El diablo de los números

Sección a cargo de

Javier Fresán

La casa de los números pequeños

por

Yuri Bilu, José Ignacio Burgos Gil y Martín Sombra

1. Introducción

Un *número algebraico* es un número complejo que es raíz de un polinomio con coeficientes enteros. Estos números forman un cuerpo que se denota por $\overline{\mathbb{Q}}$, que es el lugar natural donde se encuentran soluciones de las ecuaciones polinomiales con coeficientes racionales. Por ejemplo, por un teorema de Euler, la ecuación $X^3 + Y^3 = 1$ sólo tiene dos soluciones racionales, que son $(X, Y) = (1, 0)$ y $(0, 1)$, mientras que es fácil ver que tiene infinitas soluciones algebraicas.

Un *entero algebraico* es un número algebraico que es raíz de un polinomio mónico con coeficientes enteros. Los enteros algebraicos forman un anillo que se denota por $\overline{\mathbb{Z}}$. Todo número algebraico es el cociente de un entero algebraico por un número entero, por lo que $\overline{\mathbb{Z}}$ juega, dentro de $\overline{\mathbb{Q}}$, el mismo papel que $\mathbb{Z}$ dentro de $\mathbb{Q}$.

Dado un entero algebraico α, entre todos los polinomios mónicos con coeficientes enteros que lo tienen como raíz existe uno con el menor grado posible. Este polinomio mónico se denomina el *polinomio mínimo* de α.

La existencia del polinomio mínimo tiene varias consecuencias interesantes. La primera es que a un entero algebraico α se le puede asociar un parámetro que mide su complejidad, el *grado*, y que se define como el grado de su polinomio mínimo.

La segunda consecuencia es que los enteros algebraicos no vienen solos. Si α tiene grado d, las distintas raíces de su polinomio mínimo

$$\alpha_1, \dots, \alpha_d$$

se denominan los *conjugados* de α.

La tercera consecuencia es que los enteros algebraicos pueden ser codificados con una cantidad finita de información ya que, salvo conjugación, están determinados por su polinomio mínimo. Esto permite trabajar con los enteros algebraicos de forma

simbólica manteniendo precisión infinita, así como clasificar los enteros algebraicos según la cantidad de información necesaria para determinarlos.

Nos interesa entonces tener un parámetro adicional asociado al entero algebraico α que, junto con su grado, capture la cantidad de información necesaria para determinarlo. Hay varios candidatos con propiedades ligeramente distintas, y en este artículo vamos a centrarnos en dos de ellos. El primero se denomina la *casa* y se define como

$$\lceil \overline{\alpha} \rceil = \max_{1 \leq i \leq d} |\alpha_i|,$$

es decir, el mínimo radio de un disco centrado en el origen del plano complejo que contiene a todos los conjugados de α.

El segundo parámetro se denomina la *medida de Mahler* y se define como el producto del módulo de los conjugados que están fuera del disco unidad, es decir,

$$\mathrm{M}(\alpha) = \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

Es fácil ver que si $\alpha \neq 0$, entonces

$$1 \leq \lceil \overline{\alpha} \rceil \leq \mathrm{M}(\alpha) \leq \lceil \overline{\alpha} \rceil^d. \tag{1.1}$$

La primera desigualdad es consecuencia de que el producto del módulo de los conjugados de α coincide con el módulo del término independiente del polinomio mínimo, que es un entero positivo y por lo tanto mayor o igual a 1. De aquí deducimos que el módulo de alguno de estos conjugados debe ser mayor o igual que 1, y así la casa de α también lo es. La segunda desigualdad es consecuencia directa de la definición, mientras que la tercera se sigue de que $\max(1, |\alpha_i|) \leq \lceil \overline{\alpha} \rceil$ para todo i.

Estas desigualdades indican que la casa y la medida de Mahler tendrán propiedades similares, aunque con diferentes matices. El clásico teorema de Northcott (teorema 2.1) afirma que la cantidad de enteros algebraicos con grado y casa acotados superiormente (o, equivalentemente, con grado y medida de Mahler acotados superiormente) es finito. Así, tanto la casa como la medida de Mahler nos dan información sobre la distribución de los conjugados de un entero algebraico y, al mismo tiempo, pueden intervenir en resultados de finitud.

Las desigualdades (1.1) son óptimas. Por ejemplo, si α es una raíz de la unidad, tanto la casa como la medida de Mahler valen 1. De hecho, otro teorema clásico, esta vez de Kronecker (teorema 2.3), muestra que tener casa o medida de Mahler igual a 1 caracteriza a las raíces de la unidad.

Por otra parte, la desigualdad de la derecha es una igualdad, por ejemplo, cuando $\alpha = a^{1/d}$ con a un entero positivo libre de cuadrados. En este caso, todos los conjugados de α se obtienen multiplicando la raíz d-ésima real positiva de a por las distintas raíces d-ésimas de la unidad. Así, todos los conjugados de α tienen el mismo módulo y, por lo tanto,

$$\mathrm{M}(\alpha) = a = \lceil \overline{\alpha} \rceil^d.$$

Más interesante es la pregunta de cuándo se tiene la igualdad $\lceil\overline{\alpha}\rceil = \mathrm{M}(\alpha)$. Aquí intervienen los números de Pisot y de Salem. Un entero algebraico real mayor que 1 se denomina un *número de Pisot* si todos los demás conjugados tienen módulo menor que 1, mientras que es un *número de Salem* si estos conjugados tienen módulo menor o igual que 1 y al menos uno de ellos tiene módulo igual a 1. Estos números son importantes en la teoría de la aproximación diofántica, y resulta que un entero algebraico cumple $\lceil\overline{\alpha}\rceil = \mathrm{M}(\alpha)$ si y sólo si es, o bien una raíz de la unidad, o bien un número de Pisot o de Salem.

Los teoremas de Northcott y de Kronecker implican que, para los enteros algebraicos no nulos que no son raíces de la unidad y tienen grado fijado, tanto la casa como la medida de Mahler están acotadas inferiormente por un número real estrictamente mayor que 1.

En 1933, Derrick Henry Lehmer [11] planteó el problema de encontrar enteros algebraicos con medida de Mahler mayor que 1 pero arbitrariamente cercanos a esta cantidad. A continuación exhibió una lista de enteros algebraicos de grado menor o igual a 10 y medida de Mahler pequeña. De todos ellos, los que tienen la menor medida de Mahler son las raíces del polinomio

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1,$$

cuya medida de Mahler coincide con η, la única raíz real mayor que 1, y que aproximadamente vale $\eta \approx 1{,}17628$.

A pesar de la llegada de los ordenadores y la consiguiente mejora de la potencia de cálculo, nadie ha conseguido batir el récord de Lehmer. Esto ha dado lugar a la llamada *conjetura de Lehmer*, que afirma la existencia de una constante $c > 1$ tal que, para todo entero algebraico α no nulo que no es raíz de la unidad,

$$\mathrm{M}(\alpha) \geq c.$$

La versión optimista de esta conjetura afirma que esta cota inferior es precisamente η. Este entero algebraico es un ejemplo de un número de Salem. Es el más pequeño que se conoce y si esta versión optimista de la conjetura fuera cierta, sería efectivamente el número de Salem más pequeño que existe.

La conjetura de Lehmer es un problema central en teoría de números, y continúa abierta a pesar de los múltiples intentos llevados a cabo para demostrarla. En esta dirección, en 1979 Edward Dobrowolski [4] mostró que existe una constante $c > 0$ tal que, para todo entero algebraico α de grado d no nulo que no es una raíz de la unidad,

$$\log(\mathrm{M}(\alpha)) \geq c \left(\frac{\log\log(d^*)}{\log(d^*)} \right)^3$$

con $d^* = \max(3, d)$. Los cálculos de Dobrowolski muestran que se puede tomar $c = 1/1200$. Posteriormente, el valor de la constante ha podido ser incrementado, pero aparte de este tipo de mejoras numéricas, el resultado de Dobrowolski continúa siendo la mejor cota inferior conocida para el caso general.

Por otra parte, la conjetura de Lehmer ha podido ser verificada en unos cuantos casos particulares. En 1971, Christopher James Smyth [17] demostró que es cierta

para los enteros algebraicos no recíprocos, es decir, que no son conjugados de su inverso: si α es un entero algebraico no nulo y no recíproco, se tiene que

$$\mathrm{M}(\alpha) \geq \theta \tag{1.2}$$

con $\theta \approx 1{,}32471$ la única raíz positiva del polinomio X^3-X-1. Este entero algebraico es un ejemplo de número de Pisot. Dado que los números de Pisot de grado mayor o igual a 3 no son recíprocos, la cota inferior (1.2), junto con el análisis del caso cuadrático, permite recuperar un resultado clásico de Carl Ludwig Siegel que muestra que θ es el número de Pisot más pequeño que existe [16].

En relación a la casa, en 1965 Andrzej Bobola Maria Schinzel y Hans Julius Zassenhaus [14] demostraron que, para todo entero algebraico α no nulo que no es una raíz de la unidad y que tiene s conjugados no reales,

$$|\overline{\alpha}| > 1 + 2^{-2s-4},$$

y a continuación señalaron que no pueden refutar la cota inferior

$$|\overline{\alpha}| > 1 + \frac{c}{d}, \tag{1.3}$$

donde d es el grado de este entero algebraico y c es una constante positiva que no depende de α. Este enunciado, es decir, la existencia de una constante $c > 0$ tal que la desigualdad (1.3) es cierta para todo α no nulo que no es una raíz de la unidad, se conoce hoy en día como la *conjetura de Schinzel–Zassenhaus*.

Una versión optimista de esta conjetura fue propuesta en 1985 por David William Boyd [1], y afirma que la constante podría tomarse como

$$c = \frac{3}{2}\log(\theta) \approx 0{,}42179,$$

donde θ es la única raíz real de la ecuación $X^3 - X - 1$, es decir, el número de Pisot que ya había aparecido en el resultado de Smyth. Se puede ver que esta constante sería óptima estudiando las raíces de los polinomios $X^{3k} + X^{2k} - 1$ para $k \geq 1$.

En este punto se pueden hacer dos observaciones. En primer lugar, la conjetura de Lehmer predice una cota inferior uniforme para la medida de Mahler, mientras que la conjetura de Schinzel–Zassenhaus predice una cota inferior para la que se aproxima a 1 conforme el grado tiende a infinito. En segundo lugar, por las desigualdades (1.1), la conjetura de Lehmer implica la de Schinzel–Zassenhaus. Más generalmente, estas desigualdades permiten derivar cotas inferiores para la casa a partir de cotas inferiores para la medida de Mahler.

Por ejemplo, el resultado de Dobrowolski implica que existe $c > 0$ tal que, para todo entero algebraico α no nulo que no es una raíz de la unidad,

$$|\overline{\alpha}| > 1 + \frac{c}{d}\left(\frac{\log\log(d^*)}{\log(d^*)}\right)^3$$

con $d^* = \max(3, d)$, mientras que el resultado de Smyth implica que, si α no es recíproco,

$$|\overline{\alpha}| > 1 + \frac{\theta}{d}.$$

La conjetura de Schinzel–Zassenhaus ha permanecido abierta por más de 50 años, pero hoy en día es un teorema, consecuencia directa de un resultado presentado el 28 de diciembre de 2019 por Vesselin Dimitrov [3].

Teorema 1.1 (Dimitrov). *Si α es un entero algebraico no nulo de grado d que no es raíz de la unidad, entonces*

$$|\overline{\alpha}| \geq 2^{1/(4d)}.$$

En particular, $|\overline{\alpha}| > 1 + c/d$ *con* $c = \log(2)/4 \approx 0{,}17328$.

El objetivo principal de nuestro artículo es presentar al lector la demostración de este teorema, que combina resultados clásicos de análisis complejo y de teoría de números de una forma original y totalmente inesperada.

2. Enteros algebraicos

En esta sección veremos algunas de las propiedades básicas de los enteros algebraicos. En particular, daremos demostraciones elementales de los teoremas de Northcott y de Kronecker, estudiaremos cómo cambian la medida de Mahler y la casa cuando tomamos la potencia de un entero algebraico, y demostraremos un caso particular de las congruencias de Schönemann.

Dado $\alpha \in \overline{\mathbb{Z}}$, denotamos por $\mathrm{gr}(\alpha)$ su grado, es decir, el grado de su polinomio mínimo. Esta cantidad coincide con el número de conjugados de este entero algebraico, y también con el grado de la extensión de cuerpos $\mathbb{Q}(\alpha)/\mathbb{Q}$.

El teorema de Northcott está en la base de muchos teoremas de finitud en teoría de números.

Teorema 2.1 (Northcott). *Sea $e \geq 1$ un entero y $c \geq 0$ un número real. Entonces*

1. *el conjunto de los enteros algebraicos α con $\mathrm{gr}(\alpha) \leq e$ y $|\overline{\alpha}| \leq c$ es finito;*
2. *el conjunto de los enteros algebraicos α con $\mathrm{gr}(\alpha) \leq e$ y $\mathrm{M}(\alpha) \leq c$ es finito.*

Demostración. En vista de las desigualdades en (1.1), ambas afirmaciones son equivalentes, por lo que sólo será necesario demostrar la primera.

Sea α un entero algebraico de grado $d \leq e$ y

$$P = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

su polinomio mínimo. Cada coeficiente a_i es un número entero y, salvo por el signo, coincide con el polinomio simétrico elemental de grado i evaluado en los conjugados de α. Luego

$$|a_i| \leq \binom{d}{i} |\overline{\alpha}|^{d-i} \leq \binom{d}{i} c^{d-i},$$

lo cual sólo da un número finito de posibilidades para P, y por lo tanto para α. □

Para demostrar las siguientes propiedades de la casa y de la medida de Mahler, será conveniente interpretar el conjunto de conjugados de un entero algebraico en términos de la acción sobre este entero algebraico del *grupo de Galois absoluto*

$$G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

La teoría de Galois nos dice que, dado $\alpha \in \overline{\mathbb{Z}}$, su conjunto de conjugados coincide con la órbita de α respecto a la acción de este grupo, es decir,

$$G \cdot \alpha = \{\alpha_1, \ldots, \alpha_d\}.$$

Lema 2.2. *Sea $\alpha \in \overline{\mathbb{Z}}$ y $k \geq 1$ un entero. Entonces*

1. $\overline{|\alpha^k|} = \overline{|\alpha|}^k$,
2. $\mathrm{M}(\alpha^k) = \mathrm{M}(\alpha)^{k/e}$ *con* $e = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^k)]$.

Demostración. La aplicación de potencias k-ésimas $\gamma \mapsto \gamma^k$ es compatible con la acción de G, ya que este último es un grupo de automorfismos de cuerpos: para todo $\gamma \in \overline{\mathbb{Z}}$ y $\sigma \in G$ se tiene que $\sigma(\gamma)^k = \sigma(\gamma^k)$. Esto implica que su restricción al conjunto de conjugados de α da una aplicación

$$G \cdot \alpha \longmapsto G \cdot \alpha^k$$

que es exhaustiva y cuyas fibras tienen todas el mismo cardinal, igual a la cantidad

$$\frac{\#(G \cdot \alpha)}{\#(G \cdot \alpha^k)} = \frac{[\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\alpha^k) : \mathbb{Q}]} = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^k)] = e,$$

por la multiplicatividad de los grados de las extensiones de cuerpos. Luego

$$\overline{|\alpha^k|} = \max_{\beta \in G \cdot \alpha^k} |\beta| = \max_{\gamma \in G \cdot \alpha} |\gamma^k| = \overline{|\alpha|}^k$$

y, similarmente,

$$\mathrm{M}(\alpha^k) = \prod_{\beta \in G \cdot \alpha^k} \max(1, |\beta|) = \prod_{\gamma \in G \cdot \alpha} \max(1, |\gamma^k|)^{1/e} = \mathrm{M}(\alpha)^{k/e}. \qquad \square$$

El teorema de Kronecker caracteriza los enteros algebraicos no nulos con casa o medida de Mahler mínima.

Teorema 2.3. *Sea α un entero algebraico. Las afirmaciones siguientes son equivalentes:*

1. $\overline{|\alpha|} = 1$,
2. $\mathrm{M}(\alpha) = 1$,
3. *α es una raíz de la unidad.*

Demostración. En vista de (1.1), las condiciones $\overline{|\alpha|} = 1$ y $\mathrm{M}(\alpha) = 1$ son equivalentes, y claramente se satisfacen si α es una raíz de la unidad.

Recíprocamente, sea α un entero algebraico de grado d con $\overline{|\alpha|} = 1$. Para todo $n \geq 1$, el entero algebraico α^n es un elemento del cuerpo $\mathbb{Q}(\alpha)$, con lo cual tiene grado $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. Por otra parte, el lema 2.2, apartado 1, implica que α^n tiene casa igual a 1. El teorema 2.1 implica que estos enteros algebraicos forman un conjunto finito, con lo cual podemos encontrar $1 \leq n < m$ tales que $\alpha^n = \alpha^m$. Como α es no nulo, se tiene que $\alpha^{m-n} = 1$ y así α resulta ser una raíz de la unidad. $\square$

La teoría de Galois muestra que todo número algebraico que es *G-invariante*, es decir, invariante respecto a la acción de G, es necesariamente racional. Por otro lado, $\mathbb{Z}$ es íntegramente cerrado en $\mathbb{Q}$, es decir, $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Combinando estas dos propiedades, se deduce que todo entero algebraico G-invariante es un entero ordinario. Usaremos repetidamente este principio para ver que, por ejemplo, las sumas en el lema 2.4 y los coeficientes de los polinomios en el lema 2.5 son enteros.

Lema 2.4. *Sea $S \subset \overline{\mathbb{Z}}$ un subconjunto finito y G-invariante. Se cumple la siguiente congruencia de números enteros:*

$$\sum_{\beta \in S} \beta^4 \equiv \sum_{\beta \in S} \beta^2 \pmod 4.$$

Demostración. Dado un entero $k \geq 1$ consideramos la suma de potencias k-ésimas

$$p_k = \sum_{\beta \in S} \beta^k \in \mathbb{Z},$$

mientras que, dado otro entero $\ell \geq 0$, consideramos el ℓ-ésimo polinomio simétrico elemental

$$e_\ell = \sum_{\#I = \ell} \prod_{\beta \in I} \beta \in \mathbb{Z},$$

siendo la suma sobre todos los subconjuntos $I \subset S$ de cardinal ℓ.

Entre las identidades de Newton se encuentran

$$p_2 = e_1^2 - 2e_2, \quad p_4 = e_1^4 + 2e_2^2 + 4(e_1 e_3 - e_1^2 e_2 - e_4).$$

Estas igualdades, junto con las congruencias $a^2 \equiv a^4 \pmod 4$ y $-a \equiv a^2 \pmod 2$ para todo $a \in \mathbb{Z}$, implican que $p_4 \equiv p_2 \pmod 4$, como queríamos. □

El lema 2.4 es un caso particular de un resultado más general: para cualquier primo p y entero $r \geq 1$ se tiene la congruencia

$$\sum_{\beta \in S} \beta^{p^r} \equiv \sum_{\beta \in S} \beta^{p^{r-1}} \pmod{p^r}.$$

Esto fue demostrado para $r = 1$ en 1839 por Theodor Schönemann [15], y en 1921 para todo r por Walther Jänichen [10]. Más recientemente, en 1986 Smyth [18] ha dado una demostración combinatoria, y en 2008 Pierre Deligne [2] ha dado otra como una aplicación de los vectores de Witt de $\overline{\mathbb{Z}}$.

Para cada entero $k \geq 1$ consideramos el polinomio mónico

$$P_k = \prod_{i=1}^{d} (X - \alpha_i^k) \in \mathbb{Z}[X]. \tag{2.1}$$

Como mostraremos a continuación, el lema 2.4 implica que P_2 y P_4 son congruentes módulo 4. Las versiones más generales de Schönemann y de Jänichen que mencionamos anteriormente implican congruencias similares entre los otros polinomios de la familia (2.1).

Lema 2.5. $P_4 \equiv P_2 \pmod{4\,\mathbb{Z}[X]}$.

Demostración. Si escribimos $P_k = X^d + \sum_{j=0}^{d-1} a_{k,j} X^j$ con $a_{k,j} \in \mathbb{Z}$, la factorización en (2.1) implica que $a_{k,j} = (-1)^{d-j} \sum_{\beta \in S_j} \beta^k$ para el subconjunto finito G-invariante de $\overline{\mathbb{Z}}$ definido como

$$S_j = \left\{ \prod_{i \in I} \alpha_i \;\middle|\; I \subset \{1, \ldots, d\},\ \#I = d - j \right\}.$$

El lema 2.4 implica entonces que $a_{4,k} \equiv a_{2,k} \pmod 4$ para todo k, o equivalentemente que $P_4 \equiv P_2 \pmod{4\,\mathbb{Z}[X]}$. □

3. La constante de Chebyshov

Ahora cambiaremos drásticamente de registro, ya que pasaremos a las componentes analíticas de la demostración del teorema de Dimitrov. El rol principal lo ocupa la constante de Chebyshov, una medida del tamaño de un subconjunto compacto del plano complejo que se usa en la teoría de la aproximación.

Sea $K \subset \mathbb{C}$ un subconjunto compacto. Dado $P \in \mathbb{C}[X]$ consideramos la norma del supremo sobre este subconjunto, es decir,

$$\|P\|_K = \sup_{z \in K} |P(z)|,$$

y para cada entero $n \geq 0$ definimos

$$\mu_n(K) = \inf_{P \in \mathcal{P}_n} \|P\|_K, \tag{3.1}$$

donde $\mathcal{P}_n$ designa el conjunto de polinomios mónicos de $\mathbb{C}[X]$ de grado n. En otros términos, $\mu_n(K)$ es el error de la mejor aproximación, respecto de la norma del supremo sobre K, del monomio X^n por polinomios de grado inferior.

Lema 3.1. *Supongamos que K contiene infinitos puntos y sea $n \geq 0$ un entero. Se cumplen las siguientes propiedades:*

1. $\mu_n(K) > 0$,
2. *existe un único polinomio $T_n \in \mathcal{P}_n$ con $\|T_n(z)\|_K = \mu_n(K)$,*
3. $|T_n(z)| = \mu_n(K)$ *en al menos $n+1$ puntos $z \in K$.*

Demostración. Como K es infinito, la asignación $P \mapsto \|P\|_K$ define una norma en $\mathbb{C}[X]_{\leq n}$. Como $\mathcal{P}_n$ es un subconjunto cerrado, no vacío y disjunto de cero de este espacio vectorial de dimensión finita, el ínfimo en (3.1) se alcanza y es estrictamente positivo. Esto demuestra la propiedad 1 y la existencia de algún polinomio T_n en el apartado 2.

Sea $P \in \mathcal{P}_n$ tal que $\|P\|_K = \mu_n(K)$ y consideremos el subconjunto

$$E = \{z \in K \mid |P(z)| = \mu_n(K)\}.$$

Si $\#E \leq n$ entonces existe un polinomio R de grado menor que n tal que $R(z) = P(z)$ para todo $z \in E$. Como $P - R$ se anula en E y esta diferencia de polinomios es una función continua, podemos encontrar un entorno abierto U de E tal que $\|P-R\|_{\overline{U}} < \mu_n(K)$, donde $\overline{U}$ denota la adherencia de este abierto. Luego, para todo $0 < \varepsilon \leq 1$, se tiene que

$$\|P-\varepsilon R\|_{K\cap\overline{U}} \leq (1-\varepsilon)\|P\|_K+\varepsilon\|P-R\|_{\overline{U}} < (1-\varepsilon)\mu_n(K)+\varepsilon\mu_n(K) \leq \mu_n(K). \quad (3.2)$$

Por otra parte, $\|P\|_{K\setminus U} < \mu_n(K)$, con lo cual para todo número real $\varepsilon > 0$ suficientemente pequeño también se tiene que

$$\|P - \varepsilon R\|_{K\setminus U} < \mu_n(K). \quad (3.3)$$

Juntando (3.2) y (3.3) obtenemos que $\|P - \varepsilon R\|_K < \mu_n(K)$, lo que contradice la definición de $\mu_n(K)$ y demuestra la propiedad 3 para todo polinomio que realice el ínfimo.

Veamos ahora la unicidad en el apartado 2: si $Q \in \mathcal{P}_n$ es otro polinomio que cumple $\|Q\|_K = \mu_n(K)$, entonces

$$\mu_n(K) \leq \left\| \frac{P+Q}{2} \right\|_K \leq \frac{\|P\|_K + \|Q\|_K}{2} = \mu_n(K),$$

con lo cual $\|(P+Q)/2\|_K = \mu_n(K)$. Por el apartado 3, existen al menos $n+1$ puntos $z \in K$ tales que $|(P(z)+Q(z))/2| = \mu_n(K)$. Como en estos puntos se tiene también que $|P(z)|, |Q(z)| \leq \mu_n(K)$, necesariamente $P(z) = Q(z) = \mu_n(K)$. Luego P y Q son polinomios mónicos de grado n que coinciden en al menos $n+1$ puntos, y por lo tanto son iguales, concluyendo la demostración del apartado 2. □

Cuando K es infinito, el polinomio T_n en el lema 3.1, apartado 2, se denomina el *polinomio de Chebyshov* de K de grado n. Para todo $m, n \geq 0$ se tiene entonces que

$$\mu_{n+m}(K) = \inf_{P\in\mathcal{P}_{n+m}} \|P\|_K \leq \|T_nT_m\|_K \leq \|T_n\|_K \, \|T_m\|_K = \mu_n(K)\mu_m(K).$$

Esto implica que la sucesión $(\log(\mu_n(K)))_{n\geq 0}$ es subaditiva, y el lema de subaditividad de Fekete [7] nos dice que la sucesión $(\mu_n(K)^{1/n})_{n\geq 0}$ converge y que su límite coincide con el ínfimo. Por otra parte, si $\#K = m < +\infty$ entonces $\mu_n(K) = 0$ para todo $n \geq m$, y la sucesión $(\mu_n(K)^{1/n})_{n\geq 0}$ también converge en este caso.

La *constante de Chebyshov* de K se define como

$$\mathrm{cheb}(K) = \lim_{n\to\infty} \mu_n(K)^{1/n} = \inf_n \mu_n(K)^{1/n}.$$

Esta constante es monótona con respecto a la inclusión de conjuntos: si $K' \subset \mathbb{C}$ es otro subconjunto compacto que contiene a K, entonces

$$\mathrm{cheb}(K) \leq \mathrm{cheb}(K').$$

La constante de Chebyshov se comporta bien con respecto a aplicaciones lineales: para $\lambda, \mu \in \mathbb{C}$ se tiene que

$$\operatorname{cheb}(\lambda K + \mu) = |\lambda| \operatorname{cheb}(K). \tag{3.4}$$

La siguiente proposición nos permite calcularla también para la imagen inversa por una aplicación polinomial.

Proposición 3.2. *Sea $K \subset \mathbb{C}$ un subconjunto compacto y sea $Q \in \mathbb{C}[X]$ un polinomio mónico de grado $m \geq 1$. El subconjunto $Q^{-1}(K) \subset \mathbb{C}$ es compacto y se cumple la igualdad*

$$\operatorname{cheb}(Q^{-1}(K)) = \operatorname{cheb}(K)^{1/m}.$$

Demostración. La imagen inversa $Q^{-1}(K)$ es un cerrado acotado de $\mathbb{C}$, y por lo tanto un subconjunto compacto.

Sea $n \geq 1$ un entero. Para $P \in \mathcal{P}_n$ consideramos su *imagen inversa* respecto de Q, definida como el polinomio

$$Q^*P = P \circ Q \in \mathcal{P}_{mn}.$$

La aplicación $Q\colon \mathbb{C} \to \mathbb{C}$ es exhaustiva y por lo tanto $\|Q^*P\|_{Q^{-1}(K)} = \|P\|_K$. Tomando $P = T_n$ el polinomio de Chebyshov de K de grado n, se deduce que

$$\mu_{mn}(Q^{-1}(K)) \leq \|Q^*T_n\|_{Q^{-1}(K)} = \|T_n\|_K = \mu_n(K). \tag{3.5}$$

Para demostrar una desigualdad en sentido contrario, dado $P \in \mathcal{P}_n$ consideramos la factorización $P = \prod_{i=1}^n (X - \alpha_i)$ y definimos su *norma* con respecto a Q como

$$\mathrm{N}_Q(P) = \prod_{i=1}^n (X - Q(\alpha_i)) \in \mathcal{P}_n.$$

Dado $z \in \mathbb{C}$, se tiene que

$$\begin{aligned}\mathrm{N}_Q(P)(z) = \prod_{i=1}^n (z - Q(\alpha_i)) &= \pm \prod_{i=1}^n \prod_{w \in Q^{-1}(z)} (\alpha_i - w) \\ &= \pm \prod_{w \in Q^{-1}(z)} \prod_{i=1}^n (\alpha_i - w) = \pm \prod_{w \in Q^{-1}(z)} P(w),\end{aligned}$$

donde la segunda igualdad se demuestra considerando $z - Q(\alpha_i)$ como un polinomio en α_i, cuyas raíces son los puntos $w \in Q^{-1}(z)$ contados con multiplicidad. Deducimos que $\|\mathrm{N}_Q(P)\|_K \leq \|P\|_{Q^{-1}(K)}^m$, y tomando $P = U_n$ el polinomio de Chebyshov de $Q^{-1}(K)$ de grado n, deducimos que

$$\mu_n(Q^{-1}(K)) = \|U_n\|_{Q^{-1}(K)} \geq \|\mathrm{N}_Q(U_n)\|_K^{1/m} \geq \mu_n(K)^{1/m}. \tag{3.6}$$

Juntando las desigualdades (3.5) y (3.6) obtenemos

$$\mu_{mn}(Q^{-1}(K))^{1/(nm)} \leq (\mu_n(K)^{1/m})^{1/n} \leq \mu_n(Q^{-1}(K))^{1/n},$$

y haciendo tender $n \to +\infty$ deducimos que $\operatorname{cheb}(Q^{-1}(K)) = \operatorname{cheb}(K)^{1/m}$. □

Vamos a calcular algunos ejemplos de constantes de Chebyshov.

Ejemplo 3.3. Sea $K = D(0,1)$ el disco de radio 1 centrado en el origen. Dado un polinomio $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$, el principio del máximo nos asegura que el máximo de P en K se alcanza en la circunferencia unidad. Por lo tanto

$$\|P\|_K \geq \int_0^1 |P(e^{2\pi \mathrm{i}\theta})|^2 \, d\theta = 1 + |a_0|^2 + \cdots + |a_{n-1}|^2 \geq 1,$$

lo cual implica que $\mu_n(K) \geq 1$. Por otro lado $\|X^n\|_K = 1$, lo que muestra que $\mathrm{cheb}(K) = 1$ y que X^n es el polinomio de Chebyshov de K de grado n. Por la propiedad (3.4), la constante de Chebyshov de cualquier disco de radio $\rho \geq 0$ es igual a ρ.

Ejemplo 3.4. Consideramos ahora el segmento cerrado $K = [-2,2]$. Para $n \geq 1$, sea C_n el polinomio determinado por $C_n(2\cos\theta) = 2\cos(n\theta)$. Claramente $C_1 = X$ y $C_2 = X^2 - 1$, y se puede ver que C_n es un polinomio mónico de grado n con coeficientes reales mediante inducción gracias a la fórmula trigonométrica

$$\cos((n+1)\theta) + \cos((n-1)\theta) = 2\cos(n\theta)\cos(\theta).$$

Se tiene que $\|C_n\|_K = 2$ y $C_n(2\cos(k\pi/n)) = (-1)^k 2$, y por lo tanto $\mu_n(K) \leq 2$.

Veamos que efectivamente $\mu_n(K) = 2$. Supongamos que no es así, con lo cual $\mu_n(K) < 2$, y sea T_n el polinomio de Chebyshov de K de grado n. Por la unicidad de este polinomio y la simetría del segmento con respecto a la conjugación compleja, sabemos que T_n tiene coeficientes reales. Entonces el polinomio $Q = T_n - C_n$ toma valores no nulos en los puntos $2\cos(k\pi/n)$, $k = 0, \ldots, n$, con signos alternados, y por lo tanto tiene al menos n ceros. Como el grado de Q es menor que $n-1$ deducimos que $Q = 0$, contradiciendo la condición $\mu_n(K) < 2$. En consecuencia $\mu_n(K) = 2$ y

$$\mathrm{cheb}(K) = \lim_{n \to +\infty} 2^{1/n} = 1.$$

Usando de nuevo la propiedad (3.4), deducimos que la constante de Chebyshov de un segmento arbitrario de longitud λ es $\lambda/4$.

Ejemplo 3.5. Para un entero $m \geq 1$ consideremos el *erizo regular de m púas* definido por

$$H_m = \bigcup_{k=0}^{m-1} [0,1]\, e^{2k\pi \mathrm{i}/m}.$$

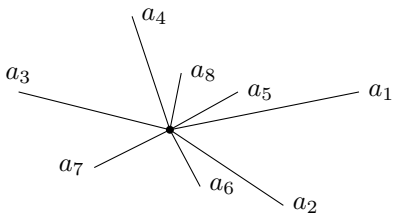
Este conjunto es la preimagen del intervalo $[0,1]$ por la aplicación $z \mapsto z^m$. Por la proposición 3.2 y el ejemplo 3.4 se tiene que

$$\mathrm{cheb}(H_m) = \mathrm{cheb}([0,1])^{1/m} = 4^{-1/m}.$$

Por la propiedad (3.4), la constante de Chebyshov de un erizo regular de m púas de longitud λ es $4^{-1/m}\lambda$.

Más generalmente, para una sucesión $a_1, \ldots, a_m$ de puntos de $\mathbb{C}$, consideramos su *erizo* asociado, definido como el conjunto compacto

$$H(a_1, \ldots, a_m) = \bigcup_{k=1}^{m} [0,1]\, a_k.$$



Un erizo de 8 púas.

Un teorema de Vladimir Nikolaevich Dubinin de 1984 muestra que la constante de Chebyshov de un erizo puede acotarse superiormente por la de un erizo regular de m púas.

Teorema 3.6 (Dubinin). *Sea $a_1, \ldots, a_m$ una sucesión de puntos de $\mathbb{C}$. Entonces*

$$\operatorname{cheb}(H(a_1, \ldots, a_m)) \leq 4^{-1/m} \sup_{1 \leq i \leq m} |a_i|.$$

Este resultado es el único ingrediente importante del teorema de Dimitrov que no demostraremos en este artículo, pues nos llevaría muy lejos en el estudio de la teoría del potencial en el plano complejo y, en particular, en la relación entre la constante de Chebyshov y la capacidad logarítmica. El lector interesado puede consultar el artículo original de Dubinin [5], el libro del mismo autor [6], o el artículo de Kersti Haliste [9] que presenta varias simplificaciones del argumento original.

4. El teorema de racionalidad de Pólya

El teorema de Pólya (teorema 4.6) da un criterio para saber cuándo una serie de potencias con coeficientes enteros se puede escribir como un cociente de polinomios. La demostración original de George Pólya [12] data de 1928 y utiliza el criterio de racionalidad de Kronecker basado en la anulación de ciertos determinantes de Hankel. La demostración que presentamos en este artículo se debe a Raphael Mitchel Robinson (1969) [13] y está basada en un teorema de Michael Fekete y Gábor Szegő (1955) [8] que explicaremos en primer lugar.

Sea $K \subset \mathbb{C}$ un subconjunto compacto. Dado un número real $\rho > \operatorname{cheb}(K)$, para n suficientemente grande se tiene que

$$\mu_n(K) < \rho^n,$$

y por lo tanto existe un polinomio mónico P de grado n tal que $\|P\|_K < \rho^n$. Si el conjunto K es simétrico con respecto a la conjugación compleja, entonces podemos elegir P con coeficientes reales. En efecto, para $z \in K$ se tiene que $|\overline{P}(z)| = |P(\overline{z})| \leq \|P\|_K < \rho^n$. Por lo tanto $\mathrm{Re}(P) = (P + \overline{P})/2$ tiene coeficientes reales y también cumple que $\|\mathrm{Re}(P)\|_K < \rho^n$.

El teorema de Fekete y Szegő que mencionamos anteriormente dice que si K es simétrico con $\mathrm{cheb}(K) < 1$ y tomamos $\rho = 1$, entonces podemos elegir este polinomio P con coeficientes enteros.

Teorema 4.1 (Fekete–Szegő). *Sea $K \subset \mathbb{C}$ un subconjunto compacto, simétrico con respecto a la conjugación compleja y tal que* $\mathrm{cheb}(K) < 1$. *Para todo entero n suficientemente grande, existe un polinomio mónico $P \in \mathbb{Z}[X]$ de grado n tal que $\|P\|_K < 1$.*

La demostración de este resultado la daremos después de establecer un lema técnico.

Lema 4.2. *Sea $K \subset \mathbb{C}$ un subconjunto compacto no vacío, simétrico con respecto a la conjugación compleja y con* $\mathrm{cheb}(K) < 1$. *Sea $\varepsilon > 0$ un número real. Entonces existe un entero $m \geq 1$ y, para todo entero $n \geq m$, un par de polinomios (P_n, Q_n) que cumplen las siguientes condiciones:*

1. *El polinomio P_n es mónico, tiene grado n y coeficientes enteros;*
2. *el grado de Q_n es menor que m;*
3. *los coeficientes de Q_n pertenecen al intervalo semiabierto $[0, 1) \subset \mathbb{R}$;*
4. *$\|P_n - Q_n\|_K \leq \varepsilon$.*

Demostración. Sea ρ un número real que cumpla $\mathrm{cheb}(K) < \rho < 1$. Elegimos un entero $m \geq 1$ con $\rho^m/(1-\rho) \leq \varepsilon$ y tal que, para todo $n \geq m$, existe un polinomio mónico $R_n \in \mathbb{R}[X]$ de grado n con coeficientes reales que cumple $\|R_n\|_K < \rho^n$, que existe, tal y como se ha explicado antes de enunciar el teorema 4.1.

Como los polinomios R_n son mónicos, para cada $n \geq m$ existe una única sucesión de números $a_{n-1}, \ldots, a_m$ en el intervalo $[0, 1)$ tal que todos los coeficientes de grado $\geq m$ del polinomio

$$S_n = R_n - a_{n-1}R_{n-1} - \cdots - a_m R_m$$

son enteros. Por ejemplo, a_{n-1} es la parte fraccionaria del coeficiente de X^{n-1} en R_n, y se continua inductivamente para calcular los otros elementos de la sucesión.

Por lo tanto existe un polinomio Q_n de grado $< m$, con coeficientes en el intervalo $[0, 1)$, tal que $P_n = S_n + Q_n$ tiene coeficientes enteros. Así las condiciones 1, 2 y 3 se cumplen por construcción. Veamos que también se cumple la condición 4. Para ello, usando la definición de S_n, la condición de acotación de los polinomios R_k y la fórmula de la suma parcial de una serie geométrica, calculamos

$$\|P_n - Q_n\|_K = \|S_n\|_K \leq \sum_{k=m}^{n} \|R_k\|_K \leq \sum_{k=m}^{n} \rho^k \leq \frac{\rho^m}{1-\rho} \leq \varepsilon,$$

con lo que concluye la demostración del lema. □

Estamos ahora en condiciones de demostrar el teorema de Fekete–Szegő.

Demostración del teorema 4.1. Elegimos un entero $m \geq 1$ y polinomios P_n, Q_n para todo $n \geq m$ que cumplan las condiciones del lema 4.2 para $\varepsilon = 1/4$. Los polinomios Q_n pertenecen a un subconjunto acotado del espacio vectorial de dimensión finita $\mathbb{R}[X]_{\leq m-1}$. Se deduce que podemos encontrar dos enteros $n_1 > n_2 > m$ tales que $\|Q_{n_1} - Q_{n_2}\|_K \leq 1/4$. En consecuencia, $R = P_{n_1} - P_{n_2}$ es un polinomio mónico de grado n_1 con coeficientes enteros, y cumple que

$$\|R\|_K \leq \|P_{n_1} - Q_{n_1}\|_K + \|Q_{n_1} - Q_{n_2}\|_K + \|Q_{n_2} - P_{n_2}\|_K \leq \frac{3}{4}.$$

Como K es compacto, en particular acotado, podemos encontrar un número real $c \geq 1$ tal que $|z| \leq c$ para todo $z \in K$. Elegimos también un entero $k \geq 1$ tal que $(3/4)^k c^{n_1-1} < 1$. Dado $n \geq kn_1$, escribimos $n = qn_1 + r$ con $0 \leq r < n_1$ y $q \geq k$. El polinomio $P = X^r R^q$ es mónico, tiene grado n y coeficientes enteros. Además

$$\|P\|_K \leq (3/4)^q c^r \leq (3/4)^k c^{n_1-1} < 1,$$

demostrando el teorema. □

Observación 4.3. En el teorema 4.1 se puede evitar la condición de que K sea simétrico con respecto a la conjugación compleja a costa de trabajar con coeficientes en los enteros de Gauss $\mathbb{Z}[i]$. No vamos a necesitar esta extensión en lo que sigue.

El teorema de Fekete–Szegő tiene la siguiente consecuencia interesante.

Corolario 4.4. *Sea $K \subset \mathbb{C}$ un subconjunto compacto con* $\operatorname{cheb}(K) < 1$. *El conjunto de enteros algebraicos cuyos conjugados están todos contenidos en K es finito.*

Demostración. Si todos los conjugados de un entero algebraico pertenecen a K entonces también pertenecen a $K \cap \overline{K}$, y, por la monotonía de la constante de Chebyshov,

$$\operatorname{cheb}(K \cap \overline{K}) \leq \operatorname{cheb}(K) < 1.$$

Luego podemos suponer que K es simétrico con respecto a la conjugación compleja.

Por el teorema 4.1, existe un polinomio mónico $P \in \mathbb{Z}[X]$ tal que $\|P\|_K < 1$. Si α es un entero algebraico con todos sus conjugados contenidos en K, entonces $P(\alpha)$ es un entero algebraico con todos sus conjugados de modulo < 1, o, equivalentemente, $\left|\overline{P(\alpha)}\right| < 1$. La primera desigualdad en (1.1) implica entonces que $P(\alpha) = 0$, y por lo tanto sólo hay un número finito de posibles elecciones para α. □

Observación 4.5. Esta proposición tiene un recíproco parcial también debido a Fekete y a Szegő, que afirma que si K es simétrico respecto a la conjugación compleja y $\operatorname{cheb}(K) \geq 1$, entonces para todo abierto U que contiene a K existe un conjunto infinito de enteros algebraicos cuyos conjugados pertenecen todos a U.

El teorema de Pólya que es clave en la demostración del teorema de Dimitrov es el siguiente. Denotamos por $\mathbb{P}^1(\mathbb{C})$ la esfera de Riemann y por ∞ su *punto del infinito*.

Teorema 4.6 (Pólya, 1928 [12]). *Sea $K \subset \mathbb{C}$ un subconjunto compacto, simétrico con respecto a la conjugación compleja y con* $\mathrm{cheb}(K) < 1$. *Sea f una función holomorfa en $\mathbb{P}^1(\mathbb{C}) \smallsetminus K$ cuyo desarrollo de Taylor en el infinito*

$$f = a_0 + \frac{a_1}{z} + \frac{a_2}{z^2} + \cdots$$

tiene todos sus coeficientes enteros. Entonces f es un cociente de polinomios.

Demostración. Por el teorema 4.1, existe un polinomio mónico $P \in \mathbb{Z}[X]$ tal que $\|P\|_K < 1$. Sea c un número real con $\|P\|_K < c < 1$ y que sea distinto de los valores de $|P|$ en las raíces de la derivada P' de P. El conjunto $C = |P|^{-1}(c)$ es una curva real analítica y acotada de $\mathbb{C}$. La condición de que c es distinto de los posibles valores de $|P|$ en las raíces de P' implica que C es lisa y, por lo tanto, una unión disjunta de curvas de Jordan $C_1, \ldots, C_n$. Sea Ω_i la componente conexa acotada de $\mathbb{C} \smallsetminus C_i$. Por el principio del máximo, la condición $|P| < c$ se cumple en Ω_i. Por lo tanto, Ω_i no contiene ninguna de las curvas C_j, con $j \neq i$. Se deduce que las componentes conexas de $\mathbb{C} \smallsetminus C$ son exactamente $\Omega_1, \ldots, \Omega_n$ y una componente conexa no acotada Ω. Como $\lim_{z\to\infty} |P(z)| = +\infty$, el teorema de Bolzano implica que $|P| > c$ en Ω, y por lo tanto $K \subset \Omega_1 \cup \cdots \cup \Omega_n$ y el borde de Ω coincide con la curva $C = C_1 \cup \cdots \cup C_n$.

Sea d el grado de P y elijamos un entero $m \geq 1$ suficientemente grande como para que

$$c^m \, \|f\|_C \, \sup(1, \|z\|_C)^{d-1} \, \frac{\mathrm{long}(C)}{2\pi} < 1, \tag{4.1}$$

donde $\mathrm{long}(C)$ denota la longitud de la curva C. El desarrollo en el infinito de la función $P^m f$ es de la forma

$$Q(z) + \frac{b_1}{z} + \frac{b_2}{z^2} + \cdots$$

con $Q \in \mathbb{Z}[X]$ y $b_i \in \mathbb{Z}$ para todo i. Supongamos que los b_i no son todos nulos. Sea $k > 0$ el menor entero tal que $b_k \neq 0$. Escribimos $k = qd + r$ con $q \geq 0$ y $1 \leq r \leq d$. El principio del desarrollo de Taylor de $P^{m+q} f$ en el infinito es de la forma

$$P^q(z)\Big(Q(z) + \frac{b_k}{z^k} + \cdots\Big) = P^q(z)Q(z) + \frac{b_k}{z^r} + \cdots .$$

Luego $-b_k$ coincide con el residuo en ∞ de la función $z^{r-1}P(z)^{m+q}f(z)$. Como esta función es holomorfa en Ω, del teorema de los residuos se deduce que

$$-b_k = \mathrm{Res}(z^{r-1}P(z)^{m+q}f(z), \infty) = \frac{1}{2\pi\mathrm{i}} \int_C z^{r-1}P(z)^{m+q}f(z)\,dz$$

con C la curva orientada como borde de Ω. Esta igualdad, junto con la condición (4.1), implica que $|b_k| < 1$. Como b_k es un entero, obtenemos $b_k = 0$. Esto contradice la hipótesis hecha y, en consecuencia, todos los coeficientes b_i son nulos y $f = Q/P^m$, terminando la demostración del teorema. □

5. El teorema de Dimitrov

Finalmente, en esta sección vamos a poner en juego todos los elementos desarrollados previamente, con el fin de explicar la demostración de Dimitrov de la conjetura de Schinzel–Zassenhaus (teorema 1.1).

Sea α un entero algebraico no nulo de grado d que no es una raíz de la unidad. Vamos a demostrar la cota inferior

$$|\overline{\alpha}| \geq 2^{1/(4d)} \tag{5.1}$$

por inducción en d. En el caso básico en que $d = 1$ tenemos que α es un entero $\neq 0, \pm 1$, con lo cual $|\overline{\alpha}| = |\alpha| \geq 2$ y la desigualdad (5.1) es válida.

Supondremos entonces que $d > 1$ y que la desigualdad es cierta para los grados inferiores. Aquí se nos presenta una dicotomía: el entero algebraico α es raíz de $X^2 - \alpha^2$, y por lo tanto el cuerpo $\mathbb{Q}(\alpha)$ es una extensión de $\mathbb{Q}(\alpha^2)$ de grado 2 o de grado 1, dependiendo de si este polinomio es irreducible sobre $\mathbb{Q}(\alpha^2)$ o no. En el primer caso $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 2$, y la multiplicatividad de los grados de las extensiones de cuerpos implica que

$$\operatorname{gr}(\alpha^2) = [\mathbb{Q}(\alpha^2) : \mathbb{Q}] = \frac{[\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)]} = \frac{\operatorname{gr}(\alpha)}{2} = \frac{d}{2}.$$

El lema 2.2, apartado 1, junto con la hipótesis inductiva, implica entonces que

$$|\overline{\alpha}| = \left|\overline{\alpha^2}\right|^{1/2} \geq \left(2^{1/(4\operatorname{gr}(\alpha^2))}\right)^{1/2} = 2^{1/(4\operatorname{gr}(\alpha))} = 2^{1/(4d)}.$$

Podemos concentrarnos entonces sobre la situación principal, que es el caso en el que los cuerpos $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\alpha^2)$ coinciden. Consideramos los polinomios mónicos en $\mathbb{Z}[X]$ de grado d definidos como

$$P_2 = \prod_{i=1}^{d}(X - \alpha_i^2), \quad P_4 = \prod_{i=1}^{d}(X - \alpha_i^4).$$

La hipótesis de que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$ implica que $\operatorname{gr}(\alpha^2) = d$, y por lo tanto P_2 es el polinomio mínimo de este entero algebraico. En particular, todas sus raíces son distintas.

Por otra parte, P_2 y P_4 no tienen ninguna raíz en común: si así fuera, tendríamos que $\alpha_i^2 = \alpha_j^4$ para algún par de índices i, j. El grupo de Galois absoluto G actúa de forma transitiva sobre los conjugados de α, y podríamos entonces tomar un elemento $\sigma \in G$ tal que $\alpha_j = \sigma(\alpha_i)$. Sea $e > 0$ el orden de este $\mathbb{Q}$-automorfismo, es decir, el entero positivo mínimo tal que $\sigma^e = \mathrm{Id}_{\overline{\mathbb{Q}}}$. Así,

$$\alpha_i^2 = \sigma(\alpha_i)^4 = \sigma(\alpha_i^2)^2 = \sigma(\sigma(\alpha_i)^4)^2 = \sigma^2(\alpha_i)^8 = \cdots = \sigma^e(\alpha_i)^{2^{e+1}} = \alpha_i^{2^{e+1}},$$

lo cual no es posible, ya que α no es ni nulo ni una raíz de la unidad.

Por el lema 2.5, estos polinomios son congruentes módulo 4, y por lo tanto existe otro polinomio $Q \in \mathbb{Z}[X]$ de grado menor que d tal que

$$P_2 = P_4 + 4Q.$$

Sean $P_4 = X^d + p_{d-1}X^{d-1} + \cdots + p_0$ y $Q = q_{d-1}X^{d-1} + \cdots + q_0$ con $p_i, q_j \in \mathbb{Z}$. Podemos escribir el cociente entre P_2 y P_4 como

$$\begin{aligned}\frac{P_2}{P_4} = 1 + 4\,\frac{Q}{P_4} &= 1 + 4\,\frac{q_{d-1}X^{d-1} + \cdots + q_0}{X^d + p_{d-1}X^{d-1} + \cdots + p_0} \\ &= 1 + 4\,\frac{q_{d-1}X^{-1} + \cdots + q_0X^{-d}}{1 + p_{d-1}X^{-1} + \cdots + p_0X^{-d}} = 1 + 4\,R(X^{-1})\end{aligned}$$

con $R \in X\mathbb{Z}[[X]]$. Este cociente define entonces una función holomorfa

$$f\colon \mathbb{P}^1(\mathbb{C}) \smallsetminus \{\alpha_1^2, \ldots, \alpha_d^2, \alpha_1^4, \ldots, \alpha_d^4\} \longrightarrow \mathbb{C}, \quad z \longmapsto \frac{P_2(z)}{P_4(z)}$$

que no se anula en ningún punto, y cuyo desarrollo de Taylor en ∞ es

$$f(z) = 1 + 4R(z^{-1}).$$

En particular, $f(\infty) = 1$.

Consideremos el erizo

$$\mathcal{H} = H(\alpha_1^2, \ldots, \alpha_d^2, \alpha_1^4, \ldots, \alpha_d^4).$$

El teorema de Dubinin (teorema 3.6) implica que su constante de Chebyshov se puede acotar superiormente por

$$\operatorname{cheb}(\mathcal{H}) \leq 4^{-1/2d}\,\operatorname{máx}(|\alpha_1^2|, \ldots, |\alpha_d^2|, |\alpha_1^4|, \ldots, |\alpha_d^4|) = 2^{-1/d}|\overline{\alpha}|^4. \tag{5.2}$$

Por otra parte, su complemento en la esfera de Riemann $\Omega = \mathbb{P}^1(\mathbb{C}) \smallsetminus \mathcal{H}$ es un abierto simplemente conexo, y por lo tanto podemos considerar la (única) función holomorfa $g\colon \Omega \to \mathbb{C}$ tal que

$$g^2 = f|_\Omega, \quad g(\infty) = 1.$$

La función g no puede ser un cociente de polinomios: como ya hemos visto, P_2/P_4 tiene d ceros simples, y por lo tanto no puede ser el cuadrado de otro cociente de polinomios ya que, si lo fuera, sus ceros serían dobles.

Queremos ahora estudiar el desarrollo de Taylor de g en el infinito. Para ello consideramos $S = 1 + \sum_{k\geq 1} a_k X^k \in \mathbb{Q}[[X]]$ la serie formal que cumple $S(0) = 1$ y $S^2 = 1 + 4X$, por lo que el desarrollo buscado es $g(z) = S(R(z^{-1}))$.

Esta serie formal tiene coeficientes

$$a_k = \frac{\frac{1}{2}(\frac{1}{2} - 1)\cdots(\frac{1}{2} - k + 1)}{k!}\,4^k.$$

Para cada primo p, denotamos por ν_p la valoración p-ádica correspondiente. Luego, para cada $k \geq 1$,

$$\nu_2(a_k) = k - \nu_2(k!) = k - \sum_{\ell \geq 1} \left\lfloor \frac{k}{2^\ell} \right\rfloor \geq k - \sum_{\ell \geq 1} \frac{k}{2^\ell} = 0.$$

Por otra parte, para cada primo impar p tomamos enteros r, b tales que $r \geq \nu_p(k!)$ y $2b \equiv 1 \pmod{p^r}$. Luego

$$\frac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-k+1)}{k!} = \frac{b(b-1)\cdots(b-k+1)}{k!} + \frac{p^r c}{2^k k!}$$

para un cierto entero c, lo cual implica $\nu_p(a_k) \geq 0$. Así, todas las valoraciones p-ádicas de a_k son no negativas y, por lo tanto, este coeficiente es un entero, con lo cual $S \in \mathbb{Z}[[x]]$.

Así, el desarrollo de Taylor de g en ∞ es $g(z) = T(z^{-1})$ con $T \in \mathbb{Z}[[X]]$. Como g no es cociente de polinomios, el teorema de racionalidad de Pólya (teorema 4.6) muestra que

$$\operatorname{cheb}(\mathcal{H}) \geq 1.$$

De esta desigualdad, junto con la obtenida en (5.2), se sigue que $\overline{|\alpha|}^4 \geq 2^{1/d}$, lo cual es equivalente a la cota inferior (5.1) y termina la demostración del teorema.

Agradecimientos. Este artículo está basado en un curso impartido por el primer autor en el Institute of Mathematical Sciences de Chennai, India, en marzo de 2021. Queremos agradecer especialmente a Joseph Oesterlé por habernos permitido utilizar sus notas de este curso. Agradecemos también a Francesco Amoroso y a Joaquim Ortega-Cerdá las discusiones y explicaciones que hemos tenido sobre la conjetura de Schinzel–Zassenhaus y la constante de Chebyshov, y a Javier Fresán su propuesta de redactar este artículo y sus correcciones sobre la versión preliminar.

Yuri Bilu forma parte del proyecto ANR JINVARIANT (Francia). José Ignacio Burgos Gil forma parte del proyecto de investigación MINECO PID2019-108936GB-C21 y del proyecto Severo Ochoa ICMAT CEX2019-000904-S. Martín Sombra forma parte del proyecto de investigación MINECO PID2019-104047GB-I0 y del proyecto María de Maeztu CRM CEX2020-001084-M.

Referencias

[1] D. W. Boyd, The maximal modulus of an algebraic integer, *Math. Comp.* **45** (1985), 243–249, S17–S20.

[2] P. Deligne, Extended Euler congruence, *Funct. Anal. Other Math.* **2** (2009), 249–250.

[3] V. Dimitrov, A proof of the Schinzel–Zassenhaus conjecture on polynomials, prepublicación, *arXiv:1912.12545* (2019).

[4] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.

[5] V. N. Dubinin, Change of harmonic measure in symmetrization, *Mat. Sb. (N.S.)* **124(166)** (1984), 272–279.

[6] V. N. Dubinin, *Condenser capacities and symmetrization in geometric function theory*, Springer, 2014.

[7] M. Fekete, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Z.* **17** (1923), 228–249.

[8] M. Fekete y G. Szegő, On algebraic equations with integral coefficients whose roots belong to a given point set, *Math. Z.* **63** (1955), 158–172.

[9] K. Haliste, On an extremal configuration for capacity, *Ark. Mat.* **27** (1989), 97–104.

[10] W. Jänichen, Über die Verallgemeinerung einer Gauss'schen Formel aus der Theorie der höheren Kongruenzen, *Sitzungsber. Berlin. Math. Ges.* **20** (1921), 23–29.

[11] D. H. Lehmer, Factorization of certain cyclotomic functions, *Ann. of Math.* **34** (1933), 461–479.

[12] G. Pólya, Über gewisse notwendige Determinantenkriterien für die Fortsetzbarkeit einer Potenzreihe, *Math. Ann.* **99** (1928), 687–706.

[13] R. M. Robinson, An extension of Pólya's theorem on power series with integer coefficients, *Trans. Amer. Math. Soc.* **130** (1968), 532–543.

[14] A. Schinzel y H. Zassenhaus, A refinement of two theorems of Kronecker, *Michigan Math. J.* **12** (1965), 81–85.

[15] T. Schönemann, Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben, *J. Reine Angew. Math.* **19** (1839), 289–308.

[16] C. L. Siegel, Algebraic integers whose conjugates lie in the unit circle, *Duke Math. J.* **11** (1944), 597–602.

[17] C. J. Smyth, On the product of the conjugates outside the unit circle of an algebraic integer, *Bull. London Math. Soc.* **3** (1971), 169–175.

[18] C. J. Smyth, A coloring proof of a generalisation of Fermat's little theorem, *Amer. Math. Monthly* **93** (1986), 469–471.

Yuri Bilu, Institut de Mathématiques de Bordeaux, Université de Bordeaux y CNRS, 351 cours de la Libération, 33405 Talence cedex, France

Correo electrónico: yuri@math.u-bordeaux.fr

Página web: https://www.math.u-bordeaux.fr/~ybilu/

José Ignacio Burgos Gil, Instituto de Ciencias Matemáticas (CSIC-UAM-UCM-UCM3), Calle Nicolás Cabrera 15, Campus UAM, Cantoblanco, 28049 Madrid, Spain

Correo electrónico: burgos@icmat.es

Página web: https://www.icmat.es/miembros/burgos/

Martín Sombra, Institució Catalana de Recerca i Estudis Avançats, Passeig Lluís Companys 23, 08010 Barcelona, Spain

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via 585, 08007 Barcelona, Spain

Centre de Recerca Matemàtica, Edifici C, Campus Bellaterra, 08193 Bellaterra, Spain

Correo electrónico: sombra@ub.edu

Página web: http://www.maia.ub.edu/~sombra/