

# EQUIDISTRIBUCIÓN, TEORÍA DEL POTENCIAL Y APLICACIONES ARITMÉTICAS

JOSÉ IGNACIO BURGOS GIL AND RICARDO MENARES

RESUMEN. En este curso daremos una breve introducción a la teoría del potencial en el plano complejo así como varias aplicaciones aritméticas. Entre las aplicaciones aritméticas veremos el Teorema de Fekete-Szegö y el Teorema de Equidistribución de Bilu.

## ÍNDICE

1. Introducción	2
2. Generalidades sobre números algebraicos	2
2.1. Números algebraicos	2
2.2. Órbita galoisiana	5
2.3. Discriminante y Resultante	6
3. Teoría del potencial y el teorema de Fekete-Szegö	7
3.1. Puntos de Fekete.	8
3.2. Medidas y convergencia débil	12
3.3. La capacidad logarítmica	14
3.4. La constante de Chebyshev	17
3.5. Potenciales y funciones armónicas	20
3.6. Demostración del Teorema de Frostman	23
3.7. El teorema de la lemniscata de Hilbert	24
3.8. Las órbitas de Galois y el teorema de Fekete.	25
3.9. El teorema de Fekete-Szegö	26
3.10. Equidistribución de órbitas de Galois en el caso de capacidad uno	28
4. Alturas y teorema de Bilu	29
4.1. Medida de Mahler de un polinomio en una variable	29
4.2. Altura de un número algebraico	30
4.3. Enunciado del Teorema de Bilu en dimensión 1	31
4.4. Energía	33
4.5. Demostración del Teorema de Bilu	35
5. Generalizaciones y aplicaciones diofantinas	37
Referencias	38

---

*Date:* La fecha de envío del documento.

2010 *Mathematics Subject Classification.* XXWXX.

El primer autor ha sido apoyado parcialmente por los proyectos MINECO MTM2016-79400-P e ICMAT Severo Ochoa project SEV-2015-0554.

El segundo autor contó con apoyo del proyecto Fondecyt 1171329.

Estas notas corresponden al curso dictado por los autores en la escuela AGRA III, Aritmética, Grupos y Análisis, del 9 al 20 de Julio de 2018 en Córdoba, Argentina.

## 1. INTRODUCCIÓN

En muchas situaciones en el estudio de ecuaciones diofantinas, es posible establecer la distribución asintótica de familias distinguidas de puntos algebraicos, en cuyo caso decimos que hay equidistribución de la familia.

Un ejemplo básico de este fenómeno es el caso de las raíces de la unidad. Denotamos por  $\mathbb{D} = \{z \in \mathbb{C} : |z| \leq 1\}$  al disco unitario. Las soluciones complejas de la ecuación  $x^n = 1$  se sitúan sobre el borde de  $\mathbb{D}$  formando los vértices de un polígono regular de  $n$  lados. Cuando  $n$  crece el polígono aproxima cada vez mejor al círculo, de donde se deduce que en el límite, las raíces de la unidad se distribuyen siguiendo la medida uniforme del círculo.

En este curso presentaremos el Teorema de Fekete-Szegö y el Teorema de Bilu, que constituyen generalizaciones diferentes de este fenómeno. En el primer caso, buscaremos reemplazar  $\mathbb{D}$  por otro conjunto, en el segundo caso buscaremos reemplazar la familia de ecuaciones  $x^n = 1$ .

En el contexto del Teorema de Fekete-Szegö, reemplazamos  $\mathbb{D}$  por un conjunto compacto  $K \subseteq \mathbb{C}$ , invariante por conjugación compleja. ¿Bajo qué condiciones podemos afirmar que hay una familia infinita de enteros algebraicos, cuyos conjugados están en  $K$  y que se equidistribuye con respecto a alguna medida natural? No es difícil ver que un disco centrado en el origen y de radio menor que 1 contiene solo un conjunto de conjugados de un entero algebraico, el punto cero. Esto sugiere que el conjunto  $K$  debiese tener "suficiente tamaño aritmético", en algún sentido a precisar. La noción adecuada de tamaño resulta ser la *capacidad* de  $K$ , concepto proveniente de la teoría del potencial.

En el contexto del Teorema de Bilu, es instructivo considerar la familia de ecuaciones  $(x - 1)^n = 0$ , que tiene una única solución. Lo que hace diferente esta familia de  $x^n = 1$  es el tamaño de los coeficientes del polinomio que determina la ecuación. La noción adecuada de tamaño es la *altura* de un número algebraico. Se demuestra que una sucesión de números algebraicos de altura que tiende a cero, tiene la propiedad que sus conjugados se equidistribuyen con respecto a la medida uniforme en el círculo unitario.

En la Sección 2 presentamos un resumen de algunas propiedades básicas de los números algebraicos que serán usadas en este curso. Luego en la Sección 3 presentamos las nociones de la teoría del potencial necesarias para formular y demostrar el Teorema de Fekete-Szegö. Por último, en la Sección 4 explicamos la noción de altura y la demostración del Teorema de Bilu.

## 2. GENERALIDADES SOBRE NÚMEROS ALGEBRAICOS

## 2.1. Números algebraicos.

**Definición 2.1.** Un elemento  $\alpha \in \mathbb{C}$  se dice *número algebraico* si existe un polinomio no constante, con coeficientes racionales,  $f(x) \in \mathbb{Q}[x]$ , tal que  $f(\alpha) = 0$ . Un número algebraico se denomina *entero algebraico* si el polinomio  $f$  se puede elegir mónico (es decir, el coeficiente del término dominante es 1) y con coeficientes enteros  $f(x) \in \mathbb{Z}[x]$ .

Notar que todo número racional es algebraico. En efecto, si  $\alpha = \frac{a}{b}$ , con  $a, b \in \mathbb{Z}$  y  $b \neq 0$ , entonces podemos tomar  $f(x) = x - \frac{a}{b}$ . Sin embargo, solo los números enteros son, a la vez, racionales y enteros algebraicos. Más ejemplos:

**Ejemplo 2.2.**

1.  $\alpha = i$ ,  $f(x) = x^2 + 1$
2.  $\alpha = \sqrt{2}$ ,  $f(x) = x^2 - 2$
3.  $\alpha = \sqrt[3]{2}$ ,  $f(x) = x^3 - 2$
4.  $\alpha = \zeta_n := e^{2\pi i/n}$ ,  $f(x) = x^n - 1$ ,  $n \in \mathbb{Z}_{>0}$
5.  $\alpha = \frac{1+\sqrt{5}}{2}$ ,  $f(x) = x^2 - x - 1$

6.  $\alpha = \sqrt{2}/2, \quad f(x) = 2x^2 - 1$

Todos los ejemplos anteriores, salvo el último, son enteros algebraicos.

Denotamos  $\overline{\mathbb{Q}}$  al conjunto de los números algebraicos. Notar que  $\overline{\mathbb{Q}}$  es un conjunto numerable. En efecto,  $\mathbb{Q}[x]$  es numerable y cada elemento no constante de  $\mathbb{Q}[x]$  tiene a lo más un número finito de raíces. Dado que  $\mathbb{C}$  no es numerable, se desprende que existen números que no son algebraicos (y de hecho son mayoría). Sin embargo, no es fácil identificar un número no algebraico. Por ejemplo, se sabe que  $e$  (Hermite 1873) y  $\pi$  (Lindemann 1882) no son algebraicos, pero a la redacción de estas líneas no se sabe decidir si  $e + \pi$  es algebraico o no.

El polinomio  $f(x)$  que figura en la Definición 2.1 no es único. Cualquier polinomio de la forma  $h(x) = f(x)g(x)$ , con  $g(x) \in \mathbb{Q}[x]$ , sirve también. Sin embargo, nos será útil contar con un polinomio asociado de manera canónica a un número algebraico.

**Proposición 2.3.** *Sea  $\alpha \in \overline{\mathbb{Q}}$ . Entonces existe un único polinomio no constante  $f_\alpha(x)$  que cumple*

1.  $f_\alpha(x)$  tiene coeficientes racionales
2.  $f_\alpha(\alpha) = 0$
3.  $f_\alpha(x)$  es mónico
4. el grado de  $f_\alpha(x)$  es mínimo entre los polinomios que satisfacen (1), (2) y (3)

*Demostración.* el principio del buen orden nos asegura que existe un polinomio  $f(x) \in \mathbb{Q}[x]$  que satisface las cuatro propiedades del enunciado. Si  $g(x)$  es otro polinomio que cumple las mismas propiedades, entonces podemos aplicar división de polinomios

$$f(x) = q(x)g(x) + r(x), \quad q(x), r(x) \in \mathbb{Q}[x], \quad \deg r(x) < \deg g(x).$$

Como  $r(\alpha) = f(\alpha) - q(\alpha)g(\alpha) = 0$ , de la minimalidad del grado de  $f(x)$  concluimos que  $r(x)$  es el polinomio nulo, es decir  $f(x) = q(x)g(x)$ . Como  $f$  y  $g$  tienen el mismo grado y son mónicos, entonces  $f = g$ . □

**Definición 2.4.** ■ Decimos que el polinomio  $f_\alpha(x)$  dado por la Proposición 2.3 es el *polinomio mínimo* de  $\alpha$ .

- Definimos el *grado de  $\alpha$*  por  $\deg \alpha := \deg f_\alpha$ .

**Definición 2.5.** Un polinomio  $f(x) \in \mathbb{Q}[x]$  se dice  $\mathbb{Q}$ -reductible si se puede escribir como producto de polinomios, con coeficientes racionales, de grado estrictamente menor. Un polinomio en  $\mathbb{Q}[x]$  que no es  $\mathbb{Q}$ -reductible se dice  $\mathbb{Q}$ -irreductible.

**Observación:** la minimalidad del grado de  $f_\alpha(x)$  asegura que éste es un polinomio  $\mathbb{Q}$ -irreductible. Recíprocamente, se tiene el siguiente resultado.

**Proposición 2.6.** *Sea  $\alpha \in \overline{\mathbb{Q}}$  y sea  $f(x) \in \mathbb{Q}[x]$  un polinomio  $\mathbb{Q}$ -irreductible y mónico tal que  $f(\alpha) = 0$ . Entonces  $f = f_\alpha$ .*

*Demostración.* aplicar el algoritmo de la división para polinomios. □

**Definición 2.7.** Dado un polinomio

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x],$$

definimos el *polinomio reverso*

$$f^*(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \mathbb{C}[x].$$

**Lema 2.8.** *Si  $f(x) \in \mathbb{Q}[x]$  es  $\mathbb{Q}$ -irreductible, entonces  $f^*(x)$  también lo es.*

*Demostración.* basta notar que  $f^*(x) = x^{\deg f} f(1/x)$  y usar la Definición 2.5. □

De la Proposición 2.6 y el Lema 2.8, se deduce

**Corolario 2.9.** Si  $\alpha \in \overline{\mathbb{Q}}$  y  $\alpha \neq 0$ , entonces  $1/\alpha \in \overline{\mathbb{Q}}$ . Más aún,  $f_{1/\alpha} = f_\alpha^*$ .

No siempre es fácil determinar el polinomio mínimo de un número algebraico. En los ejemplos 2.2, los polinomios indicados son todos irreducibles (luego coinciden con el polinomio mínimo) excepto en el Ejemplo 2.2, (4). En efecto,

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Dos herramientas básicas para decidir la irreducibilidad de un polinomio con coeficientes racionales son el Lema de Gauss y el Criterio de Eisenstein, que procedemos a explicar.

**Definición 2.10.** Un polinomio con coeficientes enteros  $p(x) \in \mathbb{Z}[x]$  se dice  $\mathbb{Z}$ -reducible si existen polinomios  $f(x), g(x) \in \mathbb{Z}[x]$  tales que

- $f(x), g(x) \notin \{\pm 1\}$
- $p(x) = f(x)g(x)$

Diremos que  $p(x) \in \mathbb{Z}[x]$  es  $\mathbb{Z}$ -irreducible si no es  $\mathbb{Z}$ -reducible.

**Teorema 2.11.** (Lema de Gauss) Un polinomio  $p(x) \in \mathbb{Z}[x]$  que es  $\mathbb{Z}$ -irreducible es también  $\mathbb{Q}$ -irreducible.

**Teorema 2.12.** (Criterio de Eisenstein) Sea  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  un polinomio con coeficientes enteros. Suponga que existe un número primo  $p$  tal que

- $p|a_i, \quad i = 0, 1, \dots, n-1$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Entonces  $f(x)$  es  $\mathbb{Q}$ -irreducible.

La demostración de estos teoremas está esbozada en los Ejercicios 2.15, (4) y (5).

Denotamos por  $\Phi_n(x)$  al polinomio mínimo de  $\zeta_n = e^{2\pi i/n}$ .

*Observación 2.13.* Se tiene que  $\Phi_n(x)$  es un divisor (en  $\mathbb{Q}[x]$ ) del polinomio  $x^n - 1$  (cf. Ejercicio 2.15 (1)). Del lema de Gauss, deducimos que  $\Phi_n(x) \in \mathbb{Z}[x]$ .

Como aplicación de los teoremas anteriores, demostraremos el siguiente

**Lema 2.14.** Sea  $p$  un número primo. Entonces  $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ . En particular,

$$x^p - 1 = (x - 1)\Phi_p(x).$$

*Demostración.* Sea  $w(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ . Veamos que  $w(x)$  es un polinomio  $\mathbb{Q}$ -irreducible. Esto último equivale a demostrar que  $h(x) := w(x+1)$  es  $\mathbb{Q}$ -irreducible. Usando la identidad  $x^p - 1 = (x - 1)w(x)$ , se tiene

$$h(x) = w(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \left( \sum_{k=2}^{p-1} \binom{p}{k} x^{k-1} \right) + p.$$

Dado que  $p \nmid \binom{p}{k}$ , para todo  $0 < k < p$ , el criterio de Eisenstein permite concluir que  $h(x)$  es  $\mathbb{Q}$ -irreducible. Tenemos entonces que  $w(x)$  es  $\mathbb{Q}$ -irreducible y mónico, luego  $w(x) = \Phi_p(x)$  por la Proposición 2.6.  $\square$

*Ejercicios 2.15.* 1. Sea  $f(x) \in \mathbb{Q}[x]$  un polinomio  $\mathbb{Q}$ -irreducible y sea  $\alpha \in \mathbb{C}$  tal que  $f(\alpha) = 0$ . Sea  $g(x) \in \mathbb{Q}[x]$  un polinomio no constante tal que  $g(\alpha) = 0$ . Demuestre que existe un polinomio  $h(x) \in \mathbb{Q}[x]$  tal que  $g(x) = f(x)h(x)$ .

2. Un polinomio  $p(x)$  se dice que tiene raíces repetidas si se puede factorizar sobre  $\mathbb{C}$  de la forma

$$p(x) = (x - z)^2 h(x), \quad z \in \mathbb{C}, \quad h(x) \in \mathbb{C}[x]$$

(de manera equivalente,  $p(z) = p'(z) = 0$ ). Demuestre que un polinomio  $\mathbb{Q}$ -irreducible  $p(x) \in \mathbb{Q}[x]$  no puede tener raíces repetidas.

3. Sea  $p$  un primo. Denotamos  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ , el cuerpo finito de  $p$  elementos. Sea

$$\nu : \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

el morfismo canónico. Para un polinomio con coeficientes enteros  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , definimos

$$\bar{f}(x) = \nu(a_n) x^n + \nu(a_{n-1}) x^{n-1} + \dots + \nu(a_1) x + \nu(a_0) \in \mathbb{F}_p[x].$$

Muestre que la operación  $f \mapsto \bar{f}$  define un morfismo de anillos  $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$  (es decir, verifique  $\overline{f+g} = \bar{f} + \bar{g}$  y  $\overline{fg} = \bar{f}\bar{g}$ ).

4. *Lema de Gauss.* Decimos que un polinomio  $f(x) \in \mathbb{Z}[x]$  es *reducido* si el máximo común divisor de sus coeficientes es 1.

a) Sean  $f(x), g(x) \in \mathbb{Z}[x]$  dos polinomios y sea  $h(x) = f(x)g(x)$ . Sea  $N$  el máximo común divisor de los coeficientes de  $h(x)$ . Suponga  $N \neq 1$  y tome un primo  $p$  tal que  $p|N$ . Usando el morfismo de anillos del ejercicio anterior, demuestre que  $p$  o bien divide a todos los coeficientes de  $f(x)$  o bien divide a todos los coeficientes de  $g(x)$

b) Deduzca que el producto de dos polinomios reducidos es reducido

c) Demuestre el Teorema 2.11

5. *Criterio de Eisenstein.* Sean  $f(x) \in \mathbb{Z}[x]$  un polinomio y  $p$  un primo que satisfacen las hipótesis del Teorema 2.12.

a) Suponga que se puede factorizar  $f(x) = g(x)h(x)$  con  $g(x), h(x) \in \mathbb{Z}[x]$ . Muestre que entonces se tiene

$$\nu(a_n)x^n = \bar{g}(x)\bar{h}(x), \quad \text{en } \mathbb{F}_p[x].$$

b) Justifique que  $\bar{g}(x) = ux^a, \bar{h}(x) = vx^b$ , con  $u, v \in \mathbb{F}_p^*$  y  $a + b = n$ .

c) Demuestre el Teorema 2.12.

6. Pruebe que  $\overline{\mathbb{Q}}$  es un cuerpo. Es decir,

$$\alpha, \beta \in \overline{\mathbb{Q}}, \alpha \neq 0 \Rightarrow \frac{1}{\alpha}, \alpha\beta, \alpha + \beta \in \overline{\mathbb{Q}}.$$

## 2.2. Órbita galoisiana.

**Definición 2.16.** ■ Sean  $\alpha \in \overline{\mathbb{Q}}$  y  $f_\alpha(x)$  su polinomio mínimo. Decimos que  $\beta \in \mathbb{C}$  es un *conjugado* de  $\alpha$  si  $f_\alpha(\beta) = 0$ .

■ Definimos la *órbita galoisiana* de  $\alpha$  por

$$\begin{aligned} \text{Gal}(\alpha) &:= \{\beta \in \mathbb{C} : \beta \text{ es un conjugado de } \alpha\} \\ &= \{\beta \in \mathbb{C} : f_\alpha(\beta) = 0\} \end{aligned}$$

*Observación 2.17.* El número de conjugados de  $\alpha$  es exactamente el grado de  $f_\alpha(x)$  (ver Ejercicio 2.15, (2)).

**Ejemplo 2.18.** ■  $\text{Gal}(i) = \{i, -i\}$

■  $\text{Gal}(\sqrt{2}) = \{\sqrt{2}, -\sqrt{2}\}$

■  $\text{Gal}(\sqrt[3]{2}) = \{\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}\}$

■  $\text{Gal}\left(\frac{1+\sqrt{5}}{2}\right) = \left\{\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$

Es de interés para nosotros calcular la órbita galoisiana de  $\zeta_n$ . Definimos

$$\begin{aligned}\mu_n &:= \{z \in \mathbb{C} : z^n = 1\} = \{\text{raíces de la unidad de orden } n\} \\ \tilde{\mu}_n &:= \{z \in \mu_n : z^k \neq 1, \quad \forall 1 \leq k < n\} = \{\text{raíces primitivas de la unidad de orden } n\}\end{aligned}$$

Notar que  $(\mu_n, \cdot)$  es un grupo cíclico de orden  $n$ . Más precisamente, si  $\zeta_n = e^{2\pi i/n}$ , entonces  $\mu_n = \{\zeta_n^j : 0 \leq j \leq n-1\}$ . Más aún, se tiene

$$(2.1) \quad \tilde{\mu}_n = \{\zeta_n^j : \text{mcd}(j, n) = 1\}.$$

En particular, el número de elementos de  $\tilde{\mu}_n$  es

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| = \#\{1 \leq j \leq n-1 : \text{mcd}(j, n) = 1\}$$

(función de Euler).

**Proposición 2.19.** *Sea  $\zeta_n = e^{2\pi i/n}$ . Entonces*

$$\text{Gal}(\zeta_n) = \tilde{\mu}_n.$$

La demostración de este hecho está esbozada en los ejercicios 2.21.

**Corolario 2.20.** *Se tiene  $\deg \Phi_n = \varphi(n)$ , para todo entero positivo  $n$ .*

*Ejercicios 2.21.* 1. Demuestre (2.1).

2. a) Demuestre que para todo  $\alpha \in \overline{\mathbb{Q}}$  y todo entero positivo  $k$ , se tiene

$$\text{Gal}(\alpha^k) = \{\beta^k : \beta \in \text{Gal}(\alpha)\}.$$

Deduzca  $\deg(\alpha^k) \leq \deg(\alpha)$ .

b) Muestre que para  $\alpha \in \overline{\mathbb{Q}}^*$ , se tiene  $\text{Gal}(1/\alpha) = \{1/\beta : \beta \in \text{Gal}(\alpha)\}$ . Deduzca  $\deg(\alpha) = \deg(1/\alpha)$ .

3. Sean  $n$  un entero y  $p$  un número primo que no divide  $n$ . Sea  $\alpha \in \mathbb{C}$  tal que  $\Phi_n(\alpha) = 0$ . El objetivo de este problema es demostrar que  $\Phi_n(\alpha^p) = 0$ .

a) Muestre que  $\alpha^p \in \overline{\mathbb{Q}}$  y que su polinomio mínimo tiene coeficientes enteros.

b) Suponga que  $\Phi_n(\alpha^p) \neq 0$ . Sea  $g(x) \in \mathbb{Z}[x]$  el polinomio mínimo de  $\alpha^p$ . Sea  $h(x) = g(x^p)$ . Muestre que  $\Phi_n(x) | h(x)$  en  $\mathbb{Z}[x]$ .

c) Sea  $j(x) \in \mathbb{F}_p[x]$  un factor irreducible de  $\overline{\Phi}_n(x) \in \mathbb{F}_p[x]$  (cf. la operación

$$f \in \mathbb{Z}[x] \mapsto \bar{f} \in \mathbb{F}_p[x]$$

definida en el Ejercicio 2.15 (3)). Muestre que  $j(x) | \bar{g}(x)$ .

d) Use lo anterior para mostrar que  $j(x)^2 | x^n - 1$ . Concluya.

4. Use el ejercicio anterior para demostrar la Proposición 2.19.

**2.3. Discriminante y Resultante.** Sea  $f(x) \in \mathbb{C}[x]$  un polinomio y lo expresamos en términos de sus raíces como

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad a, \alpha_1, \dots, \alpha_n \in \mathbb{C}.$$

Notar que las raíces  $\alpha_1, \alpha_2, \dots, \alpha_n$  no son necesariamente distintas. Se define el *discriminante* de  $f$  por

$$D(f) = a^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

Es inmediato de la definición que  $D(f) = 0$  si y solo si  $f$  tiene raíces repetidas.

**Definición 2.22.** Sean

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x] \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 \in \mathbb{C}[x]. \end{aligned}$$

Formamos la siguiente matriz de tamaño  $(n+m) \times (n+m)$

$$M(f, g) = \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_0 & \dots & 0 \\ & & \dots & & & & \\ 0 & 0 & \dots & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & & \\ 0 & b_m & b_{m-1} & \dots & b_0 & & \\ & & \dots & & & & \\ 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_0 \end{pmatrix}$$

Definimos la *resultante*  $R(f, g)$  por

$$R(f, g) := \det M(f, g).$$

**Teorema 2.23.** ([11], Proposition 8.3, p. 202) *Escribimos  $g(x) = b_m(x - \beta_1) \cdots (x - \beta_m)$ . Entonces se tiene*

$$(2.2) \quad R(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

*Observación 2.24.* De este teorema vemos que  $R(f, g) = 0$  si y solo si  $f$  y  $g$  tienen una raíz en común.

Central en lo que sigue es la siguiente

**Proposición 2.25.** *Si  $f(x)$  tiene coeficientes enteros y  $a_n$  es el coeficiente del término dominante, entonces  $a_n D(f) \in \mathbb{Z}$ .*

*Demostración.* Tomemos  $g = f'$  en (2.2). Entonces  $m = n - 1$  y  $b_m = na_n$ . Si escribimos

$$f'(x) = na_n(x - \beta_1) \cdots (x - \beta_{n-1}),$$

entonces

$$R(f, f') = n^n a_n^{2n-1} \prod_{i=1}^n \frac{f'(\alpha_i)}{na_n} = a_n^{n-1} \prod_{i=1}^n f'(\alpha_i).$$

Pero  $f'(\alpha_i) = a_n \prod_{\substack{j=1 \\ j \neq i}}^n (\alpha_i - \alpha_j)$ , luego obtenemos

$$R(f, f') = a_n^{2n-1} \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2} a_n^{2n-1} \prod_{i < j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} a_n D(f).$$

Como  $f$  y  $f'$  tienen coeficientes enteros, de la definición de resultante tenemos  $R(f, f') \in \mathbb{Z}$  □

### 3. TEORÍA DEL POTENCIAL Y EL TEOREMA DE FEKETE-SZEGÖ

En esta sección vamos a ver los rudimentos de la teoría del potencial en el plano complejo y una primera aplicación aritmética. En concreto, estudiaremos las propiedades de la capacidad logarítmica y de sus otras presentaciones, el diámetro transfinito y la constante de Chebyshev. Como aplicación de este estudio daremos una demostración del teorema de Fekete-Szegö que afirma que la capacidad logarítmica discrimina cuándo un conjunto puede contener infinitas órbitas de Galois de enteros algebraicos.

La presentación está centrada en la comparación entre el diámetro transfinito, la capacidad logarítmica y la constante de Chebyshev. La mayor parte de esta sección está basada en las excelentes notas [16]. Para más detalles y demostraciones que se han omitido, el lector puede consultar [13]. Una presentación moderna del teorema de Fekete-Szegö utilizando teoría de Arakelov se puede encontrar en las notas [1].

**3.1. Puntos de Fekete.** Empezamos con un subconjunto  $E \subset \mathbb{C}$  compacto, es decir  $E$  es un subconjunto de  $\mathbb{C}$  cerrado y acotado, por ejemplo el disco unidad. Dado un entero  $n \geq 2$ , queremos buscar un conjunto de  $n$  puntos de  $E$  que estén lo más alejados posible entre sí. Para dar una idea precisa de qué entendemos por estar lo más alejado posible, definimos la cantidad

$$\delta_n(E) = \max_{z_1, \dots, z_n \in E} \left( \prod_{1 \leq i < j \leq n} |z_i - z_j| \right)^{2/n(n-1)}$$

y buscamos colecciones de puntos donde se alcance esta cantidad. Cualquier colección de puntos  $\mathcal{F}_n = \{z_1^{(n)}, \dots, z_n^{(n)}\}$  con

$$\left( \prod_{1 \leq i < j \leq n} |z_i^{(n)} - z_j^{(n)}| \right)^{2/n(n-1)} = \delta_n(E)$$

se llama un conjunto de Fekete (de  $n$  puntos) y sus elementos puntos de Fekete. Por definición, estos puntos están lo más alejados entre sí dentro de  $E$ .

La primera observación que podemos hacer es que los puntos de Fekete se sitúan siempre en la frontera exterior del subconjunto  $E$  (la frontera exterior es la frontera de la componente conexa no acotada del complementario de  $E$ ). Por ejemplo, si  $E$  es el anillo

$$A = \{z \in \mathbb{C} : r \leq |z| \leq R\},$$

los puntos de Fekete de  $A$  se concentran en la circunferencia de radio  $R$ . Este resultado se puede demostrar usando el principio del máximo de las funciones analíticas.

**Ejemplo 3.1.** Como veremos en el Ejercicio 3.7 (2), si  $E$  es el disco unidad, el conjunto de las raíces de la unidad  $n$ -ésimas es un conjunto de Fekete.

**Ejemplo 3.2.** En el conjunto  $E = [-1, 1]$ , para cada  $n$ , hay un único conjunto de Fekete de  $n$  puntos. Y está dado por los ceros del polinomio  $(x^2 - 1)P'_{n-1}(x)$ , donde  $P_{n-1}$  es el polinomio de Legendre de grado  $n - 1$  y  $P'_{n-1}$  su derivada.



FIGURA 1. Conjunto de Fekete de 11 puntos en el intervalo  $[-1, 1]$ .

Pero, ¿para qué sirven los puntos de Fekete?



Los puntos de Fekete son muy útiles en la interpolación de Lagrange. Sea  $f$  una función continua definida en un intervalo compacto  $E \subset \mathbb{R}$  y sean  $z_0, \dots, z_n$  un conjunto de  $n + 1$  puntos en  $E$ . El método de aproximación de Lagrange consiste en buscar un polinomio de grado  $n$  que coincida con  $f$  en los puntos elegidos. Siendo  $f$  continua, es de esperar que el polinomio obtenido se parezca a la función  $f$ .

Para construir el polinomio de interpolación se definen los polinomios fundamentales de Lagrange

$$L_k(x) = \frac{\prod_{i \neq k} (x - z_i)}{\prod_{i \neq k} (z_k - z_i)}.$$

Estos polinomios cumplen  $L_k(z_k) = 1$  y  $L_k(z_i) = 0$  si  $i \neq k$ . En otras palabras  $L_k(z_i) = \delta_{ik}$ .

Una vez construidos los polinomios fundamentales de Lagrange, el polinomio de interpolación se escribe fácilmente

$$P(x) = \sum_{k=0}^n f(z_k) L_k(x).$$

Claramente, en los puntos de interpolación tenemos  $P(z_k) = f(z_k)$ ,  $k = 1, \dots, n$ . Veamos cómo funciona este método en la práctica. Vamos a interpolar funciones continuas en el intervalo  $[-1, 1]$  usando puntos equiespaciados (este método se usa mucho por ser más cómodo de cálculo) y usando puntos de Fekete. En ambos casos usaremos 11 puntos.

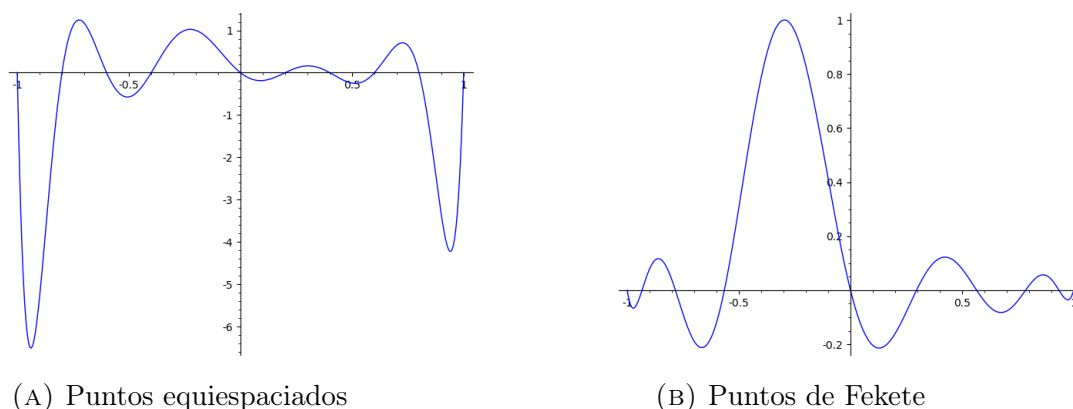


FIGURA 2. Polinomios de Lagrange

En la Figura 2 podemos ver un polinomio fundamental de Lagrange para el caso de puntos equiespaciados y para el caso de puntos de Fekete. Obsérvese la diferencia de escala en ambos gráficos. En ambos casos hay un punto donde el polinomio toma el valor 1 y otros puntos donde el polinomio toma el valor 0. Sin embargo el polinomio de Lagrange obtenido con puntos equiespaciados oscila mucho al acercarnos al borde del intervalo, alcanzando un valor cercano a  $-6$ . Por el contrario, en el polinomio obtenido usando los puntos de Fekete, las oscilaciones están mucho más controladas y en ningún momento el valor absoluto del polinomio es mayor a 1. Parece claro que la mayor oscilación en el caso de puntos equiespaciados puede ser un problema. Vamos a verlo en acción. En primer lugar aproximaremos una función suave:  $\exp(x)$ . Esta función en el intervalo  $[-1, 1]$  se aproxima muy bien, así que representamos en la Figura 3 el error cometido aproximando la función exponencial por un polinomio.

Atención, la escala es diferente en ambos gráficos. Si bien el método de puntos equiespaciados proporciona mejores resultados en la zona central, el error máximo es casi 10 veces mayor en el caso de puntos equiespaciados respecto al caso de puntos de Fekete.

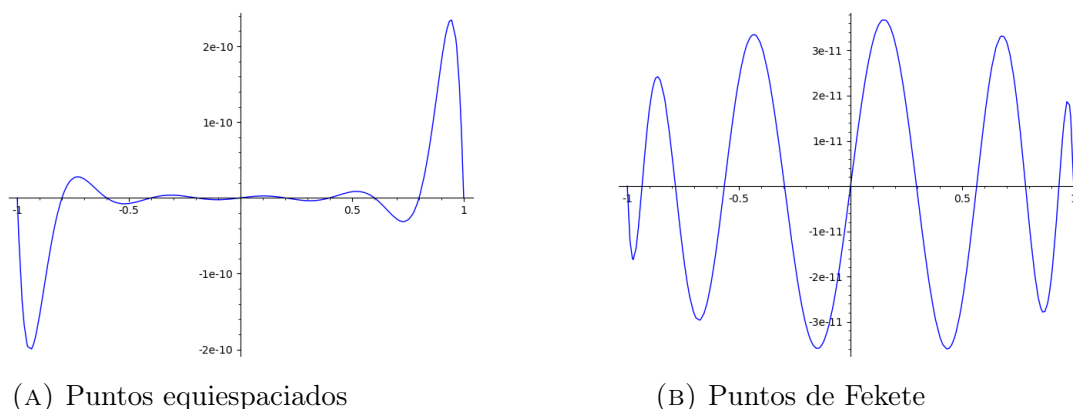
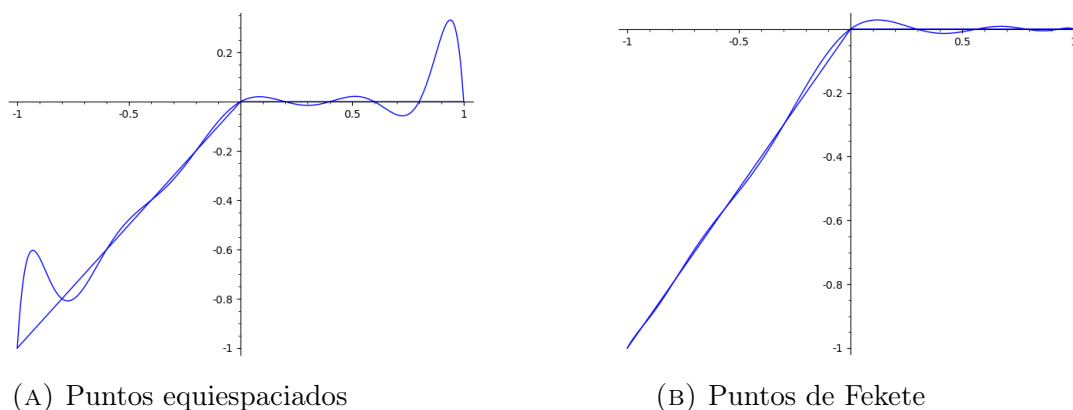


FIGURA 3. Error en la aproximación de la función exponencial.

Podemos ponerle las cosas más difíciles al método de aproximación e intentar aproximar una función continua  $f$  que no es diferenciable en el punto 0. Por ejemplo:

$$f(x) = \min(0, x).$$

En este caso el error se observa a simple vista y los resultados están en la Figura 4. De

FIGURA 4. Aproximación de la función  $f$ .

nuevo vemos que la presencia de oscilaciones incontroladas es un problema al usar puntos equiespaciados en el método de interpolación.

El Ejercicio 3.7 (3) explica por qué los puntos de Fekete son útiles en el método de aproximación. Para una función continua concreta puede que no dé el resultado óptimo. Pero da un resultado suficientemente bueno para todas las funciones continuas.

En muchos casos, calcular los puntos de Fekete de forma exacta es muy difícil y nos tenemos que conformar con unos puntos de Fekete *aproximados*, que hagan un trabajo razonable. Para saber si un conjunto de puntos se parece a un conjunto de Fekete es importante responder a las siguientes preguntas:

**Pregunta 3.3.** ¿Cuál es el comportamiento asintótico de  $\delta_n(E)$  cuando  $n$  tiende a infinito?

**Pregunta 3.4.** ¿Cuál es la distribución de los puntos de Fekete cuando  $n$  tiende a infinito?

**Lema 3.5.** La sucesión  $\delta_n(E)$ ,  $n \geq 2$ , es decreciente.

*Demostración.* Veamos que la sucesión  $\log \delta_n(E)$ ,  $n \geq 2$  es decreciente. Sea  $\mathcal{F}_n = \{z_1, \dots, z_n\} \subset E$  un conjunto de Fekete. Para cada  $k$  entre 1 y  $n$ ,

$$\begin{aligned} \frac{n(n-1)}{2} \log \delta_n(E) &= \sum_{1 \leq i < j \leq n} \log |z_i - z_j| \\ &= \sum_{i \neq k} \log |z_i - z_k| + \sum_{\substack{1 \leq i < j \leq n \\ i \neq k, j \neq k}} \log |z_i - z_j| \\ &\leq \sum_{i \neq k} \log |z_i - z_k| + \frac{(n-1)(n-2)}{2} \log \delta_{n-1}(E). \end{aligned}$$

Sumando las  $n$  desigualdades obtenidas variando  $k$  deducimos

$$\frac{n^2(n-1)}{2} \log \delta_n(E) \leq n(n-1) \log \delta_n(E) + \frac{n(n-1)(n-2)}{2} \log \delta_{n-1}(E).$$

Por tanto  $\log \delta_n(E) \leq \log \delta_{n-1}(E)$ . □

Como consecuencia del Lema 3.5 la sucesión  $\delta_n(E)$ ,  $n \geq 2$  converge a un número real  $\geq 0$ .

**Definición 3.6.** El *diámetro transfinito* del conjunto  $E$  es

$$\tau(E) = \lim_{n \rightarrow \infty} \delta_n(E).$$

Una primera respuesta a la Pregunta 3.3 es el cálculo del diámetro transfinito. Para responder a la Pregunta 3.4 usaremos el lenguaje de medidas e investigaremos el análogo continuo del problema de buscar puntos de Fekete.

*Ejercicios 3.7.* 1. La matriz de Vandermonde de tamaño  $n \times n$  está dada por  $(z_i^{j-1})$ , para  $1 \leq i \leq n$  y  $1 \leq j \leq n$ . Demostrar que el determinante de la matriz de Vandermonde es  $\prod_{1 \leq i < j \leq n} (z_j - z_i)$ . Por tanto, un conjunto de puntos de Fekete maximiza el valor absoluto del determinante de la correspondiente matriz de Vandermonde.

2. Utilizando el ejercicio anterior y la desigualdad de Hadamard para determinantes, demostrar que las raíces de la unidad forman un conjunto de Fekete en el círculo unidad.

3. Sea  $E$  un subconjunto compacto de  $\mathbb{C}$  y  $\mathcal{F}_{n+1} = \{z_1, \dots, z_{n+1}\}$  un conjunto de Fekete de  $n+1$  puntos para  $E$ .

a) Demostrar que, si  $L_k$  es el polinomio fundamental de Lagrange  $k$ -ésimo asociado a  $\mathcal{F}_{n+1}$ , entonces

$$|L_k(z)| \leq 1, \text{ para todo } z \in E.$$

b) Si, para un subconjunto  $S \subset \mathbb{C}$  y una función  $f$  denotamos

$$\|f\|_S = \sup_{z \in S} \{|f(z)|\},$$

demostrar que todo polinomio  $P$  de grado menor o igual que  $n$  satisface

$$\|P\|_E \leq (n+1) \|P\|_{n+1}.$$

c) Sea  $f: E \rightarrow \mathbb{C}$  una función continua, sea  $P_{n,f}$  el polinomio de grado menor o igual a  $n$  que aproxima mejor a  $f$  en la norma  $\|\cdot\|_E$ . Sea  $P_{\mathcal{F}_{n+1}}$  el polinomio obtenido mediante interpolación de Lagrange en los puntos  $\mathcal{F}_{n+1}$ . Demostrar que

$$\|f - P_{\mathcal{F}_{n+1}}\|_E \leq (n+2) \|f - P_{n,f}\|_E.$$

**3.2. Medidas y convergencia débil.** Para describir de forma cuantitativa la forma a la que tienden los conjuntos de Fekete o las órbitas de Galois de enteros algebraicos, es necesario introducir el lenguaje de medidas. En estas notas no podemos dar un curso completo de teoría de la medida y usaremos muchos resultados como una caja negra. El lector interesado puede consultar, por ejemplo [18] o [4].

Sea  $D \subset \mathbb{R}^m$  un subconjunto con la topología inducida y sea  $C_c^0(D, \mathbb{R})$  el espacio de las funciones continuas con soporte compacto en  $D$ . El espacio  $C_c^0(D, \mathbb{R})$  tiene una norma, la norma del supremo, definida, para  $f \in C_c^0(D, \mathbb{R})$ , por

$$\|f\|_D = \sup_{z \in D} |f(z)|.$$

Una *medida de Radon* en  $D$  es un funcional lineal continuo en  $C_c^0(D, \mathbb{R})$ . Las medidas de Radon son compatibles con la topología de  $D$  y la mayor parte de las medidas que aparecen en análisis son de este tipo. Si  $\mu$  es una medida en  $D$  y  $f \in C_c^0(D, \mathbb{R})$  es una función continua con soporte compacto, usamos tanto la notación funcional  $\mu(f)$  como la notación integral

$$\mu(f) = \int_D f d\mu = \int_D f(x) d\mu(x).$$

Una medida se denomina *positiva* si, para toda  $f \in C_c^0(D, \mathbb{R})$  con  $f(z) \geq 0, \forall z \in D$ , se tiene  $\mu(f) \geq 0$ .

Si  $D$  es compacto y  $\mu$  es una medida, se denomina la masa de  $\mu$  a la cantidad

$$\mu(D) := \int_D 1 d\mu(z).$$

Si  $D$  no es compacto, escribimos  $D = \bigcup E_n$  con  $E_1 \subset E_2 \subset \dots$  compactos, y la medida de  $D$  se define como el límite

$$\mu(D) = \lim \mu(E_n)$$

en caso de que este exista. Si la medida es positiva, el límite siempre existe aunque puede ser infinito. Una medida positiva se llama *finita* si la masa total es finita.

Una *medida de probabilidad* es una medida de Radon positiva de masa total 1. El espacio de medidas de probabilidad de  $D$  se denota  $\mathcal{M}(D)$ .

**Ejemplo 3.8.** Si  $z \in D$  la asignación  $f \mapsto f(z)$  es una medida de probabilidad en  $D$  que se denomina delta de Dirac en  $z$  y se denota  $\delta_z$ :

$$f(z) = \int_X f(x) d\delta_z(x).$$

Más generalmente, si  $F = \{z_1, \dots, z_n\}$  es un conjunto finito, la *medida de contaje* de  $F$  es la medida de probabilidad

$$(3.1) \quad \nu(F) := \frac{1}{n} \sum_{i=1}^n \delta_{z_i}.$$

En otras palabras

$$\nu(F)(f) = \int_X f d\nu(F) = \frac{1}{n} \sum_{i=1}^n f(z_i),$$

es la media de los valores de  $f$  en el conjunto  $F$ .

La teoría de medidas proporciona un lenguaje conveniente para estudiar la distribución asintótica de conjuntos de puntos mediante el concepto de convergencia débil-\*

Decimos que una sucesión de medidas  $(\mu_n)_{n \geq 1}$  converge en la topología débil-\* a una medida  $\mu$  si para toda función  $f \in C_c^0(D, \mathbb{R})$  se cumple

$$\int_D f d\mu = \lim_{n \rightarrow \infty} \int_D f d\mu_n.$$

El hecho de que la sucesión  $(\mu_n)_{n \geq 1}$  converja en la topología débil-\* a  $\mu$  se denota  $\mu_n \xrightarrow{*} \mu$ .

El siguiente resultado es consecuencia del Teorema de Banach-Alaoglu (ver [14] 3.15 y 3.16)

**Teorema 3.9.** *Sea  $E \subset \mathbb{C}$  un subconjunto compacto. Entonces el espacio  $\mathcal{M}(E)$  con la topología de la convergencia débil-\* es un espacio metrizable compacto. En particular es secuencialmente compacto.*

**Ejemplo 3.10.** Sea  $F_n = \{e^{\frac{2\pi ik}{n}} \mid 0 \leq k \leq n-1\}$  el conjunto de raíces  $n$ -ésimas de 1. Para toda función  $f \in C_c^0(\mathbb{C}, \mathbb{R})$  se tiene

$$\lim_{n \rightarrow \infty} \int_{\mathbb{C}} f d\nu(F_n) = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta.$$

Por tanto la sucesión  $\nu(F_n)$ ,  $n \geq 1$  converge en la topología débil-\* a la medida de Haar normalizada en el círculo unidad  $\frac{d\theta}{2\pi}$ .

Dada una medida  $\mu$  en  $D$  y  $U \subset D$  un subconjunto, decimos que el soporte de  $\mu$  está contenido en  $U$  si para toda función  $f \in C_c^0(D, \mathbb{R})$ , la condición  $f|_U = 0$  implica  $\mu(f) = 0$ .

**Lema 3.11.** *Sea  $E \subset \mathbb{C}$  un subconjunto compacto y  $B_n$ ,  $n \geq 0$  subconjuntos compactos con  $B_n \supset B_{n+1}$  y  $E = \bigcap B_n$ . Si  $(\mu_n)_{n \geq 0}$  es una sucesión de medidas de probabilidad con  $\mu_n \xrightarrow{*} \mu$  y soporte( $\mu_n$ )  $\subset B_n$ , entonces soporte( $\mu$ )  $\subset E$ .*

Necesitaremos un resultado técnico para extender determinadas medidas a funciones no necesariamente continuas.

**Definición 3.12.** Sea  $D \subset \mathbb{R}^m$  un subconjunto con la topología inducida. Una función  $f: D \rightarrow \mathbb{R} \cup \{\infty\}$  se denomina semi-continua inferior si para todo  $z_0 \in D$  se cumple

$$f(z_0) \leq \liminf_{z \rightarrow z_0} f(z).$$

**Lema 3.13.** *Una función es semi-continua inferior si y solo si, para todo compacto  $K \subset D$  existe una sucesión creciente de funciones continuas que converge puntualmente a  $f$ .*

Si  $f$  es una función semi-continua inferior y  $\mu$  es una medida positiva con soporte compacto  $K$ , se define

$$\int_D f(x) d\mu(x) = \lim_{n \rightarrow \infty} \int_D f_n(x) d\mu(x),$$

para cualquier sucesión creciente de funciones continuas que converge puntualmente a  $f$  en  $K$ .

**Lema 3.14.** *Sea  $f$  una función semi-continua inferior y  $\mu_n \xrightarrow{*} \mu$  una sucesión de medidas positivas, con soporte contenido en un compacto  $K$ , que converge, en la topología débil-\* a una medida  $\mu$ . Entonces*

$$\int_K f d\mu \leq \liminf_{n \rightarrow \infty} \int_K f d\mu_n.$$

- Ejercicios 3.15.*
1. Demostrar la afirmación del Ejemplo 3.10.
  2. Demostrar el Lema 3.11.
  3. Buscar una demostración del Lema 3.13.

**3.3. La capacidad logarítmica.** Discutimos ahora el análogo continuo del problema de encontrar los puntos de Fekete. Para ello imaginamos que los  $n$ -puntos representan cargas eléctricas del mismo signo que se repelen entre sí. De esta forma la configuración de puntos de Fekete es una posición de equilibrio para el problema electrostático.

Sea  $E \subset \mathbb{C}$  de nuevo un subconjunto compacto. Podemos imaginar que  $E$  es una lámina metálica a la que añadimos una carga eléctrica. Al ser una lámina metálica la carga se puede mover libremente y, dado que cargas de igual signo se repelen, tenderá a extenderse lo más posible.

Hay que tener cuidado con el símil electromagnético pues estamos acostumbrados al caso tridimensional, donde la fuerza de atracción/repulsión entre dos cargas eléctricas es proporcional al inverso de la distancia al cuadrado, mientras que la energía de dichas cargas es proporcional al inverso de la distancia. Si estamos confinados en un espacio bidimensional (como es el caso que nos ocupa) la fuerza eléctrica debe ser proporcional al inverso de la distancia, mientras que la energía debe ser proporcional al logaritmo de la distancia.

La densidad de carga se puede representar mediante una medida de probabilidad  $\mu$  en  $\mathbb{C}$  cuyo soporte está contenido en  $E$ . Por ejemplo, si toda la carga está concentrada en un punto  $z$ , la representamos mediante la medida delta de Dirac  $\delta_z$ .

**Definición 3.16.** Sea  $\mu$  una densidad de carga en  $E$ , el *potencial electrostático* asociado a  $\mu$  es

$$U^\mu(z) = \int_E \log \frac{1}{|z-t|} d\mu(t),$$

mientras que la *energía electrostática* de esta carga en  $E$  es

$$(3.2) \quad I(\mu) = \int U^\mu(z) d\mu(z) = \int \int \log \frac{1}{|z-t|} d\mu(z) d\mu(t).$$

Hay que tener cuidado con esta definición pues, en caso de haber cargas puntuales, la energía es infinita. Para tener una cantidad finita con la que trabajar, introducimos la siguiente variante de la energía. Si  $\mu = \nu(F)$  es la medida de contaje de un conjunto finito  $F = \{z_1, \dots, z_n\}$ , ponemos

$$(3.3) \quad I'(F) = I'(\mu) = \frac{1}{n(n-1)} \sum_{1 \leq i \neq j \leq n} \log \frac{1}{|z_i - z_j|} = -\log \left( \prod_{i < j} |z_i - z_j| \right)^{2/n(n-1)}.$$

El problema de encontrar un conjunto de Fekete de  $n$  puntos consiste en hallar

$$\inf_{\#F=n} I'(F).$$

**Definición 3.17.** La *constante de Robin* de un conjunto compacto  $E \subset \mathbb{C}$  es

$$V_E = \inf_{\mu \in \mathcal{M}(E)} \{I(\mu)\}.$$

Por tanto, el análogo continuo de buscar las cantidades  $\delta_n(E)$  y los puntos de Fekete es determinar el valor de la constante de Robin y encontrar una medida cuya energía coincida con este mínimo.

**Teorema 3.18.** *El valor  $V_E$  se alcanza en una medida  $\mu_E$ . Es más, si  $V_E < \infty$  entonces esta medida es única.*

La demostración de este resultado se basa en el análogo continuo del Lema 3.5.

**Lema 3.19.** *Sea  $\mu_n$  una sucesión de medidas en  $\mathcal{M}(E)$  que converge en la topología débil-\* a una medida  $\mu$ . Entonces, para todo  $z \in \mathbb{C}$*

$$(3.4) \quad U^\mu(z) \leq \liminf_{n \rightarrow \infty} U^{\mu_n}(z).$$

Además

$$(3.5) \quad I(\mu) \leq \liminf_{n \rightarrow \infty} I(\mu_n).$$

*Demostración.* Este resultado es consecuencia de que  $\log(1/|z - t|)$  es semi-continua inferior respecto de  $t$ .  $\square$

*Argumento de la demostración del Teorema 3.18.* Sean  $\mu_n$  una sucesión de medidas en  $\mathcal{M}(E)$  tales que  $\lim_{n \rightarrow \infty} I(\mu_n) = V_E$ . Por el Teorema 3.9 el espacio  $\mathcal{M}(E)$  con la topología débil-\* es secuencialmente compacto. Así existe una subsucesión de  $\mu_n$  que converge en la topología débil-\* a una medida  $\mu$ . Por el Lema 3.19 esta medida cumple  $V_E = I(\mu)$ .

Si  $V_E = \infty$ , cualquier medida  $\mu$  con soporte en  $E$  cumple  $I(\mu) = V_E$  y minimiza la energía, por lo que no hay unicidad. Por el contrario si  $V_E < \infty$ , usando que la función  $I$  en  $\mathcal{M}(E)$  es estrictamente convexa (un punto técnico que hay que precisar pues estamos en un espacio de dimensión infinita), se deduce la unicidad.  $\square$

**Definición 3.20.** La cantidad

$$\text{Cap}(E) = e^{-V_E}$$

se denomina la *capacidad logarítmica* de  $E$ . Una medida  $\mu_E$  que cumpla  $V(E) = I(\mu_E)$  se denomina una *medida de equilibrio* para  $E$  y el potencial  $U^{\mu_E}$  asociado a la medida de equilibrio se denomina el *potencial de equilibrio* de  $E$ .

Enunciamos en el siguiente resultado unas propiedades básicas de la capacidad logarítmica.

**Teorema 3.21.** 1. Si  $E_1 \subset E_2$  entonces  $\text{Cap}(E_1) \leq \text{Cap}(E_2)$ .

2. Si  $E \subset \mathbb{C}$  y  $\alpha, \beta \in \mathbb{C}$ , entonces  $\text{Cap}(\alpha E + \beta) = |\alpha| \text{Cap}(E)$ .

3. Si  $K \subset \mathbb{C}$  es compacto, entonces  $\text{Cap}(K) = \text{Cap}(\partial K)$ .

4. Si  $K_1 \supset K_2 \supset \dots$  son compactos y  $K = \bigcap K_i$ , entonces

$$\text{Cap}(K) = \lim_{i \rightarrow \infty} \text{Cap}(K_i).$$

5. Si  $\text{Cap}(K) = 0$  entonces  $K$  tiene medida de Lebesgue cero. Más aún, si  $\nu$  es una medida que satisface  $I(\nu) < \infty$ , entonces  $\nu(K) = 0$ .

El problema discreto de encontrar los puntos de Fekete y el problema continuo de encontrar la medida de equilibrio están muy relacionados y la teoría electrostática del plano complejo nos permite dar respuesta a las preguntas 3.3 y 3.4.

**Teorema 3.22.** Sea  $E \subset \mathbb{C}$  un conjunto compacto. Entonces

$$(3.6) \quad \text{Cap}(E) = \tau(E).$$

Además, si  $\text{Cap}(E) > 0$  y  $\mathcal{F}_n$ ,  $n \geq 2$  son colecciones de puntos de Fekete para  $E$  entonces

$$(3.7) \quad \nu(\mathcal{F}_n) \xrightarrow{*} \mu_E.$$

Esta última propiedad se expresa diciendo que los puntos de Fekete se equidistribuyen según la medida de equilibrio de  $E$ .

*Demostración.* En el argumento de esta demostración vamos a necesitar la medida producto de dos medidas. Más concretamente, si  $\mu$  y  $\nu$  son medidas en  $E$  entonces, la medida producto es una medida  $\mu \times \nu$  en  $E \times E$ . Para la definición y las propiedades básicas de la medida producto el lector puede consultar la Sección 1.7 de [18]. La propiedad fundamental de la medida producto es el Teorema de Fubini-Tonelli [18, Corollary 1.7.23].

Empezamos demostrando la desigualdad  $V_E \geq \log(1/\tau(E))$ . Escribimos

$$F(z_1, \dots, z_n) := I'(\{z_1, \dots, z_n\}) = \frac{2}{n(n-1)} \sum_{1 \leq i < j \leq n} \log \frac{1}{|z_i - z_j|}$$

El mínimo de la función  $F$  es  $\log(1/\delta_n(E))$ . El valor esperado de  $F$  respecto a cualquier medida de probabilidad en el producto  $\mathbb{C}^n$  debe ser mayor o igual a este mínimo. En particular, si consideramos la medida producto  $d\mu_E(z_1) \dots d\mu_E(z_n)$ , donde  $\mu_E$  es la medida de equilibrio de  $E$ , deducimos

$$V_E = \int_{E \times \dots \times E} F(z_1, \dots, z_n) d\mu_E(z_1) \dots d\mu_E(z_n) \geq \log \frac{1}{\delta_n(E)}.$$

Consideramos la sucesión de medidas  $\nu_n := \nu(\mathcal{F}_n)$ ,  $n \geq 2$ . Por el Teorema 3.9 existe una medida  $\hat{\mu}$  que es el límite en la topología débil-\* de una subsucesión  $(\nu_{n_k})_{k \in \mathbb{N}}$ . Una consecuencia del Teorema de Fubini-Tonelli para medidas es que  $(\nu_{n_k} \times \nu_{n_k})_{k \in \mathbb{N}} \xrightarrow{*} \hat{\mu} \times \hat{\mu}$ .

Para poder aplicar la convergencia débil de medidas necesitamos aplicarlas a funciones continuas. La función  $\log|x|$  no es continua cuando  $x$  tiende a cero.

Para cada  $M \in \mathbb{R}$ ,  $M > 0$ , escribimos  $\log_M(|x|) = \min(\log(|x|), M)$ . Las funciones  $\log_M(1/|x|)$  son continuas para todo  $x \in \mathbb{R}$ . Y cuando  $M$  tiende a infinito, la colección de funciones  $(\log_M(1/|x|))_M$  converge monotonamente a la función  $\log(1/|x|)$ . Calculamos

$$\begin{aligned} I(\hat{\mu}) &= \int \int \log \frac{1}{|z-t|} d\hat{\mu}(z) d\hat{\mu}(t) \\ &= \lim_{M \rightarrow \infty} \int \int \log_M \frac{1}{|z-t|} d\hat{\mu}(z) d\hat{\mu}(t) \\ &= \lim_{M \rightarrow \infty} \lim_{k \in \mathbb{N}} \int \int \log_M \frac{1}{|z-t|} d\nu_{n_k}(z) d\nu_{n_k}(t) \\ &\leq \lim_{M \rightarrow \infty} \lim_{k \in \mathbb{N}} \left( \frac{n_k - 1}{n_k} \log \frac{1}{\delta_{n_k}(E)} + \frac{M}{n_k} \right) \\ &= \lim_{M \rightarrow \infty} \lim_{k \in \mathbb{N}} \log \frac{1}{\delta_{n_k}(E)} = \log \frac{1}{\tau(E)}. \end{aligned}$$

La igualdad en la segunda línea es consecuencia del teorema de convergencia dominada, mientras que la igualdad en la tercera línea se sigue de la convergencia débil de medidas junto con el hecho de que  $\log_M(1/|x|)$  es continua en cualquier compacto de  $\mathbb{C}$ . Por la minimalidad de  $V_E$  deducimos

$$V_E \leq I(\hat{\mu}) \leq \log \frac{1}{\tau(E)} \leq V_E$$

lo que demuestra (3.6). Si  $\text{Cap}(E) > 0$ , la unicidad de la medida de equilibrio implica  $\hat{\mu} = \mu_E$  de donde se deduce (3.7).  $\square$

**Ejemplo 3.23.** En el Ejercicio 3.26 1 se busca la capacidad y la medida de equilibrio en el caso del disco unidad.

**Ejemplo 3.24.** Si  $E \subset \mathbb{R} \subset \mathbb{C}$  es el segmento  $E = [a, b]$ , entonces  $\text{Cap}(E) = \frac{b-a}{4}$  y la medida de equilibrio es

$$(3.8) \quad \mu_E = \frac{1}{\pi} \frac{dx}{\sqrt{(x-a)(b-x)}}.$$

En el Ejercicio 3.26 (2) vemos que el potencial de equilibrio es constante en el disco unidad. Esto es consistente con la intuición física, pues si hubiera diferencia de potencial, las cargas se desplazarían para disminuir la energía total. En general el resultado matemático preciso es

**Teorema 3.25** (Teorema de Frostman). *Sea  $E \subset \mathbb{C}$  un subconjunto compacto con  $\text{Cap}(E) > 0$ . Entonces*

1.  $U^{\mu_E}(z) \leq V_E$  para todo  $z \in \mathbb{C}$ ,



2.  $U^{\mu_E}(z) = V_E$  para todo  $z \in E \setminus S$ , donde  $S$  es un subconjunto con  $\text{Cap}(S) = 0$ .
3. Si  $\Omega$  es la componente conexa no acotada de  $\mathbb{C} \setminus E$ , entonces para todo  $z \in \Omega$  se tiene  $U^{\mu_E}(z) < V_E$ .

La demostración de este resultado usa el principio del máximo para potenciales 3.35. Esta demostración la daremos en la Sección 3.6.

- Ejercicios 3.26.*
1. Usando que las raíces de la unidad de orden  $n$  forman un conjunto de Fekete de  $n$  puntos en el disco unidad, demostrar que la capacidad del disco unidad es 1 y que la medida de equilibrio del disco unidad es la medida de Haar  $\frac{d\theta}{2\pi}$  en el círculo unidad.
  2. Demostrar que el potencial de equilibrio del disco unidad es

$$U^{\mu_E}(z) = \begin{cases} 0, & \text{if } |z| \leq 1 \\ \log(1/|z|), & \text{if } |z| > 1. \end{cases}$$

**3.4. La constante de Chebyshev.** En esta sección,  $E \subset \mathbb{C}$  continúa designando un subconjunto compacto. El siguiente problema es determinar el mínimo valor de la norma  $\|p\|_E$  donde  $p$  es un polinomio mónico de grado  $n$  y encontrar un polinomio que alcance este mínimo. Es decir, buscamos el valor de

$$(3.9) \quad t_n(E) := \inf_{p \in \mathcal{P}_n} \|p\|_E,$$

donde  $\mathcal{P}_n$  es el conjunto de los polinomios mónicos de grado  $n$ . Si  $E$  contiene infinitos puntos existe un único polinomio mónico  $T_n \in \mathcal{P}_n$  con  $t_n(E) = \|T_n\|_E$ , que se llama el polinomio de Chebyshev  $n$ -ésimo para  $E$ . Ver el ejercicio 1.

Debido a que

$$t_{m+n}(E) = \|T_{m+n}\|_E \leq \|T_m\|_E \|T_n\|_E = t_m(E)t_n(E),$$

la sucesión  $\log(t_n(E))$  es subaditiva y por tanto, el límite

$$\text{Cheb}(E) = \lim_{n \rightarrow \infty} t_n(E)^{1/n} = \inf_{n \geq 1} t_n(E)^{1/n}$$

existe y se denomina la constante de Chebyshev de  $E$ .

Muy relacionado con el polinomio de Chebyshev, el polinomio de Fekete  $F_n$  es un polinomio mónico de grado  $n$  cuyas raíces forman un conjunto de Fekete de  $n$  puntos.

En la Figura 5 se compara el polinomio de Chebyshev de grado 11 con el polinomio de Fekete de grado 11 en el intervalo  $[-1, 1]$ . Ambos son razonablemente similares. Se incluye también el polinomio mónico de grado 11 con las raíces equiespaciadas. Observad la diferencia de escala. La norma del supremo de este último polinomio es 8 veces mayor que la del correspondiente polinomio de Chebyshev.

El resultado fundamental de la teoría del potencial es el siguiente.

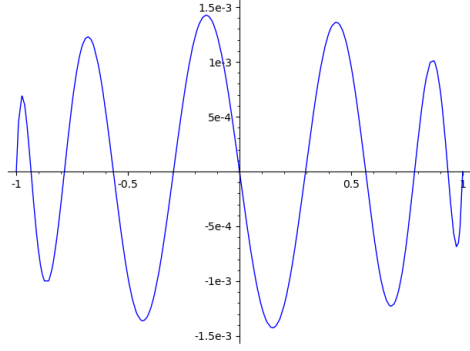
**Teorema 3.27.** *Sea  $E \subset \mathbb{C}$  un subconjunto compacto.*

1.  $\tau(E) = \text{Cap}(E) = \text{Cheb}(E)$ .
2. Los polinomios de Fekete son asintóticamente óptimos para el problema de Chebyshev:

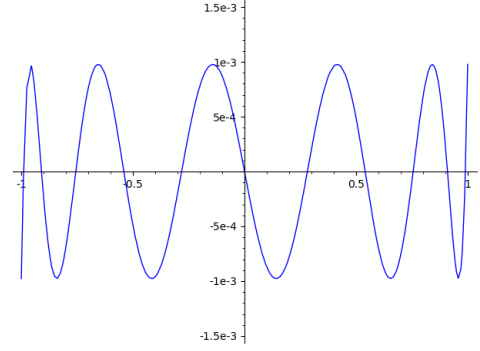
$$\lim_{n \rightarrow \infty} \|F_n\|_E^{1/n} = \text{Cheb}(E).$$

Si además,  $\text{Cap}(E) > 0$  y por tanto  $\mu_E$  es única, entonces

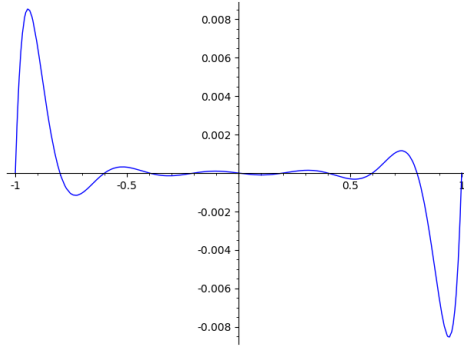
3. Los puntos de Fekete tienen distribución asintótica  $\mu_E$ . Es decir  $\nu(\mathcal{F}_n) \xrightarrow{*} \mu_E$  cuando  $n \rightarrow \infty$ .



(A) Polinomio de Fekete de grado 11.



(B) Polinomio de Chebyshev de grado 11.



(C) Polinomio de grado 11 con raíces equiespaciadas.

FIGURA 5. Polinomios de Fekete y Chebyshev.

#### 4. La convergencia

$$\lim_{n \rightarrow \infty} |F_n(z)|^{1/n} = \exp(-U^{\mu_E}(z))$$

es uniforme en cada subconjunto compacto de  $\Omega$ , la componente conexa no acotada de  $\mathbb{C} \setminus E$ .

*Demostración.* La afirmación (3) ya ha sido establecida en el Teorema 3.22. La afirmación (4) se deduce de ella. De hecho, de la definición de potencial se deduce que

$$U^{\nu(\mathcal{F}_n)}(z) = \frac{1}{n} \log \frac{1}{|F_n(z)|}$$

y todos los ceros de  $F_n$  están contenidos en  $E$ . Por tanto, si  $K \subset \Omega$  es un subconjunto compacto y  $z \in K$ , dado que  $\nu(\mathcal{F}_n) \xrightarrow{*} \mu_E$  tenemos que

$$\frac{1}{n} \log \frac{1}{|F_n(z)|} = \int \log \frac{1}{|t-z|} d\nu(\mathcal{F}_n)(t) \xrightarrow{n \rightarrow \infty} \int \log \frac{1}{|t-z|} d\mu_E(t) = U^{\mu_E}(z),$$

debido a que, para  $z \notin E$ , la función  $t \mapsto -\log|t-z|$  es continua en  $E$ . Como  $K$  es compacto y para  $t \in E$ , la función  $\frac{1}{|t-z|}$  es continua en  $K$ , esta está uniformemente acotada en  $K$ . Por tanto la convergencia es uniforme en  $K$ .

Nos queda por demostrar (1) y (2), de los que ya hemos demostrado  $\text{Cap}(E) = \tau(E)$ . Sea  $\mathcal{F}_n = \{z_1^{(n)}, \dots, z_n^{(n)}\}$  un conjunto de Fekete de  $n$  puntos. Entonces

$$\delta_{n+1}(E)^{n(n+1)/2} = \max_{\{z_i\} \subset E} \prod_{1 \leq i < j \leq n+1} |z_i - z_j| \geq \left( \prod_{1 \leq i \leq n} |z - z_i^{(n)}| \right) \delta_n(E)^{(n-1)n/2}$$

para todo  $z \in E$ . Por tanto, poniendo  $\delta_n = \delta_n(E)$ ,

$$\delta_{n+1}^{n(n+1)/2} / \delta_n^{(n-1)n/2} \geq |F_n(z)|, \quad \forall z \in E.$$

Tomando las raíces  $n$ -ésimas

$$\delta_{n+1}^{(n+1)/2} / \delta_n^{(n-1)/2} \geq \|F_n\|_E^{1/n}.$$

Como la sucesión  $\delta_n$  es decreciente,

$$\delta_{n+1}^{(n+1)/2} / \delta_n^{(n-1)/2} \leq (\delta_{n+1} \delta_n)^{1/2}.$$

Usando la definición de  $\text{Cheb}(E)$  deducimos

$$(\delta_{n+1} \delta_n)^{1/2} \geq \|F_n\|_E^{1/n} \geq \text{Cheb}(E).$$

Haciendo tender  $n$  a  $\infty$  obtenemos

$$\tau(E) \geq \limsup_{n \rightarrow \infty} \|F_n\|_E^{1/n} \geq \liminf_{n \rightarrow \infty} \|F_n\|_E^{1/n} \geq \text{Cheb}(E).$$

Por lo que para deducir (1) y (2), basta demostrar que  $\text{Cheb}(E) \geq \tau(E)$ . Si  $\tau(E) = 0$  esta desigualdad es obvia, por lo que podemos suponer  $\text{Cap}(E) > 0$ . Sea  $T_n(z)$  un polinomio de Chebyshev de grado  $n$  en  $E$  y denotamos mediante  $\nu(T_n)$  la medida de contaje en los ceros de  $T_n(z)$ . Entonces

$$\frac{1}{n} \log \frac{1}{t_n(E)} = \inf_{z \in E} \frac{1}{n} \log \frac{1}{|T_n(z)|} = \inf_{z \in E} U^{\nu(T_n)}(z).$$

Ahora bien,

$$\inf_{z \in E} U^{\nu(T_n)}(z) \leq \int U^{\nu(T_n)} d\mu_E = \int U^{\mu_E} d\nu(T_n),$$

donde la última igualdad es consecuencia del teorema de Fubini-Tonelli. Por el Teorema de Frostman 3.25 tenemos que

$$\int U^{\mu_E} d\nu(T_n) \leq V_E.$$

Juntando las desigualdades obtenidas, deducimos que

$$\frac{1}{n} \log \frac{1}{t_n(E)} \leq V_E,$$

y tomando el límite cuando  $n$  tiende a infinito,

$$\text{Cheb}(E) \geq \text{Cap}(E) = \tau(E).$$

□

*Ejercicios 3.28.* 1. Sea  $E \subset \mathbb{C}$  u subconjunto compacto que contiene al menos  $n + 1$  puntos.

- a) Demostrar que el ínfimo en la ecuación (3.9) se alcanza en algún polinomio  $T_n \in \mathcal{P}_n$ .
- b) Demostrar que hay al menos  $n + 1$  puntos de  $E$  donde se cumple la igualdad  $t_n(E) = |T_n(z)|$ . (Indicación: si no fuera cierto, podríamos encontrar un polinomio  $q$  de grado menor o igual a  $n - 1$  que coincide con  $T_n$  en todo punto  $z$  con  $|T_n(z)| = t_n(E)$ . Demostrar que, para  $\epsilon > 0$  suficientemente pequeño  $\|T_n - \epsilon q\| < t_n(E)$  contradiciendo la definición de  $t_n(E)$ .)
- c) Demostrar que  $T_n$  es único. (Indicación: si hubiera dos candidatos, aplicar 1b a la media aritmética de ambos).
- d) Demostrar que los zeros de  $T_n$  están en la envolvente convexa de  $E$ .
- e) Sea  $E = [-1, 1] \times \{-i, i\}$ . Demostrar que, para  $n$  impar,  $T_n$  tiene un zero en el eje real y por tanto fuera de  $E$ .

2. Demostrar que los polinomios de Chebyshev en el intervalo  $[-1, 1]$  son los polinomios

$$T_n(x) = 2^{1-n} \cos(n \arccos x).$$

Concluir que  $\text{Cap}([-1, 1]) = \text{Cheb}([-1, 1]) = 1/2$ .

3. Sean  $0 \leq b < a$  números reales y sea  $E = [-a, -b] \cup [b, a]$ .

a) Demostrar que, si  $p(x)$  es un polinomio de Chebyshev para  $E$  de grado par, entonces  $(p(x) + p(-x))/2$  también lo es. Por tanto podemos buscar polinomios de Chebyshev de grado  $2k$  de la forma  $q(x^2)$  con  $q$  polinomio mónico de grado  $k$ .

b) Demostrar que los polinomios

$$P_{2k}(x) = 2^{1-2k} (a^2 - b^2)^k \cos \left( n \arccos \left( 2 \frac{x^2 - b^2}{a^2 - b^2} - 1 \right) \right)$$

son polinomios de Chebyshev para  $E$ .

c) Demostrar que

$$\text{Cap}(E) = \frac{\sqrt{a^2 - b^2}}{2}.$$

4. Sea  $p(x)$  un polinomio mónico de grado  $n$ . Consideramos la *lemniscata*

$$L = \{z \in \mathbb{C} \mid |p(z)| \leq R^n\}.$$

Determinar los polinomios de Chebyshev de grado  $nk$  para  $E$  y mostrar que  $\text{Cap}(L) = R$ .

**3.5. Potenciales y funciones armónicas.** En esta sección definiremos funciones armónicas y superarmónicas, daremos algunas propiedades y las usaremos para estudiar los potenciales  $U^\mu$ . Una referencia para el material de este capítulo es el libro [13],

**Definición 3.29.** Una función  $f: D \rightarrow \mathbb{R}$  definida en un abierto  $D \subset \mathbb{C}$  es armónica si cumple la *propiedad del valor medio*: Para todo  $z \in D$ , si el disco  $|\zeta - z| \leq r$  está contenido en  $D$ , entonces

$$(3.10) \quad f(z) = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta}) d\theta.$$

Una función  $f$  es armónica si y solo si  $f$  es continua, sus primeras y segundas derivadas parciales existen y son continuas y para todo  $z \in D$ ,

$$\Delta f(z) := f_{xx}(z) + f_{yy}(z) = 0,$$

donde  $z = x + iy$  y  $f_{xx}, f_{yy}$  denotan las segundas derivadas parciales de  $f$  respecto de  $x$  e  $y$ . De hecho, esta propiedad se puede usar como definición equivalente de función armónica, por ejemplo en [13] Definición 1.1.1 y Teorema 1.2.7.

Una consecuencia directa de (3.10) es el *principio max-min* para funciones armónicas.

**Teorema 3.30.** Sea  $D \subset \mathbb{C}$  un abierto conexo y  $f: D \rightarrow \mathbb{R}$  una función armónica. Si  $f$  alcanza su mínimo o su máximo en  $D$  entonces es constante. En consecuencia, si  $f$  es una función continua en un compacto y es armónica en el interior del compacto entonces alcanza el mínimo y el máximo en la frontera del compacto.

Las funciones superarmónicas son el análogo complejo de las funciones concavas.

**Definición 3.31.** Sea  $D \subset \mathbb{C}$  un abierto. Una función  $f: D \rightarrow \mathbb{R} \cup \{\infty\}$  es *superarmónica* si no es constante igual a  $\infty$  en ninguna componente conexa de  $D$  y

1. es semicontinua inferior en  $D$ ;

2. el valor en cada punto es mayor o igual al valor medio en un círculo centrado en el punto. Esto es, si  $z \in D$  y  $r > 0$  cumplen que el disco  $|\zeta - z| \leq r$  está contenido en  $D$ , entonces

$$(3.11) \quad f(z) \geq \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta}) d\theta.$$

Una función  $f$  se llama subarmónica si  $-f$  es superarmónica.

Las funciones superarmónicas verifican el *principio del mínimo*, y por tanto las subarmónicas verifican el principio del máximo [13, Theorem 2.3.1].

**Teorema 3.32.** *Sea  $D \subset \mathbb{C}$  un conjunto abierto, conexo y acotado y  $g$  una función superarmónica no constante en  $D$  tal que*

$$\liminf_{z \rightarrow \zeta} g(z) \geq m, \quad \forall \zeta \in \partial D.$$

*Entonces  $g(z) > m$  para todo  $z \in D$ .*

La conexión entre funciones superarmónicas y potenciales viene dado por el siguiente resultado.

**Proposición 3.33.** *Sea  $\mu$  una medida positiva cuyo soporte está contenido en un compacto  $E$  y sea  $\Omega$  la componente conexa no acotada de  $\mathbb{C} \setminus E$ , entonces el potencial*

$$U^\mu(z) = \int \log \frac{1}{|z - t|} d\mu(t)$$

*es una función superarmónica y su restricción a  $\Omega$  es armónica.*

*Demostración.* Dado que la función  $\log(1/|z - t|)$  es semicontinua inferior en  $z$  para todo  $t$  se sigue que  $U^\mu(z)$  es semicontinua inferior. Es fácil comprobar que, para  $t$  fija, la función  $f_t(z) = \log(1/|z - t|)$  es superarmónica. De hecho, para  $z \neq t$ ,  $f_t(z)$  es armónica, mientras que, para  $z = t$ ,  $f_t(t) = \infty$  que es mayor o igual que la media en el círculo  $|z - t| = r$  para  $r$  suficientemente pequeño.

Usando el teorema de Fubini-Tonelli obtenemos

$$\begin{aligned} \frac{1}{2\pi} \int_0^{2\pi} U^\mu(z + re^{i\theta}) d\theta &= \int \frac{1}{2\pi} \int_0^{2\pi} \log \frac{1}{|z + re^{i\theta} - t|} d\theta d\mu(t) \\ &\leq \int \log \frac{1}{|z - t|} d\mu(t) = U^\mu(z), \end{aligned}$$

probando que  $U^\mu$  es superarmónica. Que la restricción de  $U^\mu$  a  $\Omega$  es armónica se demuestra de la misma forma, usando que  $\log(1/|z - t|)$  con  $t$  fijo y  $z \neq t$  es una función armónica.  $\square$

De hecho, toda función superarmónica se parece a un potencial con respecto de una medida positiva. Este es el contenido del Teorema de Riesz [13, Theorem A.3.2].

**Teorema 3.34** (Teorema de Riesz). *Si  $f$  es superarmónica en un abierto conexo  $D \subset \mathbb{C}$ , entonces existe una medida positiva  $\lambda$  con soporte contenido en  $D$  y en cada subconjunto abierto conexo  $D^*$  con  $\overline{D^*} \subset D$  se tiene*

$$f(z) = h(z) + \int_D \log \frac{1}{|z - t|} d\lambda(t), \quad z \in D^*$$

*donde  $h$  es armónica en  $D^*$ .*

A partir del principio del máximo para funciones superarmónicas se obtiene un principio del máximo para potenciales.

**Teorema 3.35.** *Sea  $\mu$  una medida positiva finita con soporte compacto. Si  $U^\mu(z) \leq M$  para todo  $z$  en el soporte de  $\mu$ , entonces  $U^\mu(z) \leq M$  para todo  $z \in \mathbb{C}$ .*

El principio del máximo para potenciales es un caso particular del teorema de dominación (Ver [17] II Teorema 3.2.)

**Teorema 3.36.** Sean  $\mu$  y  $\nu$  dos medidas positivas finitas con soporte compacto, masa total cumpliendo  $\nu(\mathbb{C}) \leq \mu(\mathbb{C})$  y tal que  $\mu$  tiene energía logarítmica finita ( $I(\mu) < \infty$ ). Si para una constante  $c$ , la desigualdad

$$U^\mu(z) \leq U^\nu(z) + c$$

se cumple salvo en un conjunto de  $\mu$ -medida cero, entonces la desigualdad se cumple en todo punto complejo.

Muy relacionada con el potencial  $U^{\mu_E}$  tenemos la función de Green para  $E$  con polo en el infinito. Para las propiedades de la función de Green y más detalles sobre los próximos resultados se puede consultar la sección II.4 de [17]. La función de Green está caracterizada por el siguiente resultado.

**Teorema 3.37.** Sea  $E \subset \mathbb{C}$  un subconjunto compacto y  $\Omega$  la componente conexa no acotada de  $\mathbb{C} \setminus E$ . Entonces existe una única función  $g_E(\cdot, \infty): \Omega \rightarrow \mathbb{R}$  caracterizada por las propiedades

1.  $g_E(\cdot, \infty)$  es armónica en  $\Omega$  y está acotada superior e inferiormente fuera de todo entorno de  $\infty$ ;
2. la diferencia  $g_E(z, \infty) - \log |z|$  está acotada en un entorno de  $\infty$ ;
- 3.

$$\lim_{z \rightarrow \zeta} g(z, \infty) = 0$$

para todo  $\zeta \in \partial\Omega$  excepto en un conjunto de capacidad cero.

La relación precisa entre la función de Green, la constante de Robin y el potencial viene dada por el siguiente resultado.

**Teorema 3.38.** Sean  $E$  y  $\Omega$  como en el teorema anterior y  $g_E(\cdot, \infty)$  la función de Green para  $E$  con polo en el infinito. Entonces

1.  $\lim_{z \rightarrow \infty} g(z, \infty) - \log |z| = V_E$ ,
2. el potencial de equilibrio de  $E$  es

$$U^{\mu_E}(z) = V_E - g(z, \infty).$$

En los ejercicios 3.39 del 7 al 11 usamos las propiedades que caracterizan la función de Green para estudiar el efecto de las aplicaciones holomorfas en la capacidad.

*Ejercicios 3.39.* 1. Demostrar el Teorema 3.30.

2. Demostrar que si una función  $f$  es armónica en un conjunto abierto  $D \subset \mathbb{C}$  que contiene el disco  $|z - z_0| \leq r$  entonces

$$f(z_0) = \frac{1}{\pi r^2} \int \int f(x + iy) dx dy.$$

3. Demostrar que si  $(f_n)_{n \geq 1}$  es una sucesión de funciones armónicas que converge localmente uniformemente a una función  $f$ , entonces  $f$  es armónica.
4. Demostrar que una función  $f \in C^2(D)$  en un abierto conexo  $D$  es superarmónica si y solo si

$$\Delta f := f_{xx} + f_{yy} \leq 0$$

en todos los puntos de  $D$ .

5. Sea  $F: D \rightarrow \mathbb{C}$  una función analítica en un conjunto abierto conexo  $D$  que no se anula idénticamente. Demostrar que, para  $p > 0$ ,  $|F|^p$  es subarmónica y que  $\log(1/|F|)$  es superarmónica.
6. Buscar una demostración del Teorema 3.21.

7. Sea  $f: D \rightarrow \mathbb{C}$  una función analítica en un abierto conexo  $D$ . Sea  $D' = f(D)$  y  $u: D' \rightarrow \mathbb{R}$  una función armónica (resp. superarmónica), demostrar que  $u \circ f$  es armónica (resp superarmónica).
8. Sean  $E_1$  y  $E_2$  conjuntos compactos conexos tales que  $\Omega_1 = \mathbb{P}^1(\mathbb{C}) \setminus E_1$  y  $\Omega_2 = \mathbb{P}^1(\mathbb{C}) \setminus E_2$  sean conexos y simplemente conexos. Sea  $f: \Omega_1 \rightarrow \Omega_2$  una función analítica que envía  $\partial\Omega_1$  continuamente a  $\partial\Omega_2$  y que cumple  $f(\infty) = \infty$  y  $f'(\infty) > 0$ . Si  $g_{E_2}(\cdot, \infty)$  es la función de Green de  $E_2$  entonces  $g_{E_2}(f(z), \infty)$  es la función de Green para  $E_1$ . Utilizar este resultado para comparar la capacidad de  $E_1$  y  $E_2$  y sus potenciales de equilibrio.
9. Demostrar que el potencial de equilibrio del disco unidad  $\bar{B} = \{|z| \leq 1\}$  es la función

$$-\log^+ |z| = -\max(0, \log |z|).$$

10. Utilizar los problemas 9 y 8 y la transformación  $z \mapsto z + 1/z$  para calcular la capacidad logarítmica, la medida de equilibrio y el potencial de equilibrio del segmento  $[-2, 2]$ .
11. Mostrar que, si  $E$  es un conjunto compacto de capacidad positiva y  $p$  es un polinomio mónico de grado  $n$  entonces

$$\text{Cap}(p^{-1}(E)) = \text{Cap}(E)^{1/n}.$$

**3.6. Demostración del Teorema de Frostman.** En esta sección damos la demostración del teorema de Frostman. Recordemos el resultado. Sea  $E$  un conjunto compacto con  $\text{Cap}(E) > 0$ ,  $\mu_E$  la medida de equilibrio de  $E$  y  $U^{\mu_E}$  el potencial de equilibrio asociado. Tenemos que ver

1.  $U^{\mu_E}(z) \leq V_E$  para todo  $z \in \mathbb{C}$ .
2.  $U^{\mu_E}(z) = V_E$  para todo  $z \in E \setminus S$ , donde  $S$  tiene capacidad 0.
3.  $U^{\mu_E}(z) < V_E$  para todo  $z \in \Omega$ , donde  $\Omega$  es la componente conexa no acotada de  $\mathbb{C} \setminus E$ .

La demostración se realiza en varios pasos. En primer lugar sea

$$E_n = \{z \in E \mid U^{\mu_E} \leq V_E - 1/n\}, \quad n > 0.$$

Demostraremos por contradicción que

$$(3.12) \quad \text{Cap}(E_n) = 0, \quad \forall n > 0.$$

Supongamos que  $\text{Cap}(E_n) > 0$  para algún  $n > 0$ . Como  $V_E = I(\mu_E) = \int U^{\mu_E} d\mu_E$ , existe un  $z_0$  en el soporte de  $\mu_E$  con  $U^{\mu_E}(z_0) \geq V_E$ . Por la semicontinuidad inferior de  $U^{\mu_E}$  existe un  $r > 0$  de tal forma que  $U^{\mu_E}(z) > V_E - 1/2n$  en el disco  $\bar{B}(z_0, r)$ . En particular  $\bar{B}(z_0, r) \cap E_n = \emptyset$ . Como  $z_0$  está en el soporte de  $\mu_E$ , el número

$$a := \mu_E(\bar{B}(z_0, r))$$

es estrictamente positivo.

Como suponemos que  $\text{Cap}(E_n) > 0$ , existe una medida  $\mu \in \mathcal{M}(E_n)$  con  $I(\mu) < \infty$ . Definimos una medida con signo

$$\sigma = \begin{cases} \mu, & \text{en } E_n, \\ -\mu_E/a, & \text{en } \bar{B}(z_0, r), \\ 0, & \text{en el resto.} \end{cases}$$

Para cada  $t \in (0, a)$  la medida  $\mu_t = \mu_E + t\sigma$  es positiva y de masa total 1. Por tanto  $\mu_t \in \mathcal{M}(E)$ . Un cálculo directo muestra que

$$I(\mu_E) - I(\mu_t) \geq 2t(V_E - 1/2n - V_E + 1/n) + O(t^2).$$

por tanto, para  $t$  suficientemente pequeño,  $I(\mu_E) \geq I(\mu_t)$  lo que contradice la minimalidad de  $I(\mu_E)$ .

En el segundo paso, sea

$$L_n = \{z \in \text{soporte}(\mu_E) \mid U^{\mu_E}(z) > V_E + 1/n\}, \quad n > 1.$$

Demostraremos por contradicción que

$$(3.13) \quad L_n = \emptyset.$$

Supongamos que algún  $L_n$  es no vacío y sea  $z_1 \in L_n$ , por la semicontinuidad inferior de  $U^{\mu_E}$  existe un  $s > 0$  tal que  $U^{\mu_E}(z) > V_E + 1/n$  en  $\overline{B}(z_1, s)$ . Como  $z_1$  está en el soporte de  $\mu_E$ , el número

$$b := \mu_E(\overline{B}(z_1, s))$$

es estrictamente positivo.

Por (3.12) y el Teorema 3.21 (5) sabemos que  $\mu_E(E_n) = 0$  y por tanto  $U^{\mu_E}(z) \geq V_E$  salvo en un conjunto de  $\mu_E$  medida cero. Así,

$$\begin{aligned} V_E = I(\mu_E) &= \int_E U^{\mu_E} d\mu_E \\ &= \int_{\overline{B}(z_1, s)} U^{\mu_E} d\mu_E + \int_{E \setminus \overline{B}(z_1, s)} U^{\mu_E} d\mu_E \\ &\geq \left(V_E + \frac{1}{n}\right) b + V_E(1 - b) \\ &> V_E, \end{aligned}$$

obteniendo una contradicción.

Para concluir la demostración del teorema, observamos que (3.13) implica que  $U^{\mu_E} \leq V_E$  en el soporte de  $\mu_E$ . Así, aplicando el principio del máximo para potenciales (Teorema 3.35) deducimos la afirmación (1). Usando la condición (3.12) se puede ver que el conjunto  $S = \bigcup_n E_n$  tiene capacidad cero, por lo que obtenemos la afirmación (2). La afirmación (3) se sigue del hecho que  $U^{\mu_E}$  es armónica en  $\Omega$  junto con el Teorema 3.30.

### 3.7. El teorema de la lemniscata de Hilbert.

**Definición 3.40.** Sea  $p \in \mathbb{C}[x]$  un polinomio mónico de grado  $d$  y  $0 < \rho \in \mathbb{R}$  una constante real. La *lemniscata de polinomio  $p$  y constante  $\rho$*  es el conjunto

$$L = L_{p, \rho} = \{z \in \mathbb{C} \mid |p(z)| \leq \rho^d\}.$$

En esta sección veremos que todo conjunto de capacidad mayor que cero se puede aproximar por una lemniscata.

**Teorema 3.41** (El teorema de la lemniscata de Hilbert). *Sea  $E$  un conjunto compacto con  $\text{Cap}(E) > 0$  y sea  $U \supset E$  un entorno abierto de  $E$  con  $\mathbb{C} \setminus U$  conexo. Entonces existe un polinomio mónico de grado  $d > 0$ ,  $p[x] = x^d + \dots \in \mathbb{C}[x]$  y una constante  $\rho > \text{Cap}(E)$  tal que*

$$E \subset L_{p, \rho} \subset U.$$

*Demostración.* Como  $E$  es compacto, está acotado. Restringiéndonos a un  $U$  más pequeño si hace falta, podemos suponer que  $U$  también está acotado. Sea  $R > 0$  tal que

$$U \subset B(0, R) = \{z \in \mathbb{C} \mid |z| < R\}.$$

El conjunto  $K := \overline{B}(0, R) \setminus U$  es compacto y, por el Teorema de Frostman 3.25,  $U^{\mu_E} < V_E$  en  $K$ . Por tanto existe  $\epsilon > 0$  tal que  $U^{\mu_E}(z) \leq V_E - \epsilon$  para todo  $z \in K$ .



Por el Teorema 3.27 4 existe un  $n_0$  y para todo  $n \geq n_0$  y todo  $z \in K$

$$\left| \log \frac{1}{|F_n(z)|^{1/n}} - U^{\mu_E}(z) \right| < \epsilon/2,$$

lo que implica

$$(3.14) \quad \log \frac{1}{|F_n(z)|^{1/n}} < V_E - \epsilon/2.$$

Como  $\log(1/|F_n(z)|)$  es armónica en el complementario de  $\overline{B}(0, R)$ , por el Teorema 3.30, la desigualdad (3.14) en  $K$  implica que esta desigualdad es cierta en todo  $\mathbb{C} \setminus U$ .

En consecuencia, para todo  $n \geq n_0$  y  $z \notin U$ ,

$$(3.15) \quad |F_n(z)|^{1/n} > e^{-V_E} e^{\epsilon/2} = \text{Cap}(E) e^{\epsilon/2}.$$

Utilizando ahora el Teorema 3.27 apartados (1) y (2), sabemos que existe un  $n_1$  y para todo  $n \geq n_1$  se tiene

$$\|F_n\|_E^{1/n} < \text{Cap}(E) e^{\epsilon/2}.$$

Eligiendo  $d > \max(n_0, n_1)$  y poniendo  $p = F_d$ ,  $\rho = \text{Cap}(E) e^{\epsilon/2}$  obtenemos el resultado.  $\square$

**3.8. Las órbitas de Galois y el teorema de Fekete.** Un entero algebraico es un número complejo que es solución de un polinomio mónico con coeficientes enteros. El conjunto de enteros algebraicos se denota como  $\overline{\mathbb{Z}}$ . Por tanto  $\zeta \in \overline{\mathbb{Z}}$  si y solo si existe un polinomio  $p(z) = z^n + \dots \in \mathbb{Z}[z]$  tal que

$$(3.16) \quad p(\zeta) = 0$$

Entre todos los polinomios mónicos con coeficientes enteros que cumplen la ecuación (3.16) hay uno de grado mínimo denominado el *polinomio mínimo* de  $\zeta$ . Este polinomio es irreducible sobre los enteros (en caso contrario no sería minimal) y, por tanto, tiene todas sus raíces complejas simples. La órbita de Galois de  $\zeta$  es el conjunto de raíces del polinomio mínimo de  $\zeta$ . La órbita de Galois de  $\zeta$  la denotaremos como  $\text{Gal}(\zeta)$ . El grado del polinomio mínimo de  $\zeta$  se denomina el grado de  $\zeta$ . El primer resultado [9] utiliza la identificación entre la capacidad logarítmica y el diámetro transfinito.

**Teorema 3.42** (Teorema de Fekete). *Sea  $E \subset \mathbb{C}$  un conjunto compacto. Si  $\text{Cap}(E) < 1$ , entonces existe un abierto  $U$  que contiene a  $E$  y tal que el conjunto de enteros  $\zeta \in \overline{\mathbb{Z}}$  con  $\text{Gal}(\zeta) \subset U$  es finito. En particular  $E$  contiene únicamente un número finito de órbitas de Galois.*

*Demostración.* Para cada  $\epsilon > 0$  escribimos

$$B(E, \epsilon) = \{z \in \mathbb{C} \mid d(z, E) < \epsilon\}$$

$$\overline{B}(E, \epsilon) = \{z \in \mathbb{C} \mid d(z, E) \leq \epsilon\},$$

donde  $d(z, E) = \min_{x \in E} |z - x|$ . Como  $E$  es compacto, los conjuntos  $\overline{B}(E, 1/n)$  son compactos y

$$E = \bigcap_{n \geq 1} \overline{B}(E, 1/n).$$

Por tanto

$$\text{Cap}(E) = \lim_{n \rightarrow \infty} \text{Cap}(\overline{B}(E, 1/n)).$$

Como  $\text{Cap}(E) < 1$ , existe  $n_0 > 0$  con  $\text{Cap}(\overline{B}(E, 1/n_0)) < 1$ . Si demostramos que  $\overline{B}(E, 1/n_0)$  solo contiene un número finito de órbitas de Galois, entonces  $U := \overline{B}(E, 1/n_0)$  es un abierto que contiene a  $E$  y que solo contiene un número finito de órbitas de Galois. Reemplazando  $E$  por  $\overline{B}(E, 1/n_0)$  basta demostrar que  $E$  solo contiene un número finito de órbitas de Galois.

Supongamos que  $E$  contiene un número infinito de órbitas de Galois de enteros algebraicos. Elijamos una sucesión numerable de tales orbitas,  $\text{Gal}(\zeta_n)$ ,  $n \geq 1$  y sean  $p_n$  los polinomios mínimos de cada  $\zeta_n$ . Supongamos que hubiera una cota uniforme  $d$  al grado de estos polinomios. Como  $E$  es compacto, está acotado. Dado que los coeficientes de cada  $p_n$  son las funciones simétricas elementales en las raíces de  $p_n$  y, por hipótesis, estas están en  $E$ , deducimos que los coeficientes de los polinomios  $p_n$  están uniformemente acotados. Como el grado es finito solo puede haber un número finito de ellos, contradiciendo la suposición de que el número de órbitas de Galois contenidas en  $E$  es infinito. Así podemos suponer que el grado de los polinomios mínimos no está acotado.

Como estamos asumiendo que el grado de los polinomios  $p_n$  no está acotado, después de restringirse a una subsucesión, podemos suponer que la sucesión de grados

$$d_n := \deg(p_n)$$

es estrictamente creciente.

Por definición

$$(3.17) \quad \delta_{d_n}(E) \geq \left| \prod_{\xi \neq \eta \in \text{Gal}(\zeta_n)} (\xi - \eta) \right|^{1/d_n(d_n-1)} = |\text{disc}(p_n)|^{1/d_n(d_n-1)},$$

donde  $\text{disc}(p_n)$  es el discriminante del polinomio  $p_n$  (ver sección 2.3). Dado que  $p_n$  es el polinomio mínimo de un entero algebraico, es un polinomio mónico con coeficientes enteros. Por la Proposición 2.25, sabemos que  $\text{disc}(p_n)$  es un número entero y por ser  $p_n$  irreducible,  $\text{disc}(p_n)$  es un entero distinto de cero. La ecuación (3.17) implica que  $\delta_{d_n}(E) \geq 1$ . Por tanto

$$\text{Cap}(E) = \tau(E) \geq 1$$

lo que contradice la hipótesis de que  $\text{Cap}(E) < 1$ .  $\square$

**3.9. El teorema de Fekete-Szegö.** El teorema de Fekete-Szegö [10] es casi un recíproco del teorema de Fekete y apareció más de 30 años más tarde que el teorema de Fekete. Este resultado asegura que, si la capacidad logarítmica de un conjunto simétrico respecto a la conjugación compleja, es mayor que uno, entonces todo entorno del conjunto contiene infinitas órbitas de Galois de enteros algebraicos.

**Teorema 3.43** (Fekete-Szegö). *Sea  $E \subset \mathbb{C}$  un subconjunto compacto, simétrico respecto a la conjugación compleja y tal que  $\text{Cap}(E) \geq 1$ . Si  $U \supset E$  es un abierto, entonces  $U$  contiene infinitas órbitas de Galois de enteros algebraicos.*

*Demostración.* Por simplicidad, demostraremos solo el caso en el que  $\mathbb{C} \setminus U$  es conexo. Veamos primero que una lemniscata respecto a un polinomio mónico con coeficientes enteros y con constante  $\rho = 1$  contiene infinitas órbitas de Galois de enteros algebraicos. Sea  $p(z) = z^n + \dots \in \mathbb{Z}[z]$  un polinomio mónico con coeficientes enteros y sea

$$L = \{z \in \mathbb{C} \mid |p(z)| \leq 1\}.$$

Para cada  $n \geq 1$  consideramos el polinomio

$$f_n(z) = p^n(z) - 1.$$

Claramente  $f_n(z)$  es un polinomio mónico con coeficientes enteros y todas las raíces de  $f_n$  están contenidas en  $L$ . Además el conjunto

$$S = \bigcup_{n \geq 1} \{x \in \mathbb{C} \mid f_n(x) = 0\}$$

es infinito, pues la aplicación  $S \rightarrow \{\text{raíces de } 1\}$  dada por  $x \mapsto p(x)$  es exhaustivo. Por lo que  $S$ , y por tanto  $L$ , contiene un número infinito de órbitas de Galois.

En consecuencia, para obtener el resultado, basta demostrar que el conjunto  $U$  contiene la lemniscata de un polinomio mónico con coeficientes enteros y constante 1.

Ya hemos visto, en el Teorema de la lemniscata de Hilbert 3.41, que existe un polinomio  $p(z) = z^d + \dots \in \mathbb{C}[z]$  y una constante  $\rho > 1$  tal que la lemniscata de polinomio  $p$  y constante  $\rho$  está contenida en  $U$ . Ya tenemos un polinomio  $p$ , pero tiene coeficientes complejos. Debemos hacer una serie de reducciones para conseguir un polinomio con coeficientes enteros.

Dado que  $E$  es simétrico respecto a conjugación compleja, podemos reemplazar  $U$  por  $U \cap \bar{U}$  y suponer que  $U$  también es invariante por conjugación compleja. Si ahora  $p$  cumple  $|p(z)| > \rho^d > 1$  para todo  $z \in \mathbb{C} \setminus U$ , entonces  $|p(z)\bar{p}(z)| > \rho^{2d} > 1$  para todo  $z \in \mathbb{C} \setminus U$ . En consecuencia, la lemniscata de polinomio  $p\bar{p}$  y constante  $\rho > 1$  está contenido en  $U$ . Pero el polinomio  $p_1 = p\bar{p}$  tiene coeficientes reales. Esta ha sido la primera reducción.

Usando que los números racionales son densos dentro de  $\mathbb{R}$ , es fácil ver que podemos encontrar un polinomio  $p_2$  con coeficientes racionales y una constante  $1 < \rho' < \rho$  tal que la lemniscata de polinomio  $p_2$  y constante  $\rho'$  está contenida en  $U$ . Nos hemos reducido a un polinomio con coeficientes racionales.

El último paso es ver que podemos construir una lemniscata de polinomio con coeficientes enteros y constante 1. Este proceso se denomina corrección (en inglés “patching”) y está explicado en el siguiente lema.

**Lema 3.44.** *Sea  $p(x) = x^d + \dots \in \mathbb{Q}[x]$  un polinomio mónico con coeficientes racionales y  $1 < \rho \in \mathbb{R}$  un número mayor que uno. Sea  $L$  la lemniscata de polinomio  $p$  y constante  $\rho$ :*

$$L = \{z \in \mathbb{C} \mid |p(z)| \leq \rho^d\}.$$

*Entonces existe un polinomio mónico  $\Gamma(x) \in \mathbb{Z}[x]$  con coeficientes enteros, y la lemniscata de polinomio  $\Gamma$  y constante 1 está contenida en  $L$ .*

*Demostración del Lema 3.44.* Sea  $0 < n \in \mathbb{Z}$  un entero tal que

$$p(x) = x^d + \frac{1}{n}\gamma(x), \quad \gamma(x) \in \mathbb{Z}[x].$$

Si  $n = 1$ ,  $p$  ya tiene coeficientes enteros, así que supondremos que  $n \geq 2$ . Sea  $\mu \geq 1$  un número entero que fijaremos más tarde. Escribimos  $\sigma = \mu d$  y  $\nu = \sigma!n^\sigma$ . Entonces el polinomio  $p^\nu$  tiene los coeficientes de mayor grado enteros:

$$p^\nu(x) = x^{\nu d} + \frac{\nu}{d}x^{d(\nu-1)}\gamma + \dots + \frac{\nu(\nu-1)\dots(\nu-\sigma-1)}{\sigma!n^\sigma}x^{d(\nu-\sigma)}\gamma^\sigma + \binom{\nu}{\sigma+1} \frac{1}{n^{\sigma+1}}x^{d(\nu-\sigma-1)}\gamma^{\sigma+1} + \dots,$$

dada la elección de  $\nu$  todos los coeficientes de la primera fila son enteros. Los coeficientes restantes pueden ser racionales. Observemos que el grado en el que aparece el primer coeficiente que puede ser no entero es

$$d(\nu - \sigma - 1) + (d - 1)(\sigma + 1) = d\nu - \sigma - 1 = d(\nu - \mu) - 1.$$

Así, como mucho, tenemos que corregir  $d(\nu - \mu)$  coeficientes racionales. Ahora corregimos estos coeficientes racionales intentando controlar el tamaño de la corrección. Se pueden encontrar polinomios  $q_\ell$ ,  $\ell = 0, \dots, \nu - \mu - 1$ , de grado menor o igual a  $d - 1$ , cuyos coeficientes sean racionales en el intervalo  $[0, 1)$  y tales que

$$\Gamma(x) := p^\nu(x) + \sum_{\ell=0}^{\nu-\mu-1} p^\ell(x)q_\ell(x) \in \mathbb{Z}[x]$$

tenga coeficientes enteros.

Obsérvese que el polinomio  $\Gamma$  depende de la elección de  $\mu$ . Queda por ver que, mediante una elección adecuada de  $\mu$ , el polinomio  $\Gamma$  cumple que su lemniscata con coeficiente 1 está contenido en  $L$ . La frontera de  $L$  es

$$\partial L = \{z \in \mathbb{C} \mid |p(z)| = \rho^d\}.$$

Escribimos  $\Delta = \Gamma - p^\nu$ . Como los coeficientes de los polinomios  $q_\ell$  están en el intervalo  $[0, 1)$ , para todo  $z \in \partial L$  tenemos la cota

$$\frac{|\Delta(z)|}{|p^\nu(z)|} \leq M \cdot \left| \frac{1}{\rho^{d(\mu+1)}} + \cdots + \frac{1}{\rho^{d\nu}} \right| \leq \frac{M}{\rho^{d\mu}(\rho^d - 1)},$$

donde

$$M = \sup_{z \in \partial L} (1 + |z| + \cdots + |z|^{d-1}).$$

Como  $\rho > 1$ , existe un  $\mu_0$  tal que, para todo  $\mu \geq \mu_0$  y  $z \in \partial L$ ,

$$(3.18) \quad \frac{|\Delta(z)|}{|p^\nu(z)|} \leq \frac{1}{2}.$$

Recordemos el teorema de Rouché de variable compleja. Dadas dos funciones analíticas  $f, g$  en un dominio  $K$ , si  $|f(z)| < |g(z)|$  para todo  $z \in \partial K$ , entonces el número de raíces (contadas con su multiplicidad) de  $g$  y de  $f + g$  contenidas en  $K$  es igual. Este teorema, junto con la ecuación (3.18), implica que todas las raíces de  $\Gamma$  están contenidas en  $L$ .

Por otro lado, para todo  $z \in \partial L$ , tenemos la estimación

$$|\Gamma(z)| \geq |p^\nu(z)| - |\Delta(z)| = \rho^{d\nu} \left( 1 - \frac{|\Delta(z)|}{|p^\nu(z)|} \right) > \frac{\rho^{d\nu}}{2} > \frac{\rho^{d\mu}}{2}.$$

De nuevo, debido a que  $\rho > 1$  podemos encontrar  $\mu_1$ , tal que, para todo  $\mu \geq \mu_1$  y todo  $z \in \partial L$ , se cumple

$$(3.19) \quad |\Gamma(z)| > 1.$$

Utilizando el principio del mínimo para funciones holomorfas, del hecho de que todas las raíces de  $\Gamma$  estén contenidas en  $L$  y la ecuación (3.19) se deduce que, si  $z \notin L$ , entonces  $|\Gamma(z)| > 1$ . Por tanto la lemniscata de polinomio  $\Gamma$  y constante 1 esta contenida en  $L$  concluyendo la demostración del Lema.  $\square$

El Teorema 3.43 es consecuencia del Lema 3.44 y de la discusión precedente.  $\square$

**3.10. Equidistribución de órbitas de Galois en el caso de capacidad uno.** Como siempre  $E \subset \mathbb{C}$  denota un conjunto compacto. Vamos a ver que, en el caso límite, cuando  $\text{Cap}(E) = 1$ , si bien tenemos infinitas órbitas de Galois en un entorno de  $E$ , estas no tienen espacio para moverse y se equidistribuyen según la medida de equilibrio de  $E$ .

**Teorema 3.45.** *Sea  $E \subset \mathbb{C}$  un conjunto compacto con  $\text{Cap}(E) = 1$  y sea  $(\alpha_n)_{n>0}$  una sucesión de enteros algebraicos de grado  $d_n$  cumpliendo*

1.  $\lim_{n \rightarrow \infty} d_n = \infty$ ,
2. Para todo  $n > 0$ ,  $\text{Gal}(\alpha_n) \subset B(E, 1/n)$ .

Entonces

$$\nu(\text{Gal}(\alpha_n)) \xrightarrow{*} \mu^E.$$

*Demostración.* Por el Teorema 3.9, la sucesión  $(\nu(\text{Gal}(\alpha_n)))_{n>0}$  tiene una subsucesión convergente en la topología debil-\*. Si vemos que toda subsucesión convergente de  $\nu(\text{Gal}(\alpha_n))$  converge a  $\mu_E$ , entonces, necesariamente toda la sucesión  $\nu(\text{Gal}(\alpha_n))$  converge a  $\mu^E$ .

Así basta considerar el caso en que la sucesión  $\nu(\text{Gal}(\alpha_n))$  converge en la topología debil-\* a una medida  $\hat{\mu}$  y demostrar que  $\hat{\mu} = \mu^E$ . Para cada  $n$  denotamos por  $P_n$  el

polinomio entero mónico minimal de  $\alpha_n$ . De esta forma,  $\text{Gal}(\alpha_n)$  es el conjunto de raíces de  $P_n$ .

Por el Lema 3.11, tenemos que  $\text{soporte}(\hat{\mu}) \subset E$  y, por tanto,

$$I(\hat{\mu}) \geq V_E = 0.$$

Por otro lado,

$$\begin{aligned} I(\hat{\mu}) &= \int \int \log \frac{1}{|z-t|} d\hat{\mu}(z) d\hat{\mu}(t) \\ &= \lim_{M \rightarrow \infty} \int \int \log_M \frac{1}{|z-t|} d\hat{\mu}(z) d\hat{\mu}(t) \\ &= \lim_{M \rightarrow \infty} \lim_{n \rightarrow \infty} \int \int \log_M \frac{1}{|z-t|} d\nu(\text{Gal}(\alpha_n))(z) d\nu(\text{Gal}(\alpha_n))(t) \\ &\leq \lim_{M \rightarrow \infty} \lim_{n \rightarrow \infty} \left( \frac{1}{d_n^2} \sum_{\beta \neq \beta' \in \text{Gal}(\alpha_n)} \log \frac{1}{|\beta - \beta'|} + \frac{M}{d_n} \right) \\ &\leq \lim_{M \rightarrow \infty} \lim_{n \rightarrow \infty} \left( \frac{-\log(|\text{disc } P_n|)}{d_n^2} + \frac{M}{d_n} \right) \leq 0. \end{aligned}$$

En la última desigualdad hemos usado de nuevo la Proposición 2.25 que implica que  $|\text{disc } P_n|$  es un entero positivo no nulo y, por tanto  $-\log(|\text{disc } P_n|) \leq 0$ . En consecuencia  $I(\hat{\mu}) = 0 = V_E$ . Por la unicidad de la medida de equilibrio deducimos que  $\hat{\mu} = \mu^E$  concluyendo la demostración.  $\square$

#### 4. ALTURAS Y TEOREMA DE BILU

**4.1. Medida de Mahler de un polinomio en una variable.** Sea  $f(x) \in \mathbb{C}[x]$  un polinomio no nulo con coeficientes complejos. Definimos su *medida de Mahler* por

$$M(f) = \exp \left( \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta \right).$$

No es difícil ver que la integral es absolutamente convergente, incluso si el polinomio tiene raíces sobre el círculo unitario.

**Lema 4.1.** *Para todo polinomio no nulo  $f \in \mathbb{C}[x]$ , se tiene  $M(f) = M(f^*)$ .*

*Demostración.* si  $n = \deg f$ , tenemos  $f^*(x) = x^n f(1/x)$ , luego

$$M(f^*) = \exp \left( \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{-i\theta})| d\theta \right).$$

El enunciado resulta entonces de un cambio de variable apropiado.  $\square$

Nos será útil en lo que sigue usar la función  $\log^+$ , dada por

$$\log^+ z = \begin{cases} \log z & \text{si } z \geq 1 \\ 0 & \text{si } 0 < z < 1 \end{cases}$$

La medida de Mahler satisface las propiedades siguientes:

**Teorema 4.2.** 1.  $M(fg) = M(f)M(g)$ , para todo  $f, g \in \mathbb{C}[x]$ ,  $fg \neq 0$ .

2.  $M(f) > 0$ , para todo  $f \in \mathbb{C}[x]$ , no nulo.

3. (Fórmula de Jensen) Sea  $f(x) \in \mathbb{C}[x]$ , un polinomio no nulo de grado  $n$ , que escribimos de la forma

$$(4.1) \quad f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad a, \alpha_1, \dots, \alpha_n \in \mathbb{C}.$$

Entonces

$$(4.2) \quad \log M(f) = \log |a| + \sum_{i=1}^n \log^+ |\alpha_i|.$$

*Demostración.* Las primeras dos propiedades se deducen directamente de la definición. Usando (1), nos reducimos a mostrar que para todo  $\alpha \in \mathbb{C}$ , se tiene

$$(4.3) \quad \frac{1}{2\pi} \int_0^{2\pi} \log |e^{i\theta} - \alpha| d\theta = \log^+ |\alpha|.$$

Para demostrar esta identidad, usaremos que el promedio de una función armónica  $h$  sobre el borde del círculo unitario es  $h(0)$ .

Si  $|\alpha| > 1$ , entonces la función  $h(x) = \log |x - \alpha|$  es armónica en el disco unitario, de manera que el término izquierdo de (4.3) es  $h(0) = \log |\alpha|$ .

Si  $|\alpha| < 1$ , entonces la función  $w(x) = \log |1 - \alpha\bar{x}|$  es armónica en el disco unitario y coincide con  $h(x)$  cuando  $|x| = 1$ . Por lo tanto el término izquierdo de (4.3) es  $w(0) = \log |1| = 0$ .

El caso  $|\alpha| = 1$  se deduce por la continuidad de la función  $\alpha \mapsto \int_0^{2\pi} \log |e^{i\theta} - \alpha| d\theta$ .  $\square$

*Ejercicio 4.3.* Demostrar

$$|D(f)| \leq n^n M(f)^{2n-2},$$

donde  $D(f)$  denota el discriminante de  $f$  (Sección 2.3)

Indicación: exprese el discriminante como un determinante de Vandermonde.

**4.2. Altura de un número algebraico.** Sea  $\alpha \in \overline{\mathbb{Q}}^*$  y sea  $f_\alpha(x) \in \mathbb{Q}[x]$  su polinomio mínimo. Existe un único entero positivo  $m$  tal que el polinomio

$$g_\alpha(x) := mf_\alpha(x)$$

satisface

- $g_\alpha(x)$  tiene coeficientes enteros
- el máximo común divisor de los coeficientes de  $g_\alpha(x)$  es 1.

Decimos que  $g_\alpha(x)$  es el *polinomio mínimo sobre  $\mathbb{Z}$  de  $\alpha$* .

El claro que la órbita galoisiana de  $\alpha$  se calcula por

$$\text{Gal}(\alpha) = \{\beta \in \mathbb{C} : g_\alpha(\beta) = 0\}$$

(cf. Definición 2.16).

**Definición 4.4.** Sea  $\alpha \in \overline{\mathbb{Q}}^*$ . Definimos su *altura* (de Weil) por

$$h(\alpha) = \frac{1}{\deg \alpha} \log M(g_\alpha).$$

De los lemas 2.8 y 4.1 deducimos

**Lema 4.5.** Para todo  $\alpha \in \overline{\mathbb{Q}}^*$ , se tiene  $h(\alpha) = h(1/\alpha)$ .

Escribiendo

$$g_\alpha(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

de la fórmula de Jensen (4.2) se tiene

$$(4.4) \quad h(\alpha) = \frac{1}{\deg \alpha} \left( \log |a_n| + \sum_{\beta \in \text{Gal}(\alpha)} \log^+ |\beta| \right).$$

**Proposición 4.6.** Se tiene que  $h(\alpha) \geq 0$ , para todo  $\alpha \in \overline{\mathbb{Q}}^*$ . Más aún,  $h(\alpha) = 0$  si y solo si  $\alpha$  es una raíz de la unidad.

*Demostración.* En la expresión (4.4),  $|a_n|$  es un entero positivo, de donde es claro que  $h(\alpha) \geq 0$ . Si  $\alpha$  es una raíz de la unidad, la Proposición 2.19 asegura que  $|\beta| = 1$ , para todo  $\beta \in \text{Gal}(\alpha)$ . Además, de la Observación 2.13 tenemos que su polinomio mínimo sobre  $\mathbb{Z}$  es mónico. Usando nuevamente (4.4), tenemos  $h(\alpha) = 0$ .

Supongamos ahora  $h(\alpha) = 0$ . Sea  $n = \deg(\alpha)$ . Escribamos

$$(4.5) \quad g_\alpha(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Z}.$$

Entonces la expresión (4.4) garantiza que  $a_n = 1$  y

$$(4.6) \quad |\beta| \leq 1,$$

para todo  $\beta \in \text{Gal}(\alpha)$ .

La desigualdad (4.6) también vale para productos de elementos en  $\text{Gal}(\alpha)$ . Entonces, de la fórmula  $g_\alpha(x) = \prod_{\beta \in \text{Gal}(\alpha)} (x - \beta)$ , vemos que los coeficientes de  $g_\alpha(x)$  satisfacen

$$(4.7) \quad |a_j| \leq n, \quad \forall j = 0, 1, 2, \dots, n.$$

Sea  $S_n$  el conjunto formado por todos los polinomios con coeficientes enteros, de grado a lo más  $n$ , de la forma (4.5) que además satisfacen (4.7). Tenemos que  $S_n$  es un conjunto finito.

Ahora bien, si  $k$  es un entero positivo, usando el Ejercicio 2,21, (2) vemos que el razonamiento anterior también se aplica a  $\alpha^k$ , es decir,  $\{g_{\alpha^k}(x) : k \in \mathbb{Z}_{>0}\} \subseteq S_n$ . Como  $S_n$  es finito, el conjunto de raíces de polinomios en  $S_n$  también lo es, luego el conjunto

$$\{\alpha^k : k \in \mathbb{Z}_{>0}\}$$

es finito. Por lo tanto, existen enteros  $k_1 \neq k_2$  tales que  $\alpha^{k_1} = \alpha^{k_2}$  (equivalentemente,  $\alpha^{k_1 - k_2} = 1$ ), lo que prueba que  $\alpha$  es una raíz de la unidad  $\square$

Terminamos esta sección con un problema abierto.

**Pregunta 4.7.** (Lehmer [12]). Decidir si la siguiente afirmación es cierta: existe una constante  $c > 0$  tal que

$$h(\alpha) \geq \frac{c}{\deg \alpha}, \quad \forall \alpha \in \overline{\mathbb{Q}}^* \text{ que no es una raíz de la unidad.}$$

*Ejercicio 4.8.* Adapte la demostración de la Proposición 4.6 para demostrar el teorema de Northcott: Sean  $A, B > 0$ . El conjunto

$$\{\alpha \in \overline{\mathbb{Q}}^* : \deg(\alpha) \leq A, \quad h(\alpha) \leq B\}$$

es finito.

### 4.3. Enunciado del Teorema de Bilu en dimensión 1.

**Definición 4.9.** Sean  $C \subset \mathbb{C}$  y  $\nu \in \mathcal{M}(\mathbb{C})$ . Decimos que  $\nu$  está soportada en  $C$  si para toda  $f \in C_0(\mathbb{C})$  cuyo soporte es disjunto a  $C$ , se tiene

$$\int_{\mathbb{C}} f \nu = 0.$$

Si  $\nu$  está soportada en un conjunto compacto, decimos que  $\nu$  tiene soporte compacto.

Denotamos por  $\mathcal{M}(C) \subseteq \mathcal{M}(\mathbb{C})$  al conjunto de medidas soportadas en  $C$ .

**Ejemplo 4.10.** Denotamos por  $\nu_S$  la medida caracterizada por

$$(4.8) \quad \int_{\mathbb{C}} f \nu_S = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta, \quad \forall f \in C_0(\mathbb{C}).$$

Es claro que  $\nu_S$  está soportada en el círculo unitario y una medida de contaje de la forma  $\nu(E)$  está soportada en  $E$ . Todas estas medidas tienen soporte compacto.

Recordemos el Teorema 3.9, cuando  $C$  es compacto, el espacio  $\mathcal{M}(C)$  es secuencialmente compacto. Es decir, toda sucesión  $(\nu_n) \subset \mathcal{M}(C)$  admite una subsucesión convergente.

**Definición 4.11.** Consideremos una sucesión  $E_n \subset \mathbb{C}$ , donde cada  $E_n$  es un conjunto finito. Decimos que la familia  $(E_n)$  se *equidistribuye con respecto a*  $\nu \in M$  si

$$\lim_{n \rightarrow \infty} \nu(E_n) = \nu.$$

Aquí,  $\nu(E_n)$  es la medida de conteo definida en (3.1).

De manera equivalente, se pide que para toda  $f \in C_0(\mathbb{C})$ ,

$$\lim_{n \rightarrow \infty} \frac{1}{\#E_n} \sum_{z \in E_n} f(z) = \int_{\mathbb{C}} f \nu.$$

**Definición 4.12.** Decimos que una sucesión  $(x_n) \subset \mathbb{C}$  es *genérica* si para todo  $m \in \mathbb{N}$ , el conjunto

$$\{k \in \mathbb{N} : x_k = x_m\}$$

es finito.

**Teorema 4.13.** (Bilu, [5]) Sea  $\nu_S$  la medida de probabilidad uniforme sobre el círculo, dada por (4.8). Sea  $(\alpha_n) \subset \overline{\mathbb{Q}}^*$  una sucesión genérica de números algebraicos tal que

$$\lim_{n \rightarrow \infty} h(\alpha_n) = 0.$$

Entonces la familia de conjuntos  $\text{Gal}(\alpha_n)$  se equidistribuye con respecto a  $\nu_S$ .

En particular, se tiene el siguiente resultado notable:

**Corolario 4.14.** La sucesión de conjuntos  $(\tilde{\mu}_n)$  se equidistribuye con respecto a la medida  $\nu_S$ .

*Demostración.* tomando en cuenta la Proposición 2.19 y la Proposición 4.6, el enunciado se deduce directamente del Teorema de Bilu  $\square$

*Ejercicios 4.15.* El propósito de los ejercicios de esta sección es de indicar una demostración del Corolario 4.14 que no utiliza el Teorema de Bilu.

1. Sea  $X$  un espacio métrico compacto. Los espacios  $\mathcal{M}(X)$ ,  $C_0(X)$  y la noción de convergencia de medidas se definen como en la Sección 3.2. El espacio  $C_0(X) = C(X)$  se encuentra dotado de la topología dada por la norma supremo:

$$\|f\| = \sup_{z \in X} |f(z)|.$$

Sea  $H \subset C(X)$  una subálgebra (es decir,  $f, g \in H \rightarrow fg, f + g \in H$ ). Sea  $V \subset H$  un conjunto generador (es decir, todo elemento de  $H$  es una combinación  $\mathbb{C}$ -lineal finita de elementos de  $V$ ). Suponga que  $H$  es conjunto denso. Muestre que la sucesión de medidas  $(\nu_n) \in \mathcal{M}(X)$  converge a  $\nu \in \mathcal{M}(X)$  si y solo si

$$\int_X f \nu_n = \int_X f \nu, \quad \forall f \in V.$$

2. a) En la notación del ejercicio anterior, tome  $X = \{z \in \mathbb{C} : |z| = 1\}$ . Para cada  $k \in \mathbb{Z}$ , definimos  $h_k : X \rightarrow \mathbb{C}$  por  $h_k(x) = x^k$ . Sea  $H \subset C(X)$  la subálgebra generada por  $\{h_k : k \in \mathbb{Z}\}$ . Muestre que  $H$  es densa en  $C(X)$ . Indicación: use el teorema de Stone-Weierstrass.
- b) (Criterio de Weyl) Sea  $E_n \subset X$  una sucesión de conjuntos finitos. Deduzca que la familia  $(E_n)$  se equidistribuye con respecto a  $\nu_S$  si y solo si para todo  $k \in \mathbb{Z}$ , con  $k \neq 0$ , se tiene

$$\lim_{n \rightarrow \infty} \frac{1}{\#E_n} \sum_{z \in E_n} z^k = 0.$$



- c) Utilizando el punto anterior, demuestre que la sucesión de conjuntos  $\mu_n$  se equidistribuye con respecto a  $\nu_S$ .
3. El propósito de este ejercicio es demostrar el Corolario 4.14, usando los ejercicios anteriores.

a) Sea  $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$  la función de Möbius, dada por

$$\mu(n) = \begin{cases} 0 & \text{si existe un entero } m \geq 2 \text{ tal que } m^2 | n \\ (-1)^r & \text{si } n \text{ es el producto de } r \text{ primos distintos.} \end{cases}$$

Sea  $\delta_1 : \mathbb{N} \rightarrow \{0, 1\}$  dada por

$$\delta_1(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Demuestre

$$\sum_{d|n} \mu(d) = \delta_1(n).$$

- b) *Sumas de Ramanujan.* Denotamos por  $(a, b)$  el máximo común divisor del par  $a, b$ . Para  $n \in \mathbb{N}$  y  $k \in \mathbb{Z} - \{0\}$ , definimos

$$S(n, k) = \sum_{\substack{0 \leq j \leq n-1 \\ (n, j)=1}} \zeta_n^{jk}, \quad \zeta_n = e^{2\pi i/n}.$$

Muestre que

$$S(n, k) = \sum_{d|(n, k)} d\mu\left(\frac{n}{d}\right).$$

Indicación: escriba  $S(n, k) = \sum_{j=0}^{n-1} \delta_1((n, k)) \zeta_n^{jk}$  y aplique el punto anterior.

- c) Demuestre el Corolario 4.14.

**4.4. Energía.** Consideremos la medida  $\nu_S$  definida en (4.8). Usando (4.3) y la definición de energía de una medida en (3.2), vemos que  $I(\nu_S) = 0$ . Además, para todo conjunto finito  $G \subset \mathbb{C}$ , se tiene  $I(\nu(G)) = \infty$ .

En vista del último ejemplo, es útil considera la cantidad  $I'(G)$  definida en (3.3). El nexa entre la teoría de alturas y la teoría del potencial está dado por el siguiente

**Lema 4.16.** (*Comparación Energía-Altura*) Sea  $\alpha \in \overline{\mathbb{Q}}^*$  con  $n := \deg(\alpha) \geq 2$ . Para  $a \in \mathbb{C}$  y  $0 < \varepsilon < 1$  denotamos  $D(a, \varepsilon) = \{\beta \in \text{Gal}(\alpha) : |\beta - a| \leq \varepsilon/2\}$  y  $n_\varepsilon = \#D(a, \varepsilon)$ . Entonces se tiene

$$|\log \varepsilon| \cdot \frac{n_\varepsilon(n_\varepsilon - 1)}{n(n - 1)} - \frac{2n}{n - 1} \tilde{h}(2\alpha) \leq I'(\text{Gal}(\alpha)) \leq 3h(\alpha).$$

Aquí,  $\tilde{h}(2\alpha) := \frac{1}{n} \sum_{\beta \in \text{Gal}(\alpha)} \log^+(|2\beta|)$ .

*Demostración.* Primero demostraremos la cota superior. Sea  $a_n$  el coeficiente dominante de  $g_\alpha$  y escribimos  $\text{Gal}(\alpha) = \{\alpha_1, \dots, \alpha_n\}$ . Como  $g_\alpha$  es irreducible, tenemos  $D(g_\alpha) \neq \emptyset$ . Además,  $a_n D(g_\alpha) \in \mathbb{Z}$  (Proposición 2.25), de donde

$$(4.9) \quad \log(a_n |D(g_\alpha)|) \geq \log 1 = 0.$$

Se tiene

$$\begin{aligned}
0 \leq \log a_n + \log |D(g_\alpha)| &= (2n-1) \log a_n + 2 \sum_{i < j} \log |\alpha_i - \alpha_j| \\
&= (2n-1) \log a_n + \sum_{i \neq j} \log |\alpha_i - \alpha_j| \\
&= (2n-1) \log a_n - n(n-1) I'(\text{Gal}(\alpha)).
\end{aligned}$$

Por otro lado, de (4.4) tenemos

$$\log a_n = nh(\alpha) - \sum_i \log^+ |\alpha_i| \leq nh(\alpha).$$

Combinando ambas desigualdades se obtiene la cota superior.

Ahora demostraremos la cota inferior. Escribimos  $I'(\alpha) = A + B + C$ , con

$$\begin{aligned}
A &= \frac{1}{n(n-1)} \sum_{\substack{|\alpha_i - \alpha_j| \leq \varepsilon \\ i \neq j}} \log \frac{1}{|\alpha_i - \alpha_j|} \\
B &= \frac{1}{n(n-1)} \sum_{\varepsilon < |\alpha_i - \alpha_j| \leq 1} \log \frac{1}{|\alpha_i - \alpha_j|} \\
C &= \frac{1}{n(n-1)} \sum_{|\alpha_i - \alpha_j| > 1} \log \frac{1}{|\alpha_i - \alpha_j|}
\end{aligned}$$

Claramente  $B \geq 0$ . Además, como  $\alpha_i, \alpha_j \in D(a, \varepsilon)$  implica  $|\alpha_i - \alpha_j| \leq \varepsilon$ , deducimos

$$A \geq \log(1/\varepsilon) \frac{n_\varepsilon(n_\varepsilon - 1)}{n(n-1)}.$$

Para acotar inferiormente  $C$ , supondremos  $|\alpha_1| \leq |\alpha_2| \leq \dots \leq |\alpha_n|$ . Entonces

$$\begin{aligned}
\sum_{|\alpha_i - \alpha_j| > 1} \log |\alpha_i - \alpha_j| &= 2 \sum_{i < j} \log^+ |\alpha_i - \alpha_j| \\
&= 2 \sum_{i=1}^n \sum_{j=i+1}^n \log^+ |\alpha_i - \alpha_j| \\
&\leq 2 \sum_{i=1}^n \sum_{j=i+1}^n \log^+ |2\alpha_j| \\
&\leq 2 \sum_{i=1}^n n \tilde{h}(2\alpha) \\
&= 2n^2 \tilde{h}(2\alpha),
\end{aligned}$$

de donde se obtiene  $C \geq -\frac{2n}{n-1} \tilde{h}(2\alpha)$ . Reuniendo las cotas inferiores para  $A, B$  y  $C$ , se obtiene el resultado.  $\square$

Enunciamos aquí un resultado que caracteriza la medida de Lebesgue sobre el círculo en términos del funcional de energía.

**Proposición 4.17.** *Sea  $\mathcal{M}(S)$  el conjunto de todas las medidas en  $\mathcal{M}$  soportadas en  $\{z \in \mathbb{C} : |z| = 1\}$ . Entonces*

$$I(\nu) \geq 0, \quad \forall \nu \in \mathcal{M}(S).$$

Más aún,

$$\nu \in \mathcal{M}(S), \quad I(\nu) = 0 \Leftrightarrow \nu = \nu_S.$$

*Demostración.* Usar el Ejercicio 3.26 (1) de la Sección 3. Alternativamente, ver [16], Ex. 1.10.  $\square$

**4.5. Demostración del Teorema de Bilu.** En toda esta sección asumimos que la sucesión  $(\alpha_n) \subset \overline{\mathbb{Q}}^*$  es genérica y cumple

$$h(\alpha_n) \rightarrow 0, \quad n \rightarrow \infty.$$

Unidas al Ejercicio 4.8, estas hipótesis aseguran que  $\deg(\alpha_n)$  tiende a infinito con  $n$ .

**Lema 4.18.** (*Equidistribución en radio*). *Para cada  $n \in \mathbb{N}$ , se puede escoger un conjunto  $E_n \subseteq \text{Gal}(\alpha_n)$  de manera que*

1. *se tiene*

$$\lim_{n \rightarrow \infty} \frac{\#E_n}{\#\text{Gal}(\alpha_n)} = 1.$$

2. *Para todo  $\varepsilon > 0$ , existe  $n_0$  tal que para todo  $n \geq n_0$  se tiene*

$$z \in E_n \Rightarrow 1 - \varepsilon \leq |z| \leq 1 + \varepsilon.$$

*Demostración.* Notar que por el Lema 4.5, también tenemos

$$h(1/\alpha_n) \rightarrow 0, \quad n \rightarrow \infty.$$

Procederemos por contradicción. Pasando a una subsucesión si fuese necesario, podemos suponer que existen subconjuntos  $V_n \subseteq \text{Gal}(\alpha_n)$  tales que

- $\lim_{n \rightarrow \infty} \frac{\#V_n}{\#\text{Gal}(\alpha_n)} = c > 0$ .
- existe  $a > 1$  tal que para todo  $n$ , se tiene

$$z \in V_n \Rightarrow |z| > a \text{ ó } \left| \frac{1}{z} \right| > a.$$

Descomponemos  $V_n = A_n \cup B_n$ , donde

$$z \in A_n \Leftrightarrow |z| > a, \quad z \in B_n \Leftrightarrow \left| \frac{1}{z} \right| > a.$$

Usando la fórmula de Jensen tenemos

$$h(\alpha_n) \geq \frac{1}{\deg(\alpha_n)} \left( \sum_{\beta \in A_n} \log |\beta| \right) \geq \frac{\#A_n}{\deg(\alpha_n)} \log a.$$

Por otro lado, usando el Ejercicio 2.21 (2) también se tiene

$$h(1/\alpha_n) \geq \frac{1}{\deg(\alpha_n)} \left( \sum_{\beta \in B_n} \log |1/\beta| \right) \geq \frac{\#B_n}{\deg(\alpha_n)} \log a.$$

Luego

$$h(\alpha_n) + h(1/\alpha_n) \geq \frac{\#V_n}{\deg \alpha_n} \log a.$$

Tomando el límite cuando  $n \rightarrow \infty$ , obtenemos

$$0 \geq c \log a > 0,$$

lo que es absurdo.  $\square$

**Fin de la demostración del Teorema de Bilu:** la condición (2) en el Lema 4.18, asegura que existe un compacto  $K \subset \mathbb{C}$  que contiene al círculo unitario tal que  $\nu(E_n) \in \mathcal{M}(K)$ , para todo  $n$ . Como  $\mathcal{M}(K)$  es secuencialmente compacto (cf. Teorema 3.9), tenemos que la sucesión  $\nu(E_n)$  admite una subsucesión  $\nu(E_{n_j})$  convergente a una medida  $\nu \in \mathcal{M}(K)$ . Notar que la condición (1) en el Lema 4.18 asegura que  $\nu(\text{Gal}(\alpha_{n_j}))$  también converge a  $\nu$ . Ahora estableceremos que la diagonal tiene medida nula con respecto a la medida producto  $\nu \times \nu$  (para ver generalidades y referencias sobre medidas producto revisar la demostración del Teorema 3.22).

**Afirmación.** Sea  $D = \{(x, x) : x \in \mathbb{C}\} \subseteq \mathbb{C}^2$ . Entonces  $\nu \times \nu(D) = 0$ .

Para demostrar la afirmación, razonaremos por contradicción. Si  $\nu \times \nu(D) > 0$ , entonces existe  $a \in \mathbb{C}$  tal que  $\nu(\{a\}) > 0$ . En particular, existe  $\kappa > 0$ , un conjunto infinito  $J \subset \mathbb{N}$  tal que para todo  $n \in J$  y todo  $\varepsilon > 0$  suficientemente pequeño, se cumple

$$\frac{\#\{\beta \in \text{Gal}(\alpha_n) : |\beta - a| \leq \varepsilon/2\}}{\deg \alpha_n} \geq \kappa.$$

Usando el Lema 4.16, deducimos que para  $n \in J$  se tiene

$$(4.10) \quad |\log \varepsilon| \cdot \kappa - \frac{2 \deg(\alpha_n)}{\deg(\alpha_n) - 1} \tilde{h}(2\alpha_n) \leq 3h(\alpha_n).$$

Es sencillo ver que  $\tilde{h}(2\alpha_n) \leq h(\alpha_n) + \log 2$ . Como  $\lim_{n \rightarrow \infty} h(\alpha_n) = 0$ , vemos que  $h(2\alpha_n)$  es acotado. De la desigualdad (4.10) deducimos que existe  $A \in \mathbb{R}$  tal que para todo  $\varepsilon$  suficientemente pequeño, se tiene  $|\log \varepsilon| \cdot \kappa \leq A$ . Esto es absurdo, luego la afirmación es verdadera.

Ahora demostraremos que  $\nu = \nu_S$ . Primero notemos que usando la condición (2) en el Lema 4.18, podemos concluir que  $\nu$  está soportada en el círculo unitario. De la Proposición 4.17, deducimos que  $I(\nu) \geq 0$ . Sea  $\phi : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$  una función continua no decreciente tal que

- $0 \leq \phi \leq 1$
- $\phi(t) = 0$  si  $t \leq \frac{1}{2}$
- $\phi(t) = 1$  si  $t \geq 1$

Para  $\varepsilon > 0$ , definimos  $\phi_\varepsilon(t) = \phi(t/\varepsilon)$ . Entonces, para todo  $(z, t) \in \mathbb{C}^2 - D$ , se tiene

$$\lim_{\varepsilon \rightarrow 0} \phi_\varepsilon(|z - t|) \log \frac{1}{|z - t|} = \log \frac{1}{|z - t|}.$$

Como  $D$  es un conjunto de medida nula según  $\nu \times \nu$ , el Teorema de convergencia monótona asegura que

$$\begin{aligned} I(\nu) &= \int \int \log \frac{1}{|z - t|} d\nu(z) d\nu(t) \\ &= \lim_{\varepsilon \rightarrow 0} \int \int \phi_\varepsilon(|z - t|) \log \frac{1}{|z - t|} d\nu(z) d\nu(t) \end{aligned}$$

Sea

$$S_{j,\varepsilon} = \frac{1}{|E_{n_j}|^2} \sum_{\beta, \beta' \in E_{n_j}} \phi_\varepsilon(|\beta - \beta'|) \log \frac{1}{|\beta - \beta'|}.$$

Por convergencia débil tenemos

$$\int \int \phi_\varepsilon(|z - t|) \log \frac{1}{|z - t|} d\nu(z) d\nu(t) = \lim_{j \rightarrow \infty} S_{j,\varepsilon}.$$

Si  $\varepsilon$  es suficientemente pequeño, tenemos que  $|\beta - \beta'| \leq \varepsilon \Rightarrow \log \frac{1}{|\beta - \beta'|} \geq 0$ . Además,  $|\beta - \beta'| \geq \varepsilon \Rightarrow \phi_\varepsilon(|\beta - \beta'|) = 1$ . Como  $0 \leq \phi_\varepsilon \leq 1$  en todos los casos, concluimos que

$$S_{j,\varepsilon} \leq \frac{1}{|E_{n_j}|^2} \sum_{\substack{\beta, \beta' \in E_{n_j} \\ \beta \neq \beta'}} \log \frac{1}{|\beta - \beta'|}.$$

Combinando las estimaciones anteriores, deducimos que

$$\begin{aligned} I(\nu) &\leq \liminf_{n \rightarrow \infty} \frac{1}{|E_{n_j}|^2} \sum_{\substack{\beta, \beta' \in E_{n_j} \\ \beta \neq \beta'}} \log \frac{1}{|\beta - \beta'|} \\ &= \liminf_{n \rightarrow \infty} I'(E_{n,j}) \\ &= \liminf I'(\text{Gal}(\alpha_{n_j})) \quad \text{condición (1) en el Lema 4.18} \\ &\leq 3 \liminf h(\alpha_{n_j}) \quad \text{Lema 4.16} \\ &= 0. \end{aligned}$$

Por lo tanto,  $I(\nu) = 0$ . Aplicando nuevamente la Proposición 4.17, deducimos  $\nu = \nu_S$ .

Hemos establecido que toda subsucesión convergente de  $\nu(E_n)$  tiene como límite a la medida  $\nu_S$ . Esto muestra que  $\nu(E_n)$  converge a  $\nu_S$ . Luego  $\nu(\text{Gal}(\alpha_n))$  converge a  $\mu_S$ , terminando la demostración del Teorema de Bilu.

## 5. GENERALIZACIONES Y APLICACIONES DIOFANTINAS

En esta sección haremos algunos comentarios sobre extensiones de los teoremas vistos en el curso, así como aplicaciones.

*Varias variables.* El teorema que Bilu demuestra en su artículo [5] es más general que lo que hemos formulado aquí, pues trata el caso de un número finito arbitrario de variables. La demostración en el caso de dimensión general se reduce al caso de dimensión 1 por un argumento estándar de análisis de Fourier.

*Versiones  $p$ -ádicas.* Los números complejos tienen un análogo  $p$ -ádico: si  $p$  es un número primo y  $\mathbb{Q}_p$  el cuerpo de los números  $p$ -ádicos, entonces norma  $p$ -ádica admite una única extensión a la cerradura algebraica  $\overline{\mathbb{Q}_p}$ . Así, podemos considerar su completación, denotada  $\widehat{\overline{\mathbb{Q}_p}}$ . El cuerpo resultante no es algebraicamente cerrado. Denotamos por  $\mathbb{C}_p$  a la cerradura algebraica de  $\widehat{\overline{\mathbb{Q}_p}}$ . Este último cuerpo es a la vez completo y algebraicamente cerrado. El lector podrá consultar en [15] el desarrollo de los conceptos y relaciones que dan lugar a una teoría del potencial sobre  $\mathbb{C}_p$ , análoga a la teoría sobre  $\mathbb{C}$  que hemos revisado. También encontrará una formulación del Teorema de Fekete-Szegö en tal contexto. El Teorema de Bilu también tiene un análogo  $p$ -ádico, ver [2], [7] o [8].

*Relación con problemas diofantinos* Una de las principales motivaciones para estudiar teoremas de equidistribución aritméticos es la posibilidad de aplicarlos en cuestiones diofantinas. Un ejemplo básico es el siguiente: decimos que  $(\alpha, \beta) \in \mathbb{C}^2$  es un punto de torsión si  $\alpha$  y  $\beta$  son raíces de la unidad. Una subvariedad de torsión de  $\mathbb{C}^2$  es un conjunto de la forma

$$\{x, y : x^n y^m = \zeta\},$$

donde  $m, n$  son números enteros, no ambos cero y  $\zeta \in \mathbb{C}$  es una raíz de la unidad.

**Teorema 5.1.** *Sea  $X \subseteq \mathbb{C}^2$  un subconjunto Zariski cerrado propio. Entonces  $X$  contiene infinitos puntos de torsión si y solo si  $X$  contiene una subvariedad de torsión.*

Este resultado puede deducirse del Teorema de Bilu (ver [5], Theorem 5.1) y es un caso particular de la conjetura de Manin-Mumford. Para mayor información sobre el nexo entre teoremas de equidistribución y problemas de geometría diofantina se recomienda ver [19], [20].

#### REFERENCIAS

- [1] P. Autissier, *Autour du théorème de Fekete-Szegő*, École d'été de géométrie d'Arakelov, Grenoble, 2017. <https://www.math.u-bordeaux.fr/~pautissi/>
- [2] M. Baker, R. Rumely, *Equidistribution of small points, rational dynamics, and potential theory*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 3, 625-688
- [3] P. Billingsley. *Convergence of probability measures*. Wiley Series in Probability and Statistics: Probability and Statistics. John Wiley & Sons, Inc., New York, second edition, 1999. A Wiley-Interscience Publication.
- [4] P. Billingsley. *Probability and Measure*. John Wiley & Sons, Inc., New York, second edition, 1986.
- [5] Y. Bilu. Limit distribution of small points on algebraic tori. *Duke Math. J.*, 89(3):465–476, 1997.
- [6] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.
- [7] A. Chambert-Loir, *Mesures et équidistribution sur les espaces de Berkovich*, J. Reine Angew. Math. **595** (2006), p. 215-235
- [8] Ch. Favre, J. Rivera-Letelier, *Équidistribution quantitative des points de petite hauteur sur la droite projective*, Math. Ann. **335** (2006), no. 2, p. 311-361
- [9] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. **17** (1923), p. 228-249.
- [10] M. Fekete, G. Szegő, *On algebraic equations with integral coefficients whose roots belong to a given point set*, Math. Z. **63** (1955), 158-172.
- [11] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [12] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math. (2)*, 34(3):461–479, 1933.
- [13] T. Ransford, *Potential theory in the complex plane*, Cambridge Univ. Press, 1995.
- [14] W. Rudin, *Functional analysis* McGraw Hill, 1973.
- [15] R. Rumely. *Capacity theory on algebraic curves*, volume 1378 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1989.
- [16] E. B. Saff, *Logarithmic potential theory with applications to approximation theory*, Surv. Approx. Theory **5** (2010), 165-200.
- [17] E. B. Saff, V. Totik, *Logarithmic potential with external fields*, Grundlehren der mathematischen Wissenschaften **316**, Springer Verlag 1997.
- [18] T. Tao, *An introduction to measure theory*, Graduate Studies in Mathematics **126**, AMS 2011.
- [19] E. Ullmo, *Manin-Mumford, André-Oort, the equidistribution point of view*, Equidistribution in number theory, an introduction, 103-138, NATO Sci. Ser. II Math. Phys. Chem., 237, Springer, Dordrecht, 2007
- [20] E. Ullmo, *Théorie ergodique et géométrie arithmétique*, Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), 197-206.

ICMAT (CSIC UAM UCM UC3). NICOLÁS CABRERA 13, 28049 MADRID, ESPAÑA.

*Email address:* burgos@icmat.es

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

*Email address:* rmenares@mat.uc.cl