los valores absolutos normalizados correspondientes a v. Si $x = (x_1, \ldots, x_N) \in K^N$, definimos

$$|x|_v = \max_n |x_n|_v.$$

Definición 1.5.1. La **altura homogénea** del vector $x \in K^N$ es

$$h(x) = \prod_v |x|_v,$$

donde el producto se toma sobre todos los lugares v de K.

La **altura inhomogénea** de x es

$$h_{in}(x) = \prod_v \max\{1, |x|_v\}.$$

En esta tesis, cuando decimos solamente *altura*, nos referimos a la altura homogénea.

Observación. La altura homogénea corresponde a la altura proyectiva del vector x cuando visto como un elemento del espacio proyectivo $\mathbb{P}_K^{N-1}$, mientras que la altura inhomogénea corresponde a la altura proyectiva del vector x visto como un elemento del espacio afín N-dimensional embebido en $\mathbb{P}_K^N$.

Una simple aplicación de la fórmula del producto da el siguiente resultado:

Proposición 1.5.2. *Si $x \in K^N$ y $a \in K$, entonces $h(ax) = h(x)$.*

1.5.2. Altura de una matriz

Ahora definimos la altura de una matriz $M \times N$ con entradas en K y rango $M < N$. Sea $X = (x_{mn})$ una matriz de este tipo. Si $J \subset \{1, 2, \ldots, n\}$ es un subconjunto con $|J| = M$ elementos, escribimos X_J para la submatriz de X formada por las columnas j-ésimas, para $j \in J$; es decir

$$X_J = (x_{mn})_{m\in\{1,\ldots,M\},\, n\in J} \ .$$

Definición 1.5.3 (Altura local)**.** Sea X una matriz como arriba. Para cada lugar v de K definimos la **altura local** $H_v(X)$ de la siguiente manera:

(a) Si v es finito, $H_v(X) = \text{máx}\{|\det X_J|_v : |J| = M\}$,

(b) Si v es real, $H_v(X) = |\det XX^t|_v^{\frac{1}{2}}$, donde X^t es la matriz traspuesta de X.

(c) Si v es complejo, $H_v(X) = |\det XX^*|_v^{\frac{1}{2}}$, donde X^* es el matrix conjugada traspuesta de X.

Por la fórmula de Cauche-Binet, para $v \mid \infty$, (b) y (c) son equivalentes a:

(d) $H_v(X) = \left(\sum_{|J|=M} |\det X_J|^2\right)^{\frac{d_v}{2d}}$, donde $d = [K : \mathbb{Q}]$, $d_v = [K_v : \mathbb{Q}_\infty]$ y $|\cdot|$ es el valor absoluto euclidiano habitual en $\mathbb{R}$ o $\mathbb{C}$.

Por completitud, recordamos la fórmula de Cauchy-Binet.

Lema 1.5.4 (Cauchy-Binet)**.** *Sea A una matriz $M \times N$ y B una matriz $N \times M$, y sea $J \subset \{1, \ldots, N\}$ un subconjunto con elementos M. Denotamos por A_J a la matriz $M \times N$ formada las columnas $j \in J$ de A y por B_J a la matriz $M \times M$ formada por las filas $i \in J$ de B. Entonces,*

$$\det(AB) = \sum_{|J|=M} \det(A_J)\det(B_J)\,.$$

Definición 1.5.5 (Altura global)**.** Sea X una matriz de $M \times N$ con entradas en K y rango $M < N$. El producto de las alturas locales $H_v(X)$ sobre todos los lugares de K define la **altura global** $H(X)$. Concretamente,

$$H(X) := \prod_v H_v(X)\,.$$

En los próximos capítulos, necesitaremos algunas propiedades de la altura global, que se pueden probar usando álgebra lineal elemental.

Proposición 1.5.6. *Si C es una matriz no singular de tamaño $M \times M$ sobre K, entonces*

$$H(CX) = \left(\prod_v |\det C|_v \right) H(X) = H(X).$$

Proposición 1.5.7. *Supongamos que $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$ se parte en bloques que consisten en una matriz X_1 de tamaño $M_1 \times N$ y una matriz X_2 de tamaño $M_2 \times N$. Luego, para cada lugar v de K tenemos*

$$H_v(X) \leq H_v(X_1) H_v(X_2).$$

Por lo tanto, también vale que

$$H(X) \leq H(X_1) H(X_2).$$

Observación. Podemos extender fácilmente nuestras definiciones a matrices X de tamaño $M \times N$ con rango $N < M$, definiendo

$$H_v(X) := H_v(X^t).$$

Como observación final, vemos que tanto la altura de un vector como la altura de una matriz no dependen del cuerpo K en que vemos las coordenadas del vector o la matriz. Formalmente, esto significa:

Proposición 1.5.8. *Sea K un cuerpo de números y F una extensión finita de K. Escribimos M_K y M_F para el conjunto de lugares de K y F respectivamente.*

- *Si $x \in K^N$, entonces la altura de x con respecto a K es igual a la altura de x con respecto a F, es decir,*

$$\prod_{v \in M_K} |x|_v = \prod_{w \in M_F} |x|_w.$$

- *Si $A \in K^{M \times N}$, entonces la altura de A con respecto a K es igual a la altura de A con respecto a F, es decir,*

$$\prod_{v \in M_K} H_v(A) = \prod_{w \in M_F} H_w(A),$$

donde H_v y H_w indican las alturas locales correspondientes.

Demostración. Esta proposición es una consecuencia directa del Lema 1.1.15. □

Capítulo 2

Segundo teorema de Minkowski

2.1. En el espacio euclidiano

En esta sección, recordaremos algunas definiciones y resultados básicos de geometría de números clásica sobre espacios vectoriales reales. En la siguiente sección los generalizaremos en el contexto de adeles.

Definición 2.1.1. Sea Λ un subgrupo aditivo de un espacio vectorial real V de dimensión finita. Decimos que es un **$\mathbb{R}$-lattice** (o simplemente un **lattice**) si satisface alguna de las siguientes condiciones equivalentes:

(a) Λ es discreto en V y contiene una $\mathbb{R}$-base de V.

(b) Λ es discreto en V y el grupo cociente V/Λ es compacto.

(c) Λ tiene una $\mathbb{Z}$-base que también es una $\mathbb{R}$-base de V.

Dado un espacio vectorial real V de dimensión n, siempre podemos fijar una base $\{v_1, \ldots, v_n\}$ e identificarlo con $\mathbb{R}^n$ a través del isomorfismo algebraico (y topológico) dado por

$$e_i \in \mathbb{R}^n \longmapsto v_i \in V, \quad i = 1, \ldots, n \ ,$$

donde e_i es el vector con i-ésima coordenada igual a 1 y el resto igual a cero.

Por lo tanto, nos limitaremos a estudiar lattices en el espacio euclidiano $V = \mathbb{R}^N$.

Definición 2.1.2. Sea Λ un lattice en $\mathbb{R}^N$. Sea T un isomorfismo $\mathbb{R}$ que manda Λ a $\mathbb{Z}^N$. Definimos el **volumen** o **determinante** de Λ como $\det(\Lambda) := \det T$. También se denota $\mathrm{vol}(\Lambda)$.

Observación. El volumen del lattice Λ no depende de la transformación T elegida. De hecho, $\det(\Lambda) = \mathrm{vol}(\mathbb{R}^N/\Lambda)$, donde el volumen en el cociente se toma con respecto a la única medida de Haar inducida por la medida de Lebesgue (ver Proposición 1.4.9).

Un problema básico en la geometría de los números es determinar la existencia de puntos lattice en conjuntos convexos y, más precisamente, estimar cuántos hay. Recordamos dos teoremas de Minkowski que dan algunos resultados en esta dirección.

Teorema 2.1.3 (Primer teorema de Minkowski)**.** *Sea Λ un lattice en $\mathbb{R}^N$, y sea S un subconjunto no vacío, convexo, acotado y simétrico (es decir, $S = -S$) de $\mathbb{R}^N$. Si $\mathrm{vol}(S) > 2^n \det(\Lambda)$, entonces existe un punto lattice $P \neq 0$ en S (es decir, $P \in \Lambda \cap S$).*

Este primer teorema, también conocido como el Teorema del cuerpo convexo de Minkowski, se generaliza con el segundo teorema, que esencialmente da una cota de cuánto tenemos para expandir un cuerpo convexo para que contenga una base de $\mathbb{R}$ formada por puntos lattice.

Antes de enunciar el teorema, debemos recordar la siguiente definición.

Definición 2.1.4 (Mínimos sucesivos)**.** Sea S un subconjunto acotado simétrico convexo abierto no vacío de $\mathbb{R}^N$, y sea Λ un $\mathbb{R}$-lattice. Para $n = 1, \ldots, N$, el **n-ésimo mínimo sucesivo** es

$$\lambda_n := \text{ínf}\left\{t > 0 : tS \text{ contiene } n \text{ vectores de } \Lambda \text{ linealmente independientes sobre } \mathbb{R}\right\}.$$

Se puede verificar que

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N < \infty.$$

Observación. Claramente, para cualquier $t > 0$, el conjunto $tS \cap \Lambda$ es relativamente compacto en $\mathbb{R}^N$; por lo tanto es finito. Además, la clausura de $\lambda_n S$ es la intersección de todos los λS con $\lambda > \lambda_n$. Estos dos hechos nos permiten deducir que esta clausura contiene n puntos lattice linealmente independientes.

Teorema 2.1.5 (Segundo teorema de Minkowski)**.** *Manteniendo la notación anterior, tenemos que*

$$\frac{2^N}{N!} \det(\Lambda) \leq \lambda_1 \lambda_2 \cdots \lambda_N \ \mathrm{vol}(S) \leq 2^N \det(\Lambda).$$

Repasemos brevemente las ideas principales de la demostración por Davenport y Estermann de la cota superior, que luego adaptaremos al contexto adélico. El primer paso consiste en darse cuenta de que, mediante una transformación lineal, podemos suponer que $\Lambda = \mathbb{Z}^N$ y, además, que por cada $n = 1, \dots, N$ la clausura de $\lambda_n S$ contiene los primeros n elementos de la base estándar $\{e_1, \dots, e_N\}$ de $\mathbb{R}^N$. A partir de aquí, se puede concluir que el segundo teorema de Minkowski es una consecuencia directa del siguiente teorema, que fue utilizado implícitamente por Davenport en [4] y formalmente enunciado por Estermann en [6].

Teorema 2.1.6 (Teorema de Davenport-Estermann)**.** *Sean $0 < \mu_1 \leq \mu_2 \leq \cdots \leq \mu_N$ y sea S un conjunto convexo en $\mathbb{R}^N$ con la siguiente propiedad: para cualquier $n \in \{1, \dots, N\}$ y cualquier par de puntos $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n)$ en $\mu_n S$ con $x - y \in \mathbb{Z}^N$, tenemos que $x_j = y_j$ para todo $j \in \{n, n+1, \dots, N\}$. Entonces*

$$\mu_1 \mu_2 \dots \mu_N \operatorname{vol}(S) \leq 1.$$

Observación. Por cada n, podemos tomar μ_n como el máximo de todos los $\mu \geq 0$ que cumplen que si $x, y \in \mu S$ entonces $x_n = y_n, \dots, x_N = y_N$.

Damos ahora un resumen de la prueba de Estermann del Teorema 2.1.6.

Definición 2.1.7. Para $t \in \mathbb{R}$, sea $\pi(t) = t - [t]$. Si $x = (x_1, \dots, x_N) \in \mathbb{R}^N$, para cada $n \in \{1, \dots, N\}$, definimos

$$\varphi_n(x) := (x_1, x_2, \dots, x_{n-1}, \pi(x_n), x_{n+1}, \dots, x_N)$$

y

$$\Phi_n(x) := (\pi(x_1), \dots, \pi(x_n), x_{n+1}, \dots, x_N).$$

Observar que $\varphi_{n+1} \circ \Phi_n = \Phi_{n+1}$.

Los puntos clave del argumento son los siguientes lemas.

Lema 2.1.8 ([6, Lemma 3])**.** *Sea S un conjunto convexo en $\mathbb{R}^N$, y sean $1 \leq n \leq N$ y $\mu \geq 1$. Luego*

$$\operatorname{vol}(\Phi_n(\mu S)) \geq \mu^{N-n} \operatorname{vol}(\Phi_n(S)).$$

Lema 2.1.9 ([6, Lemma 4])**.** *Sea T un conjunto medible en $\mathbb{R}^N$, sea $1 \leq n \leq N$. Supongamos que T no contiene ningún par de puntos x e y con $x - y \in \mathbb{Z}^N$ que difieren sólo en su*

coordenada n-ésima, es decir, puntos $(x_1, \dots, x_N)$ *y* $(x_1, \dots, x_{n-1}, x_n + m, x_{n+1}, \dots, x_N)$, *donde* $m \in \mathbb{N}$. *Entonces*

$$\mathrm{vol}(\varphi_n(T)) = \mathrm{vol}(T).$$

Observación. Veremos que, de hecho, este lema se usa en la forma

$$\mathrm{vol}(\Phi_{n+1}(\mu_n S))) = \mathrm{vol}(\Phi_n(\mu_n S)).$$

Para $n = 1, \dots, N$, podemos usar el Lema 2.1.8 con $\mu = \frac{\mu_{n+1}}{\mu_n}$ y el Lema 2.1.9 con $T = \Phi_n(\mu_n S)$ para probar que

$$\mathrm{vol}(\Phi_{n+1}(\mu_{n+1} S)) \geq \left(\frac{\mu_{n+1}}{\mu_n}\right)^{N-n} \mathrm{vol}(\Phi_n(\mu_n S))$$

Iterando, obtenemos

$$\mathrm{vol}(\Phi_N(\mu_N S)) \geq \left(\prod_{n=1}^{N-1} \frac{\mu_{n+1}}{\mu_n}\right)^{N-n} \mathrm{vol}(\Phi_1(\mu_1 S)).$$

Cada elemento de $\Phi_N(\mu_N S)$ tiene todas sus coordenadas de valor absoluto menor o igual a uno, por lo que

$$\mathrm{vol}(\Phi_N(\mu_N S)) \leq 1.$$

Además, utilizando Lema 2.1.9 y las propiedades de la medida de Lebesgue, tenemos

$$\mathrm{vol}(\Phi_1(\mu_1 S)) \geq \mu_1^N \,\mathrm{vol}(S).$$

Concluimos que

$$\mu_1 \mu_2 \dots \mu_N \,\mathrm{vol}(S) \leq 1.$$

2.2. En el anillo de adeles

En toda esta sección, K denota un cuerpo de números de grado d, N un entero positivo y M_K la familia de todos los lugares de K. Como siempre, K_v denota la completación de K con respecto al lugar $v \in M_K$. Por último, sean $E = K^N$, $E_v = K_v^N$, $E_\infty = \prod_{v|\infty} K_v^N$ y $E_{\mathbb{A}} = K_{\mathbb{A}}^N$.

Primero, vamos a generalizar la noción de lattice a los cuerpos K y K_v.

Definición 2.2.1. Dado un lugar finito v de K, un **K_v-lattice** en E_v es un $\mathcal{O}_v$-submódulo abierto y compacto de E_v.

Ejemplo. $\mathcal{O}_v^N$ es claramente K_v-lattice en E_v.

Proposición 2.2.2. *Sea Λ_v un $\mathcal{O}_v$-submódulo de E_v. Entonces las siguientes afirmaciones son equivalentes:*

(I) *Λ_v es un K_v-lattice en E_v.*

(II) *Λ es un $\mathcal{O}_v$-módulo finitamente generado que genera a E_v como espacio vectorial sobre K_v.*

Demostración. Ver, por ejemplo, [2, Prop. C.2.2]. □

Definición 2.2.3. Un **K-lattice** en E es un $\mathcal{O}_K$-submódulo de E que genera a E como espacio vectorial sobre K.

Ejemplo. $(\mathcal{O}_K)^N$ es un K-lattice en E.

Hay un tipo de principio local-global que relaciona K-lattices y K_v-lattices.

Proposición 2.2.4. *Los K-lattices se pueden caracterizar de la siguiente forma:*

(a) Sea Λ en E y, para cada lugar finito v de K, sea Λ_v su clausura topológica en E_v. Luego, para cada v, Λ_v es un K_v-lattice. Además, se tiene que $\Lambda_v = \mathcal{O}_v^N$ para casi todo v.

(b) Recíprocamente, si para cada lugar finito v tenemos un K_v-lattice Λ_v en E_v con $\Lambda_v = \mathcal{O}_v^N$ para casi todo v, entonces hay un K-lattice Λ tal que Λ_v es la clausura de Λ en E_v. Además, tenemos que $\Lambda = \bigcap_{v \text{ finito}}(E \cap \Lambda_v)$.

Demostración. Ver, por ejemplo, [2, Prop. C.2.6]. □

Proposición 2.2.5. *La imagen Λ_∞ del K-lattice Λ por el embedding diagonal $E \hookrightarrow E_\infty$ es un $\mathbb{R}$-lattice.*

Demostración. Ver, por ejemplo, [2, Prop. C.2.6]. □

Ahora, generalizamos el segundo teorema de Minkowski.

Definimos la multiplicación de $x = (x_v) \in K_{\mathbb{A}}$ por un número real λ como el elemento $\lambda x \in K_{\mathbb{A}}$ dado por

$$(\lambda x)_v := \begin{cases} \lambda x_v \text{ si } v \text{ es arquimediano} \\ x_v \text{ si } v \text{ es no arquimediano}\,. \end{cases}$$

Si $x = (x_1, \ldots, x_N) \in E_{\mathbb{A}} = K_{\mathbb{A}}^N$, y $\lambda \in \mathbb{R}$, definimos

$$\lambda x := (\lambda x_1, \ldots, \lambda x_N) \in E_{\mathbb{A}}.$$

Para cada $v|\infty$, consideramos un subconjunto convexo acotado simétrico abierto no vacío S_v de K_v. Como en la sección anterior, simétrico significa que $S_v = -S_v$. Sea Λ un K-lattice y, para cada lugar finito $v \in M_K$, sea Λ_v su clausura en K_v. Sea S el producto de los S_v y Λ_v; esto es

$$S := \prod_{v|\infty} S_v \times \prod_{v\nmid\infty} \Lambda_v \subset E_{\mathbb{A}}.$$

Para los subconjuntos de esta forma, podemos definir los mínimos sucesivos como en el caso euclidiano.

Definición 2.2.6. Para $n = 1, \ldots, N$, el **n-ésimo mínimo sucesivo** es

$$\lambda_n := \text{ínf}\left\{t > 0 : tS \text{ contiene } n \text{ vectores de } \Lambda \text{ linealmente independientes sobre } K\right\}.$$

O equivalentemente,

$$\lambda_n = \text{ínf}\left\{t > 0 : (tS) \cap E \text{ contiene } n \text{ vectores linealmente independientes sobre } K\right\}.$$

Notar que

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N < \infty\,.$$

Observación. No es difícil demostrar que, al igual que en el caso euclidiano, $(\lambda S) \cap E$ es discreto y relativamente compacto en $E_{\mathbb{A}}$, y por lo tanto es finito. Además, la clausura de $\lambda_n S$ es igual a la intersección de todos los λS por $\lambda > \lambda_n$, y por lo tanto dicha clausura contiene n vectores de Λ que son linealmente independiente sobre K.

Estamos en condiciones de enunciar el segundo teorema de Minkowski sobre el anillo de adeles de K.

Teorema 2.2.7 (Segundo teorema de Minkowski en adeles)**.** *Sea Λ un K-lattice en E con clausura Λ_v para cada lugar finito $v \in M_K$. Para cada lugar arquimediano v, sea S_v un subconjunto convexo acotado simétrico abierto no vacío de $E_v = K_v^N$. Sea $S = \prod_{v|\infty} S_v \times \prod_{v\nmid\infty} \Lambda_v \subset E_{\mathbb{A}}$. Entonces,*

$$(\lambda_1\lambda_2\cdots\lambda_N)^d \operatorname{vol}(S) \leq 2^{dN},$$

donde el volumen se calcula con respecto a la medida de Haar en $E_{\mathbb{A}}$ dada por el producto de las medidas normalizadas de Haar β en $K_{\mathbb{A}}$.

Más aún, supongamos que para cada lugar complejo v, el conjunto S_v es simétrico en el sentido más fuerte de que $\alpha S = S$ si $|\alpha| = 1$. Si r y s denotan el número de lugares reales y complejos de K respectivamente, tenemos la cota inferior

$$\frac{2^{dN}\pi^{sN}}{((N!)^r((2N)!)^s}\left|D_{K/\mathbb{Q}}\right|^{-N/2} \leq (\lambda_1\lambda_2\cdots\lambda_N)^d \operatorname{vol}(S),$$

donde $D_{K/\mathbb{Q}}$ es el discriminante de alguna base íntegra de $K/\mathbb{Q}$.

La parte más difícil es la prueba respecta a la cota superior, y consiste en una generalización de los argumentos de Davenport y Estermann discutidos en la sección anterior. El primer paso entonces es adaptar el Teorema 2.1.6.

Sea Λ un K-lattice, y sea T_v un conjunto abierto convexo (no necesariamente simétrico) no vacío en E_v. Sea $T = \prod_{v|\infty} T_v \times \prod_{v \text{ finito}} \Lambda_v$. Para $n = 1, \ldots, N$, sea μ_n el supremo de todos los $\mu > 0$ tales que si $x, y \in \mu T$ satisfacen que $x - y \in E$, luego $x_j = y_j$ para $j = n, \ldots, N$.

Observación. Se puede probar que

$$0 < \mu_1 \leq \mu_2 \leq \cdots \leq \mu_N < \infty.$$

Teorema 2.2.8 (Teorema de Davenport-Estermann en adeles)**.** *Sean T y $\mu_1, \ldots, \mu_N$ como arriba. Entonces,*

$$(\mu_1\mu_2\cdots\mu_N)^d \operatorname{vol}(T) \leq 1.$$

Nuestro objetivo ahora es generalizar Lema 2.1.8 y Lema 2.1.9, ya que esto nos permitiría reproducir la parte final del argumento de Estermann sin mayores cambios. El primer paso de este proceso es encontrar un análogo a la Definición 2.1.7. Notar que, en un sentido más abstracto, tomar la parte fraccionaria de un número real x se puede pensar

como tomar la clase $\overline{x}$ de x en el cociente $\mathbb{R}/\mathbb{Z}$. En el contexto adélico, el análogo a $\mathbb{R}$ es intuitivamente $K_{\mathbb{A}}$ y el análogo a $\mathbb{Z}$ es el subgrupo discreto K. Por lo tanto, hacemos la siguiente definición.

Definición 2.2.9. Para cada $n = 1, \ldots, N$, definimos el homomorfismo

$$\Phi_n : E_{\mathbb{A}} = (K_{\mathbb{A}})^N \longrightarrow (K_{\mathbb{A}}/K)^n \times (K_{\mathbb{A}})^{N-n},$$
$$\Phi_n(x_1, \ldots, x_N) = (\overline{x_1}, \ldots, \overline{x_n}, x_{n+1}, \ldots, x_N),$$

donde $\overline{x_j}$ denota la clase de x_j.

Además, para cualquier N-producto H de $K_{\mathbb{A}}$ y $K_{\mathbb{A}}/K$ donde el factor n-ésimo es $K_{\mathbb{A}}$, sea φ_n el homomorfismo en H definido por

$$\varphi_n(x_1, \ldots, x_N) = (x_1, \ldots, x_{n-1}, \overline{x_n}, x_{n+1}, \ldots, x_N).$$

Procedemos a enunciar y probar las versiones adélicas de los lemas de Estermann.

Lema 2.2.10. *Sean T y $\Phi_1, \ldots, \Phi_N$ como arriba. Luego, para $\mu \geq 1$ y $n = 1, \ldots, N$, tenemos que*

$$\operatorname{vol}(\Phi_n(\mu T)) \geq \mu^{d(N-n)} \operatorname{vol}(\Phi_n(T)) \tag{2.1}$$

donde se toma el volumen con respecto a la medida de Haar dada por el producto de las medidas normalizadas en $K_{\mathbb{A}}$ y en el cociente $K_{\mathbb{A}}/K$.

Demostración. Primero, supongamos que $n = N$. Si tomamos un elemento arbitrario $y \in T$, entonces $T - y$ es convexo y contiene al 0. Como $\mu \geq 1$, se sigue que $\mu(Ty) \subset Ty$, y así

$$\operatorname{vol}(\Phi_N(\mu T - \mu y)) \geq \operatorname{vol}(\Phi_N(Ty)).$$

Ahora, dado que Φ_N es un homomorfismo y la medida de Haar es invariante por traslaciones, sabemos que

$$\operatorname{vol}(\Phi_N(\mu T - \mu y)) = \operatorname{vol}(\Phi_N(\mu T))$$

y

$$\operatorname{vol}(\Phi_N(T - y)) = \operatorname{vol}(\Phi_N(T)).$$

Con esto concluye la prueba para el caso $n = N$.

Supongamos que $1 \leq n < N$. Denotamos los elementos de $E_{\mathbb{A}} = (K_{\mathbb{A}})^n \times (K_{\mathbb{A}})^{N-n}$ por (w, y) con $w \in (K_{\mathbb{A}})^n$ y $y \in (K_{\mathbb{A}})^{N-n}$. Para cada $y \in (K_{\mathbb{A}})^{N-n}$, sea

$$T(y) := \{w \in (K_{\mathbb{A}})^n : (w, y) \in T\}.$$

Usando el teorema de Fubini, obtenemos

$$\begin{aligned}\mathrm{vol}(\Phi_n(\mu T)) &= \int_{(K_{\mathbb{A}})^{N-n}} \left(\int_{\Phi_n((\mu T)(y)} d\overline{w} \right) dy \\ &= \int_{(K_{\mathbb{A}})^{N-n}} \mathrm{vol}(\Phi_n((\mu T)(y)))dy\end{aligned}$$

donde dy y $d\overline{w}$ denotan las medidas de Haar en $(K_{\mathbb{A}})^{N-n}$ y $(K_{\mathbb{A}}/K)^n$ respectivamente.

Aplicamos la sustitución $y \to \mu y$. Como la multiplicación por números reales sólo ocurre en los lugares infinitos, para ver cómo esta sustitución afecta a la integral, necesitamos calcular la dimensión de $(K_{\mathbb{A}})_\infty^{N-n} = \prod_{v|\infty}(K_v)^{N-n}$ como espacio vectorial real. Si $d_v = [K_v : \mathbb{R}]$ es el grado local, entonces por el Corolario 1.1.12 tenemos

$$\dim_{\mathbb{R}} (K_{\mathbb{A}})_\infty^{N-n} = \left(\sum_{v|\infty} d_v \right) (N-n) = d(N-n).$$

Por lo tanto, aplicar la sustitución $y \to \mu y$ da

$$\mathrm{vol}(\Phi_n(\mu T)) = \mu^{d(N-n)} \int_{(K_{\mathbb{A}})^{N-n}} \mathrm{vol}(\Phi_n((\mu T)(\mu y)))dy\,.$$

Observar que $(\mu T)(\mu y) = \mu(T(y))$. Como $T(y)$ es convexo y $\mu \geq 1$, siguiendo el mismo argumento que en el caso $n = N$, obtenemos

$$\mathrm{vol}(\Phi_n((\mu T)(\mu y)) = \mathrm{vol}(\Phi_n((\mu(Ty))) \geq \mathrm{vol}(\Phi_n(T(y))).$$

Juntando todo y usando el teorema de Fubini una vez más, concluimos que

$$\mathrm{vol}(\Phi_n(\mu T)) \geq \mu^{d(N-n)} \int_{(K_{\mathbb{A}})^{N-n}} \mathrm{vol}(\Phi_n(T)(y))dy \geq \mu^{d(N-n)}\, \mathrm{vol}(\Phi_n(T)).$$

□

Ahora damos una versión adélica del Lema 2.1.9.

Lema 2.2.11. *Para cada $n = 1, \ldots, N$, sean T, Φ_n y μ_n como antes. Adicionalmente, sea Φ_0 la función identidad en $E_{\mathbb{A}}$. Luego, para cada $n \in \{0, 1, \ldots, N-1\}$,*

$$\mathrm{vol}(\Phi_{n+1}(\mu_{n+1}T)) = \mathrm{vol}(\Phi_n(\mu_{n+1}T)).$$

Demostración. La prueba se divide en dos pasos. Primero, probaremos que la aplicación φ_{n+1} definida arriba es inyectiva cuando se restringe a $\Phi_n(\mu_{n+1}T)$. Luego, usaremos el teorema de Fubini y la Proposición 1.4.9 para deducir el lema.

Considerar la aplicación

$$\varphi_{n+1} : \Phi_n(\mu_{n+1}T) \to (K_{\mathbb{A}}/K)^{n+1} \times K_{\mathbb{A}}^{Nn-1},$$

$$\varphi_{n+1}(\overline{x_1}, \ldots, \overline{x_n}, x_{n+1}, \ldots, x_N) = (\overline{x_1}, \ldots, \overline{x_{n+1}}, x_{n+2}, \ldots, x_N).$$

Está claro por definición que $\varphi_{n+1}(\Phi_n(\mu_{n+1}T)) = \Phi_{n+1}(\mu_{n+1}T)$. Veamos ahora que φ_{n+1} es inyectiva. Sean $x, y \in \mu_{n+1}T$. Debemos probar que si $\Phi_{n+1}(x) = \Phi_{n+1}(y)$ entonces $\Phi_n(x) = \Phi_n(y)$.

Supongamos que $\Phi_{n+1}(x) = \Phi_{n+1}(y)$. Esto significa que

$$\begin{cases} x_m - y_m \in K \text{ si } 1 \leq m \leq n+1 \\ x_m = y_m \text{ si } n+1 < m \leq N. \end{cases}$$

En particular, $x - y \in E = K^N$. Como T_v es abierto para $v|\infty$ (más explícitamente, es un subconjunto abierto de $\mathbb{R}$ o $\mathbb{C}$) es fácil ver que, para algún $\mu < \mu_{n+1}$, $x, y \in \mu T$ y así, por definición de μ_{n+1}, se deduce que $x_{n+1} = y_{n+1}$. Por lo tanto, $\Phi_n(x) = \Phi_n(y)$. Concluimos de esta forma que φ_n restringida a $\Phi_n(\mu_{n+1}T)$ es inyectiva.

Probemos ahora que $\text{vol}(\Phi_{n+1}(\mu_{n+1}S)) = \text{vol}(\Phi_n(\mu_{n+1}S))$.

Para cada $y = (\overline{y_1}, \ldots, \overline{y_n}, y_{n+2}, \ldots, y_N) \in (K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n-1}$, escribimos

$$\Phi_n(\mu_{n+1}T)_y := \{w \in K_{\mathbb{A}} : (\overline{y_1}, \ldots, \overline{y_n}, w, y_{n+2}, \ldots, y_N) \in \Phi_n(\mu_{n+1}T)\}.$$

Del mismo modo, definimos

$$\Phi_{n+1}(\mu_{n+1}T)_y := \{w \in K_{\mathbb{A}}/K : (\overline{y_1}, \ldots, \overline{y_n}, w, y_{n+2}, \ldots, y_N) \in \Phi_{n+1}(\mu_{n+1}T)\}.$$

Entonces, por el teorema de Fubini, tenemos

$$\text{vol}(\Phi_n(\mu_{n+1}T)) = \int_{(K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n-1}} \text{vol}(\Phi_n(\mu_{n+1}T)_y) dy \ .$$

Por el momento, fijamos un $y \in (K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n-1}$. Sea $\pi : K_{\mathbb{A}} \to K_{\mathbb{A}}/K$ la aplicación cociente. Usando la Proposición 1.4.9 y el hecho de que $\pi(\Phi_n(\mu_{n+1}T)_y) = \Phi_{n+1}(\mu_{n+1}T)_y$,

obtenemos

$$\begin{aligned}\mathrm{vol}(\Phi_n(\mu_{n+1}T)_y) &= \int_{K_{\mathbb{A}}} \chi_{\Phi_n(\mu_{n+1}T)_y}(z)dz \\ &= \int_{K_{\mathbb{A}}/K} \left(\sum_{x\in K} \chi_{\Phi_n(\mu_{n+1}T)_y}(w+x) \right) d\pi(w) \\ &= \int_{\Phi_{n+1}(\mu_{n+1}T)_y} d\pi(w) \\ &= \mathrm{vol}(\Phi_{n+1}(\mu_{n+1}T)_y)\ .\end{aligned}$$

Aquí hemos utilizado la inyectividad de φ_{n+1} para establecer que π es una biyección entre $\Phi_n(\mu_{n+1}T)_y$ y $\Phi_{n+1}(\mu_{n+1}T)_y$. Así,

$$\sum_{x\in K} \chi_{\Phi_n(\mu_{n+1}T)_y}(w+x) = \begin{cases} 1 \text{ si } \pi(w) \in \Phi_{n+1}(\mu_{n+1}T)_y \\ 0 \text{ si no }. \end{cases}$$

Finalmente, aplicando de nuevo Fubini, concluimos que

$$\begin{aligned}\mathrm{vol}(\Phi_n(\mu_{n+1}T)) &= \int_{(K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n-1}} \mathrm{vol}(\Phi_{n+1}(\mu_{n+1}T)_y)dy \\ &= \mathrm{vol}(\Phi_{n+1}(\mu_{n+1}T))\ .\end{aligned}$$

□

De estos dos lemas podemos deducir fácilmente la versión adélica del teorema de Davenport-Estermann, siguiendo la demostración de Estermann para el caso euclidiano.

En efecto, aplicando el Lema 2.2.10 con $\mu = \frac{\mu_{n+1}}{\mu_n}$, y después el Lema 2.2.11, obtenemos que, para cada $n = 1, \ldots, N-1$,

$$\mathrm{vol}(\Phi_{n+1}(\mu_{n+1}T)) \geq \left(\frac{\mu_{n+1}}{\mu_n}\right)^{d(N-n)} \mathrm{vol}(\Phi_n(\mu_n T)).$$

Además, Lema 2.2.11 da

$$\mathrm{vol}(\Phi_1(\mu_1 T)) \leq \mathrm{vol}(\mu_1 T) = \mu_1^{dN}\,\mathrm{vol}(T).$$

Iterando, deducimos que

$$\mathrm{vol}(\Phi_N(\mu_N T)) \geq \left(\prod_{n=1}^{N} \left(\frac{\mu_{n+1}}{\mu_n}\right)^{d(N-n)} \right) \mu_1^{dN}\,\mathrm{vol}(T).$$

Claramente, el lado izquierdo es menor o igual que el volumen de $(K_{\mathbb{A}}/K)^N$, que es 1, y el lado derecho es igual a $(\mu_1\mu_2\cdots\mu_N)^d \operatorname{vol}(T)$. Esto concluye la prueba de Teorema 2.2.8.

Ahora, probemos la versión adélica del segundo teorema de Minkowski.

Comencemos por probar la cota superior. Recordemos que el teorema afirma que

$$(\lambda_1\lambda_2\cdots\lambda_N)^d \operatorname{vol}(S) \leq 2^{dN},$$

donde $S = \prod_{v|\infty} S_v \times \prod_{v \text{ finito}} \Lambda_v$ con $S_v \subset E_v$ no vacío convexo abierto simétrico acotado y Λ un K-lattice en E, y $\lambda_1, \ldots, \lambda_N$ son los mínimos sucesivos correspondientes.

Por definición de los mínimos sucesivos, hay una base $\{u_1, \ldots, u_N\}$ de E sobre K tal que por cada $n \in \{1, \ldots, N\}$, tenemos que $u_1, \ldots, u_n \in (\lambda S) \cap E$ para todo $\lambda > \lambda_n$ (equivalentemente, $u_1, \ldots, u_n \in \overline{\lambda_n S} \cap E$). Sea $U = (u_1\ u_2\ \cdots\ u_N)$ la matriz no singular $N \times N$ cuyas columnas son los vectores $u_1, \ldots, u_N$. U define un automorfismo de $E_{\mathbb{A}}$. Por Corolario 1.4.8 y la fórmula del producto, tenemos

$$\operatorname{vol}(U^{-1}S) = \left(\prod_{v \in M_K} \left\| \det U^{-1} \right\|_v \right) \operatorname{vol}(S) = \operatorname{vol}(S).$$

Además, es fácil ver que $U^{-1}S_v$ es un subconjunto acotado abierto simétrico convexo de E_v, y que $U^{-1}\Lambda$ es un K-lattice con clausura $U^{-1}\Lambda_v$ para cada lugar finito v. Notar que los mínimos sucesivos de $U^{-1}S$ son los mismos que los correspondientes a S; sin embargo, los vectores asociados pueden tomarse como $e_1, \ldots, e_N$, donde e_j es el vector con j-ésima coordenada 1 y el resto 0. Sin pérdida de generalidad, podemos asumir que, para $1 \leq n \leq N$, el vector e_n está contenido en la clausura de $\lambda_n S$.

Ahora aplicamos el teorema de Davenport-Estermann con $T = S$, lo cual nos dice que

$$(\mu_1\mu_2\cdots\mu_N)^d \operatorname{vol}(S) \leq 1.$$

Por lo tanto, para obtener la cota superior en el teorema de Minkowski, es suficiente demostrar que $\mu_n \geq \lambda_n/2$ para todo n.

Recordar que μ_n es el supremo de los $\mu > 0$ tales que si $x, y \in \mu S$ satisfacen que $x - y \in E$, entonces $x_j = y_j$ para $j = n, \ldots, N$. Por consiguiente, solo necesitamos ver que si tomamos dos elementos arbitrarios $x, y \in \frac{\lambda_n}{2} S$ que cumplen que $x - y \in E$, entonces necesariamente $x_j = y_j$ para $j = n, \ldots, N$.

Sean $x, y \in \frac{\lambda_n}{2} S$ tal que $x - y \in E$. Dado que S es simétrico y convexo, $(S - S)/2 = S$ y por lo tanto $x - y \in (\lambda_n S) \cap E$. De ello se deduce que $x - y$ es una combinación lineal de $e_1, \ldots, e_{n-1}$ sobre K. Por lo tanto, $x_j = y_j$ para $j = n, \ldots, N$.

Esto concluye la prueba de la cota superior en el teorema de Minkowski.

Para la cota inferior, podemos suponer una vez más que para $n = 1, \ldots, N$ el vector e_n está contenido en la clausura de $\lambda_n S$. Definimos para cada lugar infinito v el conjunto

$$S'_v = \{t = (t_1, \ldots, t_n) \in E_v : \sum_{i=1}^{N} \lambda_i |t_i| < 1\}.$$

Afirmamos que $S'_v \subset S_v$. Sea t un elemento de S'_v y sea $\delta = \sum_{i=1}^{N} \lambda_i |t_i| < 1$. Por definición, $t = \sum_i t_i e_i$. Reescribiendo adecuadamente los elementos de la suma,

$$\begin{aligned} t &= \sum_{i=1}^{N} a_i \frac{\delta e_i}{\lambda_i} \\ &= \sum_{i=1}^{N} |a_i| \left(\frac{a_i}{|a_i|} \, \frac{\delta e_i}{\lambda_i} \right), \end{aligned}$$

donde $a_i = \lambda_i t_i \delta^{-1}$. Como $\lambda_i \delta^{-1} > \lambda_i$, se deduce que $e_i \in \lambda_i \delta^{-1} S_v$; equivalentemente, $(\lambda_i)^{-1} \delta e_i \in S_v$. Por la hipótesis de simetría más fuerte que tenemos sobre S_v, se sigue que $\frac{a_i}{|a_i|} \, \frac{\delta e_i}{\lambda_i} \in S_v$. Finalmente, el hecho de que

$$\sum_{i=1}^{N} |a_i| = \frac{1}{\delta} \sum_{i=1}^{N} \lambda_i |t_i| = 1$$

significa que t es una combinación convexa de elementos de S_v. Luego, $t \in S_v$ por convexidad de S_v. En conclusión, hemos demostrado que $S'_v \subset S_v$.

Sea ahora

$$S' := \prod_{v|\infty} S'_v \times \prod_{v \nmid \infty} \mathcal{O}_v.$$

Está claro que $S' \subset S$ y por lo tanto $\mathrm{vol}(S') \leq \mathrm{vol}(S)$. Para terminar la prueba, veremos que

$$\mathrm{vol}(S') = \frac{2^{dN} \pi^{sN}}{((N!)^r ((2N)!)^s} \left| D_{K/\mathbb{Q}} \right|^{-N/2}. \tag{2.2}$$

Observar que, por definición de S' y de la medida adélica,

$$\mathrm{vol}(S') = \prod_{v|\infty} \beta_v^N(S'_v) \prod_{v \nmid \infty} \beta_v^N(\mathcal{O}_v). \tag{2.3}$$

Recordar que $\beta_v^N(\mathcal{O}_v) = \left|D_{K_v/\mathbb{Q}_p}\right|_p^{N/2}$ si v es un lugar de K sobre el primo $p \in \mathbb{Z}$, y que $\prod_v \left|D_{K_v/\mathbb{Q}_p}\right|_p^{N/2} = \left|D_{K/\mathbb{Q}}\right|^{-N/2}$. Esto implica que

$$\prod_{v\nmid\infty} \beta_v^N(\mathcal{O}_v) = \left|D_{K/\mathbb{Q}}\right|^{-N/2}. \tag{2.4}$$

El siguiente lema, junto con (2.3) y (2.4), da (2.2), concluyendo la prueba de Teorema 2.2.7.

Lema 2.2.12. *Sean $b, \lambda_1, \ldots, \lambda_N$ números reales positivos. Para cada lugar infinito v, definimos*

$$M_v(b) := \{t \in E_v : \sum_{i=1}^{N} \lambda_i |t_i| < b\}.$$

Entonces,

$$\beta_v^N(M_v(b)) = \begin{cases} \frac{2^N}{N!} b^N (\lambda_1\lambda_2\cdots\lambda_N)^{-1} & \text{si } v \text{ es real,} \\ \frac{(4\pi)^N}{(2N)!} b^{2N} (\lambda_1\lambda_2\cdots\lambda_N)^{-2} & \text{si } v \text{ es complejo.} \end{cases}$$

Demostración. Lo probamos por inducción en N. El caso $N = 1$ es fácil porque $M_v(b)$ es un intervalo o una bola, dependiendo de si v es real o complejo.

Ahora, sea $N \geq 2$ y supongamos que el lema es verdadero para todo $n < N$. Primero, asumimos que v es real.

$$\begin{aligned} \beta_v^N(M_v(b)) &= \int_{-b/\lambda_N}^{b/\lambda_N} \beta_v^{N-1}(M_v(b - \lambda_N|t_N|))dt_N \\ &= 2\int_0^{b/\lambda_N} \frac{2^{N-1}}{(N-1)!} (\Lambda_1\cdots\lambda_{N-1})^{-1} (b - \lambda_N t_N)^{N-1} dt_N \\ &= \frac{2^N}{(N-1)!} (\lambda_1\lambda_2\cdots\lambda_N)^{-1} b^N. \end{aligned}$$

Segundo, supongamos que v es complejo. Recordar que en este caso, la medida β_v en K_v es dos veces la medida de Lebesgue.

$$\begin{aligned}
\beta_v^N(M_v(b)) &= 2\int_{B(0,b/\lambda_N)} \beta_v^{N-1}(M_v(b-\lambda_N|t_N|))dt_N \\
&= 2\int_{B(0,b/\lambda_N)} \frac{(4\pi)^{N-1}}{(2N-2)!}(\Lambda_1\cdots\lambda_{N-1})^{-2}(b-\lambda_N|t_N|)^{2N-2}dt_N \\
&= 2\frac{(4\pi)^{N-1}}{(2N-2)!}(\lambda_1\lambda_2\cdots\lambda_N)^{-2}\int_{B(0,b/\lambda_N)}(b-|x|)^{2N-2}dx \\
&= 2\frac{(4\pi)^{N-1}}{(2N-2)!}(\lambda_1\lambda_2\cdots\lambda_N)^{-2}\int_0^b\int_0^{2\pi}(b-r)^{2N-2}rd\theta dr \\
&= \frac{(4\pi)^N}{(2N-2)!}(\lambda_1\lambda_2\cdots\lambda_N)^{-2}\left(\int_0^b b(b-r)^{2N-2}dr + \int_0^b (rb)^{2N-1}dr\right) \\
&= \frac{(4\pi)^N}{(2N-2)!}(\lambda_1\lambda_2\cdots\lambda_N)^{-2}\left(\frac{b^{2N}}{2N-1} - \frac{b^{2N}}{2N}\right) \\
&= \frac{(4\pi)^N}{(2N)!}(\lambda_1\lambda_2\cdots\lambda_N)^{-2}b^{2N}.
\end{aligned}$$

Notar que en el tercer paso del cálculo anterior aplicamos la sustitución $x = \lambda_N t_N$, y en el cuarto paso usamos coordenadas polares. □

Capítulo 3

Rebanado de cubos

3.1. En $\mathbb{R}^N$

Sea $Q_N = [-\frac{1}{2}, \frac{1}{2}]^N$ el cubo N-dimensional de volumen 1. Estamos interesados en estudiar el volumen de las "rebanadas" (*slices*) del cubo. Es decir, si V es un subespacio de $\mathbb{R}^N$ de dimensión L, queremos estimar el volumen L-dimensional de la intersección $V \cap Q_N$. Si se piensa en los casos $N = 2$ o $N = 3$, es intuitivamente obvio que la cota inferior óptima para dicho volumen debe ser de 1. En [18], Vaaler obtuvo esta estimación como corolario de una desigualdad más general relativa al producto de esferas de diferentes dimensiones.

Denotamos por B_n a la bola

$$B_n = \{x \in \mathbb{R}^n : |x| \leq \rho_n\}, \tag{3.1}$$

donde $\rho_n = \pi^{-1/2}(\Gamma(n/2+1))^{1/n}$. Esta es la bola n-dimensional de volumen 1 (con respecto a la medida de Lebesgue en $\mathbb{R}^n$).

Observación. Es un hecho conocido que

$$\Gamma\left(\frac{n}{2}+1\right) = \begin{cases} \left(\frac{n}{2}\right)! \text{ si } n \text{ es par} \\ \sqrt{\pi}\frac{n!!}{2^{(n+1)/2}} \text{ si } n \text{ es impar.} \end{cases}$$

Aquí $n!!$ es el doble factorial de n, que en el caso de enteros impares es

$$n!! = \prod_{j=1}^{\frac{n+1}{2}}(2j-1).$$

En particular, $B_1 = [-\frac{1}{2}, \frac{1}{2}]$.

Recordar, además, que Γ satisface la ecuación funcional

$$\Gamma(z+1) = z\Gamma(z). \tag{3.2}$$

El resultado principal de Vaaler en [18] es el siguiente teorema, conocido como teorema de rebanado de cubos (*cube slicing theorem*) o desigualdad de rebanado de cubos (*cube slicing inequality*).

Teorema 3.1.1 (Desigualdad de rebanado de cubos)**.** *Sea $N = n_1 + \cdots + n_r$ una partición del entero positivo N y sea $Q_N := B_{n_1} \times B_{n_2} \times \cdots \times B_{n_r}$. Para cualquier matriz B de tamaño $N \times L$ y rango $L < N$, tenemos*

$$\det(B^t B)^{-\frac{1}{2}} \leq \text{ vol}\left(\{y \in \mathbb{R}^L : By \in Q_N\}\right) . \tag{3.3}$$

Veremos que este teorema es, de hecho, equivalente a:

Teorema 3.1.2. *Sea Q_N como en el teorema anterior y sea V un subespacio de $\mathbb{R}^N$ de dimensión L. Luego,* $\text{vol}(Q_N \cap V) \geq 1$*, donde el volumen se toma con respecto a la medida de Haar del subespacio V.*

Observación. Cuando se aplica con $r = 1$, Teorema 3.1.2 da una respuesta óptima al problema de encontrar una cota inferior para el volumen de las rebanadas de un cubo.

Proposición 3.1.3. *Teorema 3.1.1 es equivalente a Teorema 3.1.2.*

Demostración. Primero, veamos que el Teorema 3.1.1 implica el Teorema 3.1.2. Sea B una matriz de $N \times L$ cuyas columnas forman una base ortonormal de V. El lado derecho de (3.3) es $\text{vol}(Q_N \cap V)$ y, dado que $B^t B = id$, el lado izquierdo es 1.

Ahora, probemos la otra implicación. Sea B una matriz $N \times L$ de rango L. Sea V la imagen de B; es un subespacio de $\mathbb{R}^N$ de dimensión L. Sea $v_1, \ldots, v_L$ una base ortonormal de V. Consideramos el isomorfismo $E : \mathbb{R}^L \to V$ definido por

$$e_i \longmapsto v_i, \quad i = 1, \ldots, L \ ,$$

donde $e_1, \ldots, e_L$ es la base estándar de $\mathbb{R}^L$. Entonces la medida de Haar de V está definida por

$$\nu(\mathcal{U}) := \text{vol}(E^{-1}(\mathcal{U})),$$

y la integral correspondiente es

$$\int_V f(x)d\nu(x) = \int_{\mathbb{R}^L} f(Ey)dy.$$

En particular, por definición,

$$\mathrm{vol}(Q_N \cap V) = \int_V \chi_{Q_N}(x)d\nu(x) = \int_{R^L} \chi_{Q_N}(Ey)dy.$$

Dado que $B : \mathbb{R}^L \to V$ es otro isomorfismo, el teorema de cambio de variables aplicado con la transformación $T = B^{-1}E$ da

$$\begin{aligned}\int_{R^L} \chi_{Q_N}(By)dy &= \left|\det(B^{-1}E)\right| \int_{\mathbb{R}^L} \chi_{Q_N}(Ey)dy \\ &\geq \left|\det(B^{-1}E)\right| \\ &= \det(B^tB)^{-1/2},\end{aligned}$$

donde el último paso se sigue del hecho de que E es ortogonal. Concluimos que (3.3) es válido para una matriz arbitraria B. □

La prueba de Teorema 3.1.1 requiere de un lema sobre funciones log-cóncavas, que describimos a continuación. La demostración, así como otras propiedades de las funciones log-cóncavas, pueden encontrarse en [14].

Definición 3.1.4. Una función real no negativa $f : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ se dice **log-cóncava** si para cualquier $x, y \in \mathbb{R}$ y cualquier par de números reales $\lambda, \mu > 0$ tales que $\lambda + \mu = 1$, tenemos que

$$f(\lambda x + \mu y) \geq f(x)^\lambda f(y)^\mu.$$

Observación. Sea f una función cóncava de log y sea $U = \{x \in \mathbb{R}^n : f(x) > 0\}$; observar que U es un subconjunto abierto convexo de $\mathbb{R}^n$. Podemos definir la función $\log f : U \to \mathbb{R}$, que es claramente cóncava. Por lo tanto, f es continua en cada punto de U.

Lema 3.1.5. *Sea $f : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ una función log-cóncava y sea A un conjunto convexo de $\mathbb{R}^m$. Entonces, la función*

$$x \longmapsto \int_A f(x, y)dy$$

es log-cóncava en $\mathbb{R}^n$ si la integral es siempre finita.

Demostración. Ver, por ejemplo, [14, Th. 6]. □

Sea μ la medida de probabilidad en $\mathbb{R}^n$ correspondiente a la densidad normal de Gauss. Para un conjunto boreliano Ω, está dada por

$$\mu(\Omega) = \int_\Omega \exp(-\pi|x|^2)dx\,,$$

donde la integral se toma con respecto a la medida de Lebesgue. Observar que $\exp(-\pi|x|^2)$ es una función log-cóncava, simétrica y continua en $\mathbb{R}^n$.

Para $s \in (0,1)$, considerar el subconjunto simétrico convexo compacto K_s de $\mathbb{R}^n$, con interior no vacío, definido por

$$K_s := \{x \in \mathbb{R}^n : \exp(-\pi|x|^2) \geq s\}.$$

Una aplicación del teorema de Fubini da

$$\mu(\Omega) = \int_0^1 \left(\int_{K_s \cap \Omega} dx \right) ds.$$

Lema 3.1.6. *Sea $N = n_1 + \cdots + n_r$ una partición de N. Sea $Q_N = B_{n_1} \times \cdots \times B_{n_r}$, donde B_{n_i} se define como en (3.1). Sea A un subconjunto convexo simétrico cerrado de $\mathbb{R}^N$. Entonces,*

$$\mu(A) \leq \mathrm{vol}(A \cap Q_N)\,,$$

donde μ es la medida de Gauss y vol *es la medida de Lebesgue en $\mathbb{R}^N$.*

Demostración. Probamos el lema por inducción en r.

Supongamos que $r = 1$. Entonces $N = n_1 =: n$. Integrando en coordenadas polares, obtenemos

$$\mu(A) = \int_{S^{n-1}} \int_0^\infty \chi_A(rx') \exp(-\pi|x|^2) r^{n-1}\, dr\; d\lambda_{n-1}\,,$$

donde λ_{n-1} es la medida en S^{n-1} definida por $\lambda_{n-1}(E) = \mathrm{vol}(\widetilde{E})$ para cada conjunto $E \subset S^{n-1}$ tal que

$$\widetilde{E} := \{x \in \mathbb{R}^n : \frac{x}{|x|} \in E, 0 < x < 1\}$$

es Lebesgue-medible en $\mathbb{R}^n$.

Fijamos $x' \in S^{n-1}$. Por convexidad, o bien

$$\mathbb{R}x' \cap A \subset \mathbb{R}x' \cap B_n,$$

o bien

$$\mathbb{R}x' \cap B_n \subset \mathbb{R}x' \cap A. \tag{3.4}$$

En el primer caso, queda claro que

$$\int_0^\infty \chi_A(rx') \exp(-\pi|x|^2) r^{n-1}\, dr \leq \int_0^\infty \chi_{B_n \cap A}(rx') r^{n-1}\, dr.$$

En el segundo caso,

$$\begin{aligned}
\int_0^\infty \chi_A(rx') \exp(-\pi|x|^2) r^{n-1}\, dr &\leq \int_0^\infty \exp(-\pi|x|^2) r^{n-1}\, dr \\
&= \int_0^\infty \exp(-t) \left(\frac{t}{\pi}\right)^{\frac{n-2}{2}} (2\pi)^{-1} dt \\
&= \frac{\pi^{n/2}}{n} \Gamma\left(\frac{n}{2}+1\right) \\
&= \int_0^{\rho(n)} r^{n-1}\, dr \\
&= \int_0^\infty \chi_{B_n}(rx') r^{n-1}\, dr \\
&= \int_0^\infty \chi_{B_n \cap A}(rx') r^{n-1}\, dr.
\end{aligned}$$

Notar que obtuvimos la primera igualdad aplicando la sustitución $t = \pi r^2$, la segunda igualdad utilizando (3.2) y la última igualdad por nuestra hipótesis (3.4).

Concluimos que, en ambos casos,

$$\int_0^\infty \chi_A(rx') \exp(-\pi|x|^2) r^{n-1}\, dr \leq \int_0^\infty \chi_{B_n \cap A}(rx') r^{n-1}\, dr.$$

Por lo tanto,

$$\begin{aligned}
\mu(A) &\leq \int_{S^{n-1}} \int_0^\infty \chi_{B_n \cap A}(rx') r^{n-1}\, dr\, d\lambda_{n-1} \\
&= \mathrm{vol}(B_n \cap A).
\end{aligned}$$

Esto prueba el lema para $r = 1$.

Ahora hacemos el paso inductivo. Sea $n = n_1 + \cdots + n_{r-1}$, entonces $N = n + n_r$. Denotaremos los puntos en $\mathbb{R}^N = \mathbb{R}^n \times \mathbb{R}^{n_r}$ como $x = (y, z)$. Para cada $y \in \mathbb{R}^n$, sea

$$A_y := \{z \in \mathbb{R}^{n_r} : (y, z) \in A\}.$$

Por Lema 3.1.5, la función simétrica

$$f(y) := \int_{B_{n_r} \cap A_y} dz = \int_{B_{n_r}} \chi_A(y, z) dz$$

es log-cóncava en $\mathbb{R}^n$.

Para cada $k, m \in \mathbb{N}$, sea $E_{k,m} = \{y \in \mathbb{R}^n : f(y) \geq k/m\} \subset \mathbb{R}^n$. Es fácil ver que $E_{k,m}$ es cerrado, simétrico y convexo. Considerar la sucesión de funciones

$$f_m := \sum_{k=0}^{\infty} \frac{1}{m} \chi_{E_{k,m}}.$$

Observar que, por cada $y \in \mathbb{R}^n$, la sucesión $(f_m(y))$ es decreciente y que

$$\lim_{m\to\infty} f_m(y) = f(y).$$

Por hipótesis inductiva,

$$\mu(E_{k,m}) \leq \mathrm{vol}(E_{k,m} \cap Q_n),$$

donde $Q_n = B_{n_1} \times \cdots \times B_{n_{r-1}}$. Por lo tanto

$$\int \frac{1}{m} \chi_{E_{k,m}}(y) d\mu(y) \leq \int_{Q_n} \frac{1}{m} \chi_{E_{k,m}}(y) dy.$$

Dos aplicaciones sucesivas del teorema de convergencia monótona dan

$$\int f(y) d\mu(y) \leq \int_{Q_n} f(y) dy.$$

Ahora escribimos cada lado de esta desigualdad más explícitamente. El lado derecho es

$$\int_{Q_n} f(y) dy = \int_{Q_n} \int_{B_{nr}} \chi_A(y, z) dz dy = \mathrm{vol}(A \cap Q_N).$$

En cuanto al lado izquierdo, tenemos

$$\begin{aligned} \int f(y) d\mu(y) &= \int_{\mathbb{R}^n} \int_{B_{n_r}} \chi_A(y, z) dz d\mu(y) \\ &= \int_{B_{n_r}} \left(\int_{\mathbb{R}^n} \chi_A(y, z) d\mu(y) \right) dz \\ &= \int_0^1 \int_{B_{n_r}} \int_{K_s \cap A^z} dy dz ds, \end{aligned}$$

donde $A^z := \{y \in \mathbb{R}^n : (y, z) \in A\}$, por cada $z \in \mathbb{R}^{n_r}$.

Ahora, el mismo argumento de antes se puede aplicar a la función

$$g(z) := \int_{K_s \cap A^z} dy$$

para probar que

$$\int_{\mathbb{R}^{n_r}} g(z)d\mu(z) \leq \int_{B_{n_r}} g(z)dz,$$

lo que a su vez implica que

$$\int_0^1 \int_{\mathbb{R}^{n_r}} \int_{K_s \cap A^z} dyd\mu(z)ds \leq \text{vol}(A \cap Q_N).$$

Pero, por Fubini, el lado izquierdo de esta desigualdad es

$$\int_{\mathbb{R}^{n_r}} \left(\int_0^1 \int_{K_s \cap A^z} dyds \right) = \int_{\mathbb{R}^{n_r}} \mu(A^z)dz = \mu(A).$$

Con esto concluye la prueba del lema. □

Ahora, probaremos la desigualdad de rebanado de cubos de Vaaler. Por la Proposición 3.1.3, basta con probar el Teorema 3.1.2. Sea V un subespacio de $\mathbb{R}^N$ de dimensión L. Sin pérdida de generalidad, podemos suponer que $V = \mathbb{R}^L \times \{0\}^{N-L}$ (canónicamente lo identificamos con $\mathbb{R}^L$) y por lo tanto su medida de Haar es la Lebesgue en $\mathbb{R}^L$.

Sea $\epsilon > 0$, definimos

$$V_\epsilon := \{x \in \mathbb{R}^N : \inf_{y \in V} |x - y| \leq \epsilon\}.$$

Observar que, dado que $V = \mathbb{R}^L$, claramente $V_\epsilon = V \times D_\epsilon$, donde $D_\epsilon = \overline{B_\epsilon}(0)$ es la bola cerrada de radio ϵ centrada en 0. De ello se deduce que V_ϵ es cerrado, convexo y simétrico. Por Lema 3.1.6,

$$\text{vol}(D_\epsilon)^{-1}\mu(V_\epsilon) \leq \text{vol}(D_\epsilon)^{-1} \int_{\mathbb{R}^N} \chi_{Q_N \cap V_\epsilon}(x)dx. \tag{3.5}$$

Dado que el producto de las medidas de Gauss da la medida de Gauss del espacio del producto, tenemos

$$\mu_{\mathbb{R}^N}(V_\epsilon) = \mu_V(V)\mu_{\mathbb{R}^{NL}}(D_\epsilon) = \mu(D_\epsilon).$$

Además, por el Teorema de diferenciación de Lebesgue,

$$\lim_{\epsilon \to 0} \frac{\mu_{\mathbb{R}^{NL}}(D_\epsilon)}{\text{vol}_{\mathbb{R}^{NL}}(D_\epsilon)} = 1.$$

Por lo tanto, si $\epsilon \to 0$, el lado izquierdo de (3.5) tiende a 1.

Por otra parte,

$$\text{vol}(D_\epsilon)^{-1} \int_{\mathbb{R}^N} \chi_{Q_N \cap V_\epsilon}(x)dx = \int_V \left(\text{vol}(D_\epsilon)^{-1} \int_{\mathbb{R}^{NL}} \chi_{Q_N \cap V_\epsilon}(y, z)dz \right) dy.$$

Si $y \in V$ no está en el borde de $L \cap Q_N$ (en cuyo caso, $\chi_{Q_N \cap V_\epsilon}$ es continua en el punto $(y,0) \in \mathbb{R}^N$), entonces

$$\lim_{\epsilon \to 0} \mathrm{vol}(D_\epsilon)^{-1} \int_{\mathbb{R}^{NL}} \chi_{Q_N \cap V_\epsilon}(y,z)dz = \chi_{V \cap Q_N}(y),$$

nuevamente por el teorema de diferenciación de Lebesgue.

Finalmente, por el teorema de convergencia dominada, llegamos a que el límite del lado derecho de (3.5) cuando $\epsilon \to 0$ es

$$\int_V \chi_{V \cap Q_N}(y)dy = \mathrm{vol}(V \cap Q_N).$$

En conclusión, si tomamos $\epsilon \to 0$ en (3.5), obtenemos

$$1 \leq \mathrm{vol}(Q_N \cap V),$$

Así, hemos probado el Teorema 3.1.2 y, por consiguiente, el Teorema 3.1.1.

3.2. En el anillo de adeles

Ahora, generalizaremos la desigualdad de rebanado de cubos en el contexto del anillo de adeles de un cuerpo de números. A lo largo de esta sección, usamos la misma notación que en la Sección 2.2.

Para cada lugar $v \in M_K$, sea Q_v^N un cubo en K_v^N dado por

- $Q_v^N := \{x \in K_v^N : \max_n \|x\|_v \leq 1\}$ si v es finito;
- $Q_v^N := \{x \in K_v^N : \max_n \|x\|_v < \frac{1}{2}\}$ si v es real;
- $Q_v^N := \{x \in K_v^N : \max_n \|x\|_v < \frac{1}{2\pi}\}$ si v es complejo;

donde $\|\cdot\|_v$ son los valores absolutos normalizados con respecto a la extensión $K/\mathbb{Q}$. Notar que para cada lugar infinito, este es el cubo de la medida de Haar normalizada igual a 1, y para cada lugar finito v, $Q_v^N = \mathcal{O}_v^N$. Definimos $Q := \prod_{v \in M_K} Q_v^N$.

Sea B una matriz $N \times L$ de rango L con entradas en K. Para cada lugar v, sea

$$S_v := \{y \in K_v^L : By \in Q_v^N\},$$

y sea

$$S := \prod_v S_v.$$

Verificaremos en lo que sigue que S es, como se espera, un subconjunto de $K_{\mathbb{A}}^L$; de hecho, $S_v = \mathcal{O}_v$ para casi todos los lugares finitos v (ver la observación final de este capítulo).

Teorema 3.2.1 (Desigualdad de rebanado de cubos, en adeles)**.** *Sea B una matriz de $N \times L$ del rango $L < N$ con entradas en K, y sean S y Q como arriba. Entonces, tenemos la desigualdad*

$$H(B)^{-d}\left|D_{K/\mathbb{Q}}\right|^{-L/2} \leq \mathrm{vol}(S),$$

donde $H(B)$ es la altura de la matriz B definida como en la Sección 1.5.2, $D_{K/\mathbb{Q}}$ es el discriminante de alguna base íntegra de K, y el volumen se toma con respecto al producto de medidas normalizadas en el anillo de adeles.

Demostración. Observar que $\mathrm{vol}(S) = \prod_v \beta_v^L(S_v)$. (Recordar que β_v denota la medida normalizada en K_v y β_v^L denota el producto L de dichas medidas). Entonces, basta con encontrar una cota inferior apropiada para $\beta_v^L(S_v)$, para cada $v \in M_K$.

Si v es un lugar real, aplicando la desigualdad de rebanado de cubos en $\mathbb{R}^L$ con $n_j = 1$ para todo j, tenemos

$$\beta_v^L(S_v) \geq \det(B^t B)^{-\frac{1}{2}} = \left\|\det(B^t B)\right\|_v^{\frac{1}{2}} = H_v(B)^{-d}\,,$$

ya que $\|\cdot\|_v = |\cdot|_v^{1/d}$ es el valor absoluto habitual en $\mathbb{R}$, $d = [K : \mathbb{Q}]$ y $H_v(B) = |\det(B^t B)|_v^{1/2}$.

Supongamos que v es un lugar complejo. Siempre podemos escribir $B = U + iV$ para ciertas matrices reales U, V, y, para cualquier $y \in K_v^L = \mathbb{C}^L$, $y = u + iv$ para ciertos vectores reales u, v. De esta manera identificamos K_v^L con $\mathbb{R}^{2L}$, y de manera similar K_v^N con $\mathbb{R}^{2N}$. Estamos trabajando entonces con espacios vectoriales reales, por lo que la aplicación $y \mapsto By$ viene dado por la matriz real $2L \times 2N$ $B' = \left(\begin{smallmatrix} U & -V \\ V & U \end{smallmatrix}\right)$. Además, vía esta identificación,

$$Q_v^N = \{(u, v) \in \mathbb{R}^L \times \mathbb{R}^L : u_j^2 + v_j^2 < \frac{1}{2\pi} \text{ para cada } j = 1, \ldots, L\}.$$

Usando el Teorema 3.1.1, esta vez con $n_1 = \cdots = n_L = 2$, obtenemos

$$\beta_v^L(S_v) \geq \det((B')^* B')^{-\frac{1}{2}}\,.$$

Ya que la aplicación $A \in \mathbb{C}^{N\times L} \mapsto A' \in \mathbb{R}^{2N\times 2L}$ es un homomorfismo de anillos, podemos concluir que

$$\det((B')^*B')^{-\frac{1}{2}} = \det((B^*B)')^{-\frac{1}{2}} = |\det(B^*B)|^{-1},$$

donde $|\cdot|$ es el valor absoluto usual de $\mathbb{C}$. La última igualdad se desprende del siguiente resultado sobre matrices.

Lema 3.2.2. *Sea $A = A_1 + iA_2$ una matriz compleja, y sea $A' = \left(\begin{smallmatrix} A_1 & -A_2 \\ A_2 & A_1 \end{smallmatrix}\right)$. Luego, $\det(A') = |\det A|^2$.*

Ahora, como $\|\cdot\|_v = |\cdot|^2$, concluimos que

$$\beta_v^L(S_v) \geq \|\det(B^*B)\|_v^{-\frac{1}{2}} = H_v(B)^{-d}\,.$$

Por último, sea v un lugar finito. Existe $J \subset \{1,\dots,N\}$ con $|J| = L$ tal que

$$\|\det B_J\|_v = \max_{|I|=L} \|\det B_I\|_v\,,$$

donde B_I es la matriz formada por las filas i-ésimas de B, para $i \in I$.

Si $J = \{j_1,\dots,j_L\}$, consideramos la aplicación lineal σ que permuta las filas de forma que la fila j_l-ésima se convierte en la fila l-ésima. En particular, tenemos

$$\|\det B_J\|_v = \max_{|I|=L} \|\det B_I\|_v = \max_{|I|=L} \|\det(\sigma B)_I\|_v\,.$$

Dado que la matriz correspondiente a σ no es singular y consta de ceros y unos, se deduce que $\sigma(Q_v^N) = Q_v^N$ (recordar que en el caso no arquimediano, $Q_v^N = \mathcal{O}_v^N$). Luego, uno puede deducir fácilmente que $S_v = \{y \in K_v^L : (\sigma B)y \in Q_v^N\}$.

Por lo tanto, podemos asumir, sin pérdida de generalidad, que $J = \{1,\dots,L\}$, por lo que B_J es la submatriz $L \times L$ de B formada por las primeras L filas. Claramente, B_J es inversible. Considerar la matriz $W := BB_J^{-1}$ de tamaño $N \times L$. Observar que $W = (w_{ij})$ tiene la forma

$$W = \left(\frac{id_L}{W'}\right), \tag{3.6}$$

donde id_L es la matriz de identidad $L \times L$ y W' es una matriz $(N-L)\times L$. Dado que $\|\det B_J\|_v$ se eligió para que sea máximo, se deduce que para cada $I \subset \{1,\dots,N\}$ con $|I| = L$ tenemos

$$\|\det W_I\|_v \leq 1\,.$$

En particular, si tomamos $I = \{1, \dots, l-1, l+1, \dots, L, L+j\}$ para cualquier $l \in \{1, \dots, L\}$ y cualquier $j \in \{1, \dots, N-L\}$, entonces

$$\|w_{L+j,l}\|_v = \|\det W_I\|_v \leq 1\,.$$

Por lo tanto, W es una matriz con entradas en $\mathcal{O}_v$. Este hecho, junto con (3.6), nos permite concluir que $Wx \in Q_v^N = \mathcal{O}_v^N$ si y solo si $x \in \mathcal{O}_v^L$. Luego, $B_J S_v = \mathcal{O}_v^L$. En efecto,

$$\begin{aligned} B_J S_v &= \{B_J y \in K_v^L : By \in Q_v^N\} \\ &= \{z \in K_v^L : Wz \in Q_v^N\} \\ &= \mathcal{O}_v^L\,. \end{aligned}$$

Aplicando el cambio de las variables $y' = B_J^{-1} y$, el volumen se transforma por un factor $\|\det B_J\|_v^{-1}$ y así

$$\begin{aligned} \beta_v^L(S_v) &= \|\det B_J\|_v^{-1}\ \beta_v^L(B_J S_v) \\ &= (\max_I \|\det B_I\|_v)^{-1}\ \beta_v^L(\mathcal{O}_v^L) \\ &= H_v(B)^{-1} \big|D_{K_v/\mathbb{Q}_p}\big|_v^{L/2}. \end{aligned}$$

Resumiendo, hemos probado:

- $\beta_v^L(S_v) \geq H_v(B)^{-d}$ si $v|\infty$, y
- $\beta_v^L(S_v) = H_v(B)^{-1} \big|D_{K_v/\mathbb{Q}_p}\big|_v^{L/2}$ si $v \nmid \infty$.

Tomando el producto sobre todo $v \in M_K$ y recordando que

$$\prod_{v \text{ finito}} \big|D_{K_v/\mathbb{Q}_p}\big|_v = \big|D_{K/\mathbb{Q}}\big|^{-1},$$

finalmente llegamos a que

$$H(B)^{-d} \big|D_{K/\mathbb{Q}}\big|^{-L/2} \leq \mathrm{vol}(S).$$

□

Observación. Para cada lugar infinito $v \in M_K$, está claro que S_v es no vacío, abierto, convexo, simétrico y acotado.

Por cada lugar finito v, podemos ver como consecuencia de la demostración anterior que S_v es un K_v-lattice en E_v. En efecto, $S_v = B_J^{-1}\mathcal{O}_v^L$ y B_J es un automorfismo. Por otra parte, salvo para finitos lugares v, $S_v = \mathcal{O}_v^L$. Esto se debe a que, para casi todo v, tanto B_J como B_J^{-1} tienen todas sus entradas en $\mathcal{O}_v$, y entonces $S_v = B_J^{-1}\mathcal{O}_v^L = \mathcal{O}_v^L$.

Capítulo 4

El lema de Bombieri-Vaaler

Sea K un cuerpo y sea $S = \{s^1, \ldots, s^h\}$ un subconjunto finito de K^N. Supongamos que queremos encontrar un polinomio $P \in K[X_1, \ldots, X_N]$ de grado "pequeño" (digamos, a lo sumo d) que se anula en cada punto en S.

La forma más sencilla de hacer esto es la siguiente. Escribimos

$$P = \sum_{i_1+\cdots+i_N \leq d} c_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_N^{i_N}$$

para describir a un polinomio genérico con coeficientes en K. Si $P(s^i) = 0$ para cada i, entonces los coeficientes $(c_{i_1,\ldots,i_N})$ son soluciones del sistema de ecuaciones lineales

$$\begin{cases} P(s^1) = \sum_{i_1+\cdots+i_N \leq d} c_{i_1,\ldots,i_N} (s_1^1)^{i_1} \ldots (s_n^1)^{i_n} = 0 \\ \vdots \\ P(s^n) = \sum_{i_1+\cdots+i_n \leq d} c_{i_1,\ldots,i_n} (s_1^n)^{i_1} \ldots (s_n^n)^{i_n} = 0\,. \end{cases} \tag{4.1}$$

Por lo tanto, para garantizar la existencia del polinomio, todo lo que tenemos que hacer es demostrar que un determinado sistema lineal tiene solución. Más aún, podríamos pedir que los coeficientes del polinomio pertenezcan a un subanillo particular de K (por ejemplo, si K es un cuerpo de números, generalmente es el anillo adecuado es $\mathcal{O}_K$) y que sean "pequeños" en términos de altura. Esto es, por supuesto, equivalente a encontrar soluciones adecuadas del sistema de ecuaciones correspondiente.

El objetivo de este capítulo es, por lo tanto, estudiar el problema de encontrar solu-

ciones enteras de un sistema

$$\begin{cases} a_{11}x_1 + \cdots + a_{1N}x_N = 0 \\ \vdots \\ a_{M1}x_1 + \cdots + a_{MN}x_N = 0 \end{cases}$$

de M ecuaciones lineales en variables N. Para que la existencia de soluciones sea posible, asumimos que $M < N$. En general, también asumimos que el rango la matriz $A = (a_{mn})$ asociada al sistema de ecuaciones es exactamente M. Si ese no fuera el caso, podríamos simplemente eliminar las ecuaciones superfluas y trabajar con una matriz más pequeña.

4.1. Lema de Siegel

En el caso $K = \mathbb{Q}$, tenemos el siguiente resultado clásico.

Lema 4.1.1 (Lema de Siegel)**.** *Sea $A = (a_{ij})$ una matriz no nula de tamaño $M \times N$ con entradas en $\mathbb{Z}$. Supongamos que $N > M$ y que $|a_{ij}| \leq B$ para todo i, j. Luego, el sistema lineal $Ax = 0$ tiene una solución no nula $x = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, que satisface*

$$\max_{1 \leq i \leq n} |x_i| \leq (NB)^{\frac{M}{N-M}}. \tag{4.2}$$

Demostración. La prueba se basa en el principio del palomar (también llamado principio de Dirichlet). La idea es mostrar que hay muchos vectores $x \in \mathbb{Z}^N$ que satisfacen (4.2) pero relativamente pocos valores posibles para Ax. Entonces, debe haber dos vectores distintos y y z en $\mathbb{Z}^N$, de manera que $Ay = Az$, con lo cual $x = y - z$ es la solución deseada.

Para un entero positivo k, consideremos el conjunto

$$T := \{x \in \mathbb{Z}^N : 0 \leq x_i \leq k, i = 1, \ldots, N\}.$$

Denotamos por S_m^+ a la suma de las entradas positivas en la fila m-ésima de A, y por S_M^- a la suma de las entradas negativas. Si notamos $y = Ax$ para $x \in T$, entonces

$$kS_m^- \leq y_m \leq kS_m^+.$$

Sea

$$T' := \{y \in \mathbb{Z}^M : kS_m^- \leq y_m \leq kS_m^+, m = 1, \ldots, M\}.$$

Como $|a_{mn}| \leq B$ para cada par (m,n), se sigue que $S_m^+ - S_m^- \leq NB$ para todo m. Concluimos que

$$|T'| \leq (NkB+1)^M .$$

Ahora, queremos elegir k de manera que T tenga más elementos que T', es decir,

$$(NkB+1)^M < (k+1)^N . \tag{4.3}$$

Pensando en términos asintóticos, esencialmente necesitamos que k^N sea más grande que $(NkB)^M$, así que elegimos $k = \lfloor (NB)^{\frac{M}{N-M}} \rfloor$. Probemos que esta elección funciona. Como $N > M \geq 1$, está claro que $NkB + 1 < NB(k+1)$, y entonces

$$(NkB+1)^M < (NB(k+1))^M \leq (k+1)^{\left(\frac{N-M}{M}+1\right)M}.$$

Pero $\left(\frac{N-M}{M}+1\right) M = N$, con lo cual $k = \lfloor (NB)^{\frac{M}{N-M}} \rfloor$ satisface (4.3).

Por el principio del palomar, hay dos elementos distintos $x', x'' \in T$ con $Ax' = Ax''$. Por lo tanto, el punto $x = x' - x''$ es una solución distinta de cero de $Ax = 0$ con coeficientes enteros y

$$\max_n |x_n| \leq k \leq (NB)^{\frac{M}{N-M}}.$$

□

El lema de Siegel se puede extender a cuerpos de números arbitrarios en forma relativamente directa. Es, de hecho, una consecuencia del lema de Siegel clásico.

Proposición 4.1.2 (Lema de Siegel para cuerpos de números)**.** *Sea K un cuerpo de números de grado d contenido en $\mathbb{C}$ y sea $|\cdot|$ el valor absoluto habitual en $\mathbb{C}$. Sean M, N enteros positivos con $M < N$. Luego, existen constantes absolutas C_1, C_2 tales que para cualquier matriz $M \times N$ no nula, con entradas $a_{mn} \in \mathcal{O}_K$, existe una solución no nula $x \in (\mathcal{O}_K)^N$ de $Ax = 0$ tal que*

$$h(x) \leq C_1 (C_2 NB)^{\frac{M}{N-M}},$$

donde $B := \sup_{\sigma,m,n} |\sigma(a_{mn})|$ con σ en el conjunto de embeddings de K en $\mathbb{C}$.

Demostración. La idea básica de la demostración es transformar el sistema original en un sistema con coeficientes en $\mathbb{Z}$ usando una base íntegra de K, y luego aplicar el Lema 4.1.1.

Sea $\omega_1, \ldots, \omega_d$ una $\mathbb{Z}$-base del anillo de enteros $\mathcal{O}_K$. Podemos escribir

$$a_{mn} = \sum_{j=1}^{d} a_{mn}^{(j)} \omega_j \tag{4.4}$$

para ciertos $a_{mn}^{(j)} \in \mathbb{Z}$. Luego, si para un vector $x = (x_1, \ldots, x_N) \in K^N$, escribimos

$$x_n = \sum_{k=1}^{d} x_n^{(k)} \omega_k,$$

obtenemos

$$\begin{aligned}(Ax)_m &= \sum_{n=1}^{N} \sum_{1 \le j,k \le d} a_{mn}^{(j)} \omega_j \omega_k x_n^{(k)} \\ &= \sum_{l=1}^{d} \sum_{n=1}^{N} \sum_{1 \le j,k \le d} a_{mn}^{(j)} b_{jk}^{(l)} x_n^{(k)} \omega_l \,,\end{aligned}$$

donde $\omega_j \omega_k = \sum_{l=1}^{d} b_{jk}^{(l)} \omega_l$.

Sea

$$A' := \left(\sum_{j=1}^{d} a_{mn}^{(j)} b_{jk}^{(l)} \right)$$

la matriz $(Md) \times (Nd)$ con filas indexadas por (m, l) y columnas indexadas por (n, k). Luego, el lema de Siegel clásico da una solución no nula $y = (x_n^{(k)}) \in \mathbb{Z}^{Nd}$ de $A'y = 0$, con

$$\max_{n,k} \left| x_n^{(k)} \right| \le \left(Nd^2 \max_{m,n,j} \left| a_{mn}^{(j)} \right| \max_{j,k,l} \left| b_{jk}^{(l)} \right| \right)^{\frac{M}{N-M}}. \tag{4.5}$$

Supongamos que σ varía entre los $d = [K : \mathbb{Q}]$ embeddings de K en $\mathbb{C}$. Como

$$\left(\det \left(\sigma(\omega_i) \right)_{\sigma,j} \right)^2 = d(\omega_1, \ldots, \omega_d)$$

y el discriminante de una base íntegra es distinto de cero, deducimos que $\left(\sigma(\omega_i) \right)_{i,\sigma}$ es una matriz invertible $d \times d$. Conjugando (4.4) con todo σ, obtenemos

$$\left(a_{mn}^{(j)} \right)_{(m,n),j} = \left(\sigma(a_{mn}) \right)_{(m,n),\sigma} \left(\sigma(\omega_j) \right)_{j,\sigma}^{-1},$$

así que en particular

$$a_{mn}^{(j)} = \sum_{\sigma} \sigma(a_{mn}) C_{\sigma,j},$$

donde $C_{\sigma,j}$ es un número real positivo que depende solo de σ y j.

De aquí obtenemos la cota

$$\max_{m,n,j}\left|a_{mn}^{(j)}\right| \leq C_2' B\,,$$

para C_2' alguna constante absoluta. Si tomamos $C_2 = d^2 \max_{j,k,l}\left|b_{jk}^{(l)}\right| C_2'$, entonces (4.5) implica que

$$\max_{n,k}\left|x_n^{(k)}\right| \leq (C_2 N B)^{\frac{M}{N-M}}\,.$$

Observar que podemos asumir que las coordenadas de la solución entera $y = (x_n^{(k)})$ de $A'y = 0$ son coprimas; concretamente, que $\gcd\{x_n^{(k)} : n = 1, \ldots, N;\ k = 1, \ldots, d\} = 1$. Luego, $\max_{n,k}\left|x_n^{(k)}\right| = h(y)$.

Sea $x = (x_1, \ldots, x_N) \in (\mathcal{O}_K)^N$ definido por $x_n = \sum_{k=1}^d x_n^{(j)}\omega_k$. Para cada lugar v de K,

$$|x_n|_v \leq \left(\sum_{k=1}^d |\omega_k|_v\right) \max_k \left|x_n^{(k)}\right|_v\,.$$

Si v es un lugar finito, entonces

$$\sum_{k=1}^d |\omega_k|_v \leq \max_k |\omega_k|_v \leq 1.$$

Por lo tanto, si $C_1 = \prod_{v|\infty}\left(\sum_{k=1}^d |\omega_k|_v\right)$, deducimos que $h(x) \leq C_1 h(y)$. Esto concluye la demostración de la proposición. □

4.2. El lema de Bombieri-Vaaler

En estas últimas dos secciones, estudiaremos una serie de mejoras del lema de Siegel por Bombieri y Vaaler. Son mejoras tanto cualitativas como cuantitativas, en el sentido de que aseguran no sólo la existencia de una solución sino también una base de soluciones en $\mathcal{O}_K$, y dan una estimación más precisa para la altura de cada solución. Para ello usaremos los poderosos resultados en geometría de números desarrollados en los capítulos anteriores, en lugar del elemental principio del palomar.

Como siempre, sea K un cuerpo de números de grado d, sea K_v su completación con respecto al lugar v de K y sea $d_v = [K_v : \mathbb{Q}_p]$ el grado local. Sean r y s la cantidad de lugares reales y complejos de K, respectivamente. Recordar que por el Corolario 1.1.12, $r + 2s = \sum_{v|\infty} d_v = d$. Sea $D_{K/\mathbb{Q}}$ el discriminante de alguna base íntegra adecuada de K.

Teorema 4.2.1 (Lema de Bombieri-Vaaler)**.** *Sea A una matriz $M \times N$ de rango $M < N$ con entradas en K. Luego existen $N-M$ vectores linealmente independientes $x_1, \ldots, x_{N-M}$ en $(\mathcal{O}_K)^N$ que forman una base del K-espacio vectorial de soluciones de $Ax = 0$. Más aún, estas soluciones satisfacen la desigualdad*

$$\prod_{l=1}^{N-M} h(x_l) \leq \left\{ \left(\frac{2}{\pi}\right)^s \sqrt{|D_{K/\mathbb{Q}}|} \right\}^{\frac{N-M}{d}} H(A)\,,$$

donde s es el número de lugares complejos de K.

Observación. Se deduce inmediatamente que, en la hipótesis del teorema, hay una solución $x \in (\mathcal{O}_K)^N$ tal que

$$h(x) \leq \left\{ \left(\frac{2}{\pi}\right)^s \sqrt{|D_{K/\mathbb{Q}}|} \right\}^{\frac{1}{d}} H(A)^{\frac{1}{N-M}}\,.$$

Antes de probar Teorema 4.2.1, probemos que este resultado es, en efecto, más fuerte que el lema de Siegel. Como hemos visto, Lema 4.1.1 implica Proposición 4.1.2, por lo que basta con ver que Teorema 4.2.1 implica Lema 4.1.1. Para ello, enunciamos explícitamente el lema de Bombieri-Vaaler para $K = \mathbb{Q}$, que sigue del resultado general calculando la altura de la matriz A en este caso particular.

Corolario 4.2.2 (Lema de Bombieri-Vaaler en $\mathbb{Q}$)**.** *Sea A una matriz $M \times N$ de rango $M < N$ con entradas en $\mathbb{Z}$. Entonces, existen $N - M$ vectores linealmente independientes $x_1, \ldots, x_{N-M}$ en $\mathbb{Z}^N$ que forman una base del espacio vectorial real de soluciones de $Ax = 0$. Más aún, si escribimos $x_l = (x_{1l}, x_{2l}, \ldots, x_{Nl})$, estas soluciones satisfacen la desigualdad*

$$\prod_{l=1}^{N-M} \max_n |x_{nl}| \leq D^{-1}\sqrt{|\det(AA^t)|}\,,$$

donde D es el máximo común divisor de los menores $M \times M$ de A.

En particular, existe una solución no nula $y = (y_1, \ldots, y_N) \in \mathbb{Z}^N$ con

$$\max_n |y_n| \leq \left(D^{-1}\sqrt{|\det(AA^t)|}\right)^{\frac{1}{N-M}}\,.$$

Proposición 4.2.3. *Corolario 4.2.2 implica Lema 4.1.1.*

Demostración. Sea A una matriz de tamaño $M \times N$ con coeficientes enteros tales que $\max_{m,n}|a_{mn}| \leq B$ para un cierto número real positivo B.

Primero, supongamos que rango$(A) = M < N$. En este caso, si el Corolario 4.2.2 es verdadero, hay una solución $x \in \mathbb{Z}^N$ de $Ax = 0$ con

$$\max_n |x_n| \leq \left(D^{-1}\sqrt{|\det(AA^t)|}\right)^{\frac{1}{N-M}} .$$

Dado que $A \in \mathbb{Z}^{M\times N}$ y es de rango M, está claro que $D \geq 1$. Además, como los coeficientes de A están acotadas por B, un cálculo sencillo nos dice que $|\det(AA^t)| \leq (NB)^{2M}$. Por lo tanto,

$$\max_n |x_n| \leq (NB)^{\frac{M}{N-M}} .$$

Supongamos ahora que rank$(A) = M' < M < N$. Sea A' una submatriz $M' \times N$ de A de rango M'. Por el argumento anterior, hay una solución entera x de $A'x = 0$ con

$$\max_n |x_n| \leq (NB)^{\frac{M'}{N-M'}} .$$

Observemos, sin embargo, que $\frac{M'}{N-M'} \leq \frac{M}{N-M}$, porque la función $f(x) = \frac{x}{Nx}$ es creciente en el intervalo $(0, N)$. Así, hemos probado el Lema 4.1.1. □

Nuestro objetivo ahora es probar el Teorema 4.2.1. Para ello, necesitamos el siguiente teorema, que es, en última instancia, una consecuencia del segundo teorema de Minkowski y la desigualdad de rebanado de cubos en el anillo de adeles.

Teorema 4.2.4. *Sea B una matriz de $N \times L$ sobre K de rango $L < N$. Luego, existen L vectores linealmente independientes $u_1, u_2, \ldots, u_L$ en K^L tales que $Bu_l \in (\mathcal{O}_k)^N$ para cada l y*

$$\prod_{l=1}^{L} h(Bu_l) \leq \left\{\left(\frac{2}{\pi}\right)^s \sqrt{|D_{K/\mathbb{Q}}|}\right\}^{\frac{L}{d}} H(B), \tag{4.6}$$

donde s es el número de lugares complejos de K.

Demostración. Para cada lugar v, sea $S_v := \{x \in K_v^L : Bx \in Q_v^N\}$, donde Q_v^N denota el cubo en K_v^N definido como en la Sección 3.2. Sean $\lambda_1, \ldots, \lambda_L$ los mínimos sucesivos asociados con $S := \prod_v S_v$. El segundo teorema de Minkowski nos dice entonces que

$$(\lambda_1\lambda_2\cdots\lambda_L)^d \operatorname{vol}(S) \leq 2^{dL}.$$

Por la desigualdad de rebanado de cubos,

$$H(B)^{-d}\left|D_{K/\mathbb{Q}}\right|^{-L/2} \leq \operatorname{vol}(S),$$

así que

$$\lambda_1\lambda_2\cdots\lambda_L \leq H(B)\left|D_{K/\mathbb{Q}}\right|^{\frac{L}{2d}}2^L. \tag{4.7}$$

Por definición de los mínimos sucesivos, sabemos que existen $u_1,\ldots,u_L$ que forman una base de K^L sobre K, de manera que para cada $l=1,\ldots,L$, los primeros l elementos de la base están contenidos en la clausura de $\lambda_l S$. En particular, esto significa que

$$\max_{1\leq n\leq N}\|(Bu_l)_n\|_v \leq \frac{1}{2}\lambda_l \qquad \text{si } v \text{ es real ,} \tag{4.8}$$

$$\max_{1\leq n\leq N}\|(Bu_l)_n\|_v \leq \frac{1}{2\pi}(\lambda_l)^2 \quad \text{si } v \text{ es complejo,} \tag{4.9}$$

$$\max_{1\leq n\leq N}\|(Bu_l)_n\|_v \leq 1 \qquad \text{si } v \text{ es finito.} \tag{4.10}$$

Para cada $l=1,\ldots,L$, tomando el producto de los $\max_{1\leq n\leq N}\|(Bu_l)_n\|_v$ sobre todo $v\in M_K$, se sigue que

$$h(Bu_l) \leq \left(\frac{\lambda_l}{2}\right)^{\frac{r}{d}}\left(\frac{(\lambda_l)^2}{2\pi}\right)^{\frac{s}{d}} = \frac{\lambda_l}{2}\left(\frac{2}{\pi}\right)^{\frac{s}{d}}.$$

Multiplicando sobre todo $l\in\{1,\ldots,L\}$, obtenemos

$$2^L\left(\frac{\pi}{2}\right)^{\frac{sL}{d}}\prod_{l=1}^{L}h(Bu_l) \leq \lambda_1\lambda_2\cdots\lambda_L\ .$$

Combinando la cota superior y la cota inferior encontradas para el producto de los mínimos sucesivos, deducimos (4.6).

Finalmente, observemos que, como $Bu_l\in K^N$, (4.10) implica que $Bu_l\in(\mathcal{O}_K)^N$. □

Ahora procedemos a probar el lema de Bombieri-Vaaler.

Sea $L := N-M$. Sea $y_1,\ldots y_L\in K^N$ una base de soluciones de $Ax=0$, y sea $B=(y_1\ \ y_2\ \ \cdots\ \ y_L)$ la matriz $N\times L$ cuyas columnas son exactamente los vectores de dicha base. Notar que la imagen de B es igual al núcleo de A.

Por el teorema anterior, existen $x_1,\ldots,x_L\in\mathcal{O}_K$ que forman una base de la imagen de B (y, por lo tanto, del espacio de soluciones de $Ax=0$) y satisfacen la desigualdad

$$\prod_{l=1}^{L}h(x_l) \leq \left\{\left(\frac{2}{\pi}\right)^s\sqrt{|D_{K/\mathbb{Q}}|}\right\}^{\frac{L}{d}}H(B)\ .$$

Para completar la prueba, basta con ver que $H(A)=H(B)$. Esto se desprende fácilmente del siguiente lema.

Lema 4.2.5. *Sea K un cuerpo arbitrario y sea $|\cdot|_v$ un valor absoluto de K. Sea A una matriz $M \times N$ de rango $M < N$ con entradas en K. Sea B una matriz $N \times (N-M)$ cuyas columnas forman una base del núcleo de A; es decir, $AB = 0$. Luego, existe una constante $\gamma \in K$ no nula tal que para cada subconjunto $I \subset \{1, \ldots, N\}$ con $|I| = L$,*

$$|\det B_I|_v = |\gamma \det A_J|_v ,$$

donde J es el complemento de I en $\{1, \ldots, N\}$. (De hecho, $\det B_I$ y $\gamma \det A_J$ son iguales salvo signo).

Demostración. A lo largo de la prueba, sea $L = N - M$, y, para cualquier entero positivo n, sea I_n la matriz identidad de tamaño $n \times n$.

Primero, supongamos que A y B son de la forma

$$A = \left(\, I_M \, \middle| \, C \, \right), \quad B = \begin{pmatrix} -C \\ \hline I_L \end{pmatrix}. \tag{4.11}$$

No es difícil ver que para cualquier I y J como en el teorema, $\det B_I$ y $\det A_J$ son iguales salvo signo. En efecto, para ciertos r, s, podemos escribir

$$I = \{i_1, \ldots, i_L\},\ i_1 < \ldots < i_r \leq M < i_{r+1} < \ldots < i_L$$

y

$$J = \{j_1, \ldots, j_L\},\ j_1 < \ldots < j_s \leq M < j_{s+1} < \ldots < j_M .$$

Notar que $r + s = M$, porque $\{1, \ldots, M\} = \{i_1, \ldots, i_r, j_1, \ldots, j_s\}$. Consideremos dos permutaciones $\eta \in S_M$ y $\psi \in S_L$ definidas por

$$\eta(m) = \begin{cases} j_m & \text{si } m = 1, \ldots, s \\ i_{ms} & \text{si } m = s+1, \ldots, M , \end{cases}$$

y

$$\psi(l) = \begin{cases} j_{r+l} - M & \text{si } l = 1, \ldots, r \\ i_l - M & \text{si } m = r+1, \ldots, L . \end{cases}$$

Calculemos los determinantes correspondientes:

$$\begin{aligned}\det A_J &= \sum_{\sigma\in S_M} \operatorname{sgn}(\sigma)\delta_{\sigma(1),\,j_1}\cdots\delta_{\sigma(s),\,j_s}c_{\sigma(s+1),\,j_{s+1}-M}\cdots c_{\sigma(M),\,j_M-M}\\ &= \operatorname{sgn}(\eta)\sum_{\sigma\in S_M} \operatorname{sgn}(\sigma)\delta_{\eta\sigma(1),\,j_1}\cdots\delta_{\eta\sigma(s),\,j_s}c_{\eta\sigma(s+1),\,j_{s+1}-M}\cdots c_{\eta\sigma(M),\,j_M-M}\\ &= \operatorname{sgn}(\eta)\sum_{\tau\in S_r} \operatorname{sgn}(\tau)c_{\eta(s+\tau(1)),\,j_{s+1}-M}\cdots c_{\eta(s+\tau(r)),\,j_M-M}\\ &= \operatorname{sgn}(\eta)\det\left(c_{i_l,\,j_{s+m}-M}\right)_{l,m}\ ;\end{aligned}$$

$$\begin{aligned}\det B_I &= \sum_{\sigma\in S_L} \operatorname{sgn}(\sigma)c_{i_1,\sigma(1)}\cdots c_{i_r,\sigma(s)}\delta_{i_{r+1}-M,\sigma(r+1)}\cdots\delta_{i_L-M,\sigma(M)}\\ &= \operatorname{sgn}(\psi)\sum_{\tau\in S_r} \operatorname{sgn}(\tau)c_{i_1,\psi(\tau(1))}\cdots c_{i_r,\psi(\tau(r))}\\ &= \operatorname{sgn}(\psi)\det\left(c_{i_l,j_{s+m}-M}\right)_{l,m}\ .\end{aligned}$$

Por lo tanto, $\det B_I = \operatorname{sgn}(\psi)\operatorname{sgn}(\eta)\det A_J$.

Ahora abordamos el caso general. Dado que A es de rango M, permutando columnas podemos suponer que

$$A = \left(\ X \,\middle|\, A_2\ \right),$$

con X una matriz inversible de tamaño $M\times M$ y A_2 una cierta matriz $M\times L$. Entonces,

$$A = XA',$$

con

$$A' := \left(\ I_M; \,\middle|\, X^{-1}A_2\ \right)$$

una matriz de la forma (4.11). Se puede deducir fácilmente que, en este caso, existe una matriz invertible $Y\in K^{L\times L}$ tal que $B = B'Y$. En particular, notar que para cualquier I y J como en el teorema, $A_J = XA'_J$ y $B_I = B'_IY$. Por lo tanto,

$$\begin{aligned}|\det B_I|_v &= |\det B'_I|_v\,|\det Y|_v\\ &= |\det A'_J|_v\,|\det Y|_v\\ &= |\det A_J|_v\,|\det X|_v^{-1}\,|\det Y|_v.\end{aligned}$$

Tomando $\gamma = \det Y(\det X)^{-1}\in K$, concluimos la prueba del lema. □

Para terminar la prueba de Teorema 4.2.1, usamos Lema 4.2.5 y la fórmula del producto para obtener

$$H(B) = (\prod_{v\in M_K} |\gamma|_v)H(A) = H(A)\,.$$

Hasta ahora hemos trabajado con la altura homogénea. Siguiendo un argumento análogo, veremos que se puede probar un teorema similar que involucra la altura inhomogénea. Primero, necesitamos una versión inhomogénea de Teorema 4.2.4.

Teorema 4.2.6. *Sea B una matriz $N \times L$ sobre K de rango $L < N$. Luego existen L vectores linealmente independientes $u_1, u_2, \ldots, u_L$ en K^L tales que $Bu_l \in (\mathcal{O}_k)^N$ para cada l y*

$$\prod_{l=1}^{L} h_{in}(u_l) \leq |D_{K/\mathbb{Q}}|^{\frac{L}{2d}} H(B). \tag{4.12}$$

Demostración. Igual que en la prueba de Teorema 4.2.4, consideramos para cada lugar v el conjunto

$$S_v = \{x \in K_v^L : Bx \in Q_v^N\},$$

donde Q_v^N denota el cubo en K_v^N definido como en la Sección 3.2. Sea $S = \prod_v S_v$.

La prueba de Teorema 4.2.4 se puede adaptar, casi en su totalidad, de forma inmediata a este caso. La única diferencia importante es que necesitamos

$$h_{in}(Bu_l) \leq \frac{\lambda_l}{2}, \tag{4.13}$$

en lugar de

$$h(Bu_l) \leq \frac{\lambda_l}{2}\left(\frac{2}{\pi}\right)^{\frac{s}{d}}. \tag{4.14}$$

Dado que B es una matriz $N \times L$ de rango L, esta define una tranformación lineal inyectiva, con lo cual, en particular, Bu_l tiene alguna de sus coordenadas distinta de cero, digamos, la j-ésima coordenada. Luego, por la fórmula del producto y (4.14),

$$1 = \prod_v |(Bu_l)_j|_v \leq \prod_v \max_{1\leq n\leq N} |(Bu_l)_n|_v \leq \frac{\lambda_l}{2}\left(\frac{2}{\pi}\right)^{\frac{s}{d}}.$$

En particular, esto significa que

$$1 \leq \left(\frac{\pi}{2}\right)^{\frac{s}{d}} \leq \frac{\lambda_l}{2}.$$

Recordemos que, por construcción,

$$\begin{aligned}
|Bu_l|_v = \|Bu_l\|_v^{1/d} &\leq \left(\frac{\lambda_l}{2}\right)^{1/d} && \text{si } v \text{ es real,}\\
|Bu_l|_v = \|Bu_l\|_v^{1/d} &\leq \left(\frac{\lambda_l}{\sqrt{2\pi}}\right)^{2/d} && \text{si } v \text{ es complejo,}\\
|Bu_l|_v = \|Bu_l\|_v^{1/d} &\leq 1 && \text{si } v \text{ es finito.}
\end{aligned}$$

Luego, para cada lugar v finito, $\max\{1, |Bu_l|_v\} \leq 1$. Combinando las estimaciones obtenidas, obtenemos que

$$\begin{aligned}
h_{in}(Bu_l) &\leq \prod_{v|\infty} \max\{1, |Bu_l|_v\}\\
&\leq \left(\frac{\lambda_l}{2}\right)^{r/d} \max\left\{1, \left(\frac{\lambda_l}{\sqrt{2\pi}}\right)^{2s/d}\right\}\\
&\leq \frac{\lambda_l}{2}.
\end{aligned}$$

Con esto concluye la demostración del teorema. □

Si esencialmente rehacemos la demostración de Teorema 4.2.1 usando (4.12) en lugar de (4.6), obtenemos el lema de Bombieri-Vaaler para alturas inhomogéneas.

Teorema 4.2.7 (Lema de Bombieri-Vaaler inhomogéneo)**.** *Sea A una matriz $M \times N$ de rango $M < N$ con entradas en K. Luego existen $N - M$ vectores linealmente independientes $x_1, \ldots, x_{N-M}$ en $(\mathcal{O}_K)^N$ que forman una base del K-espacio vectorial de soluciones de $Ax = 0$. Más aún, estas soluciones satisfacen la desigualdad*

$$\prod_{l=1}^{N-M} h_{in}(x_l) \leq |D_{K/\mathbb{Q}}|^{\frac{N-M}{2d}} H(A)\,.$$

4.3. Generalizaciones

Presentamos ahora una versión más general del lema de Bombieri-Vaaler. Como antes, consideramos un sistema lineal de ecuaciones $Ax = 0$ dado por un matriz A de tamaño $M \times N$ y rango $M < N$ con entradas en un cuerpo de números K, y queremos probar la existencia de una base de soluciones de altura pequeña. La diferencia aquí es que deseamos que sea una base sobre k, para k un subcuerpo de K. Sea $t = [k : \mathbb{Q}]$ y $r = [K : k]$.

Sea F una extensión de Galois finita de k tal que $k \subset K \subset F$; observar que F también es una extensión de Galois finita de K. Notamos $G(F/k)$ y $G(F/K)$ a los respectivos grupos de Galois. Observar que $G(F/K)$ es un subgrupo de $G(F/k)$ de índice r. Sea $\sigma_1, \sigma_2, \ldots, \sigma_r \in G(F/k)$ un conjunto de representantes de las coclases de $G(F/K)$ en $G(F/k)$. Para cada $i = 1, \ldots, r$, escribimos $\sigma_i(A) := (\sigma_i(a_{mn})) \in F^{M\times N}$. Finalmente, definimos la matriz $Mr \times N$

$$\mathcal{A} := \begin{pmatrix} \sigma_1(A) \\ \sigma_2(A) \\ \vdots \\ \sigma_r(A) \end{pmatrix}. \tag{4.15}$$

Teorema 4.3.1. *Sea $\mathcal{A}$ definida como arriba, y supongamos que* $\text{rango}(\mathcal{A}) = Mr < N$. *Luego, existen $N - Mr$ vectores linealmente independientes $x_1, x_2, \ldots, x_{N-Mr} \in (O_k)^N$, que son soluciones de $Ax = 0$ y satisfacen*

$$\prod_{l=1}^{N-Mr} h(x_l) \leq \left\{ \left(\frac{2}{\pi}\right)^s \sqrt{|D_{k/\mathbb{Q}}|} \right\}^{\frac{N-Mr}{t}} H(\mathcal{A}),$$

donde s es el número de lugares complejos de k.

Demostración. Sea $w_1, \ldots, w_r$ una base de K sobre k. Luego, para ciertos $b_{mn}^{(j)} \in k$, podemos escribir

$$a_{mn} = \sum_{j=1}^{r} b_{mn}^{(j)} w_j \tag{4.16}$$

y entonces, para cada $m = 1, \ldots, M$,

$$\sum_{n=1}^{N} a_{mn} x_n = \sum_{j=1}^{r} \left(\sum_{n=1}^{N} b_{mn}^{(j)} x_n \right) w_j .$$

Se sigue que $x \in k^N$ es una solución de $Ax = 0$ si y solo si es una solución del sistema

$$\sum_{n=1}^{N} b_{mn}^{(j)} x_n = 0, \quad m = 1, \ldots, M, \ j = 1, \ldots, r. \tag{4.17}$$

El sistema (4.17) se puede representar con una matriz $\mathcal{B} \in k^{Mr\times N}$ definida por

$$\mathcal{B} = \begin{pmatrix} B(1) \\ B(2) \\ \vdots \\ B(r) \end{pmatrix},$$

donde, para cada $j = 1, \dots, r$, $B(j) := (b_{mn}^{(j)})_{m,n}$.

Aplicando el Teorema 4.2.1 para el cuerpo de números k y la matriz $\mathcal{B}$, sabemos que hay $N - Mr$ vectores linealmente independientes $x_1, x_2, \dots, x_{N-Mr} \in (O_k)^N$ que son soluciones de $\mathcal{B}x = 0$ y satisfacen

$$\prod_{l=1}^{N-Mr} h(x_l) \leq \left\{ \left(\frac{2}{\pi}\right)^s \sqrt{|D_{K/\mathbb{Q}}|} \right\}^{\frac{N-M}{t}} H(\mathcal{B})\,.$$

Para concluir la demostración, basta con ver que $H(\mathcal{B}) = H(\mathcal{A})$. Sea Ω la matriz $Mr \times Mr$ con entradas en F definida por

$$\Omega = \begin{pmatrix} \sigma_1(w_1)I_M & \cdots & \sigma_1(w_r)I_M \\ \sigma_2(w_1)I_M & \cdots & \sigma_2(w_r)I_M \\ \vdots & & \vdots \\ \sigma_r(w_1)I_M & \cdots & \sigma_r(w_r)I_M \end{pmatrix},$$

donde I_M es la matriz de identidad $M \times M$. Observar que si aplicamos σ_i a (4.16), obtenemos

$$\sigma_i(a_{mn}) = \sum_{j=1}^{r} b_{mn}^{(j)} \sigma_i(w_j)\,,$$

y por lo tanto

$$\Omega\mathcal{B} = \mathcal{A}.$$

Por Proposición 1.5.6, el hecho de que Ω sea no singular implica que $H(\mathcal{B}) = H(\mathcal{A})$. □

Observación. En el teorema anterior, la altura de $\mathcal{A}$ se calcula con respecto al cuerpo F. Según Teorema 4.2.1, la altura de $\mathcal{B}$ debe calcularse con respecto al cuerpo k; sin embargo, por Proposición 1.5.8, es la misma que la altura con respecto a F. Entonces, $H(\mathcal{B}) = H(\mathcal{A})$ es una igualdad de alturas de matrices con entradas en F.

En algunas situaciones, puede ser más conveniente tener el Teorema 4.3.1 con una cota que no dependa de $\mathcal{A}$, sino de la altura de A o incluso de la altura de las filas de A. En lo que sigue, $A(m)$ denota la m-ésima fila de A.

Lema 4.3.2. *Supongamos que $\mathcal{A}$ está en las hipótesis del Teorema 4.3.1. Entonces*

$$H(\mathcal{A}) \leq H(A)^r \leq \prod_{m=1}^{M} H(A(m))^r.$$

En particular, estas cotas pueden ser usadas en el lado derecho de la desigualdad del Teorema 4.3.1.

Demostración. Por la Proposición 1.5.7,

$$H(\mathcal{A}) \leq \prod_{i=1}^{r} H(\sigma_i(A)).$$

Como consecuencia de la Proposición 1.1.16, $H(\sigma_i(A)) = H(A)$. Luego, una segunda aplicación de la Proposición 1.5.7 da

$$H(\mathcal{A}) \leq H(A)^r \leq \prod_{m=1}^{M} H(A(m))^r.$$

□

Para terminar, describimos una forma en que Teorema 4.3.1 podría ser modificado.

Es posible que la matriz A se pueda dividir en bloques

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_L \end{pmatrix},$$

de forma que A_l sea una matriz $M_l \times N$ sobre un cuerpo de números K_l con $[K_l : k] = r_l$, para cada $l = 1, \ldots, L$. Sea F una extensión de Galois finita de k que contiene cada K_l. Para cada A_l, definimos la matriz $\mathcal{A}_l \in (K_l)^{M_l r_l \times N}$ como en (4.15), y luego juntamos todas estas matrices en una matriz de tamaño $(\sum_{l=1}^{L} M_l\, r_l) \times N$ definida por

$$\mathcal{Z} := \begin{pmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \\ \vdots \\ \mathcal{A}_L \end{pmatrix}.$$

Haciendo algunas pequeñas modificaciones a la demostración del Teorema 4.3.1, obtenemos

Teorema 4.3.3. *En el contexto anterior, supongamos que* $z = rango(\mathcal{Z}) = \sum_{l=1}^{L} M_l\, r_l < N$. *Entonces, existen* $N - z$ *vectores linealmente independientes* $x_1, \ldots, x_N$ *en* $(\mathcal{O}_k)^N$ *que son soluciones de* $Ax = 0$ *y satisfacen*

$$\prod_{l=1}^{N-z} h(x_l) \leq \left\{ \left(\frac{2}{\pi}\right)^s \sqrt{|D_{k/\mathbb{Q}}|} \right\}^{\frac{N-z}{t}} H(\mathcal{Z}), \tag{4.18}$$

donde s es el número de lugares complejos de k. Más aún, en el lado derecho de (4.18) podemos usar

$$H(\mathcal{Z}) \leq \prod_{l=1}^{L} H(A_l)^{r_l}.$$

Bibliografía

[1] T. M. Apostol. *Mathematical Analysis, Second Edition*. Pearson, 1974.

[2] E. Bombieri and W. Gubler. *Heights in Diophantine Geometry*. Cambridge University Press, 2007.

[3] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. math.*, 73:11–13, 1983.

[4] H. Davenport. Minkowski's inequality for the minima associated with a convex body. *Q. J. Math.*, 10:119–121, 1939.

[5] Z. Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22.4:1093–1097, 2009.

[6] T. Estermann. Note on a theorem of Minkowski. *J. London Math. Soc.*, 21:179–182, 1946.

[7] F. Gouvea. *p-adic Numbers*. Springer-Verlag Berlin Heidelberg, 1997.

[8] N. Jacobson. *Basic Algebra II: Second Edition*. Dover Publications, 2009.

[9] S. Lang. *Algebra*. Springer-Verlag New York, 2002.

[10] D. Masser. *Auxiliary Polynomials in Number Theory*. Cambridge University Press, 2016.

[11] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1989.

[12] L. Nachbin. *The Haar integral*. Van Nostrand, 1965.

[13] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999.

[14] A. Prekopa. On logarithmically concave measures and functions. *Acta. Math. Acad. Hungar*, pages 335–343, 1973.

[15] D. Ramakrishnan and R. J. Valenza. *Fourier Analysis on Number Fields*. Springer-Verlag New York, 1999.

[16] A. Sutherland. MIT Mathematics 18.785, Lecture Notes: Number Theory I, 2016. URL: http://math.mit.edu/classes/18.785/2016fa/lectures.html.

[17] T. Tao. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics. *EMS Surv. Math. Sci.*, 1.1:1–46, 2014.

[18] J. D. Vaaler. A geometric inequality with applications to linear forms. *Pacific J. Math.*, 83:543–553, 1979.

[19] M. N. Walsh. Bounded rational points on curves. *Int. Math. Res. Not. IMRN*, 14:5644–5658, 2014.

[20] M. N. Walsh. *Characteristic subsets and the polynomial method*. Proceedings of the International Congress of Mathematicians, 2018.

Índice alfabético