POLINOMIOS CON TODAS SUS RAÍCES EN S^1

R. Toledano
FIQ-UNL-IMAL

16 de octubre 2009

Enteros Algebraicos

- Un número complejo α se dice que es un **entero algebraico** si α es raíz de un polinomio mónico en $\mathbb{Z}[x]$.

Enteros Algebraicos

- Un número complejo α se dice que es un **entero algebraico** si α es raíz de un polinomio mónico en $\mathbb{Z}[x]$.
- Ejemplos:

Enteros Algebraicos

- Un número complejo α se dice que es un **entero algebraico** si α es raíz de un polinomio mónico en $\mathbb{Z}[x]$.
- Ejemplos:
- Todo entero racional (es decir, todo elemento de $\mathbb{Z}$) es entero algebraico.

Enteros Algebraicos

- Un número complejo α se dice que es un **entero algebraico** si α es raíz de un polinomio mónico en $\mathbb{Z}[x]$.
- Ejemplos:
- Todo entero racional (es decir, todo elemento de $\mathbb{Z}$) es entero algebraico.
- $\sqrt{2}$, $\sqrt[4]{-3}$, i, $\frac{1+\sqrt{5}}{2}$ son enteros algebraicos.

Enteros Algebraicos

- Un número complejo α se dice que es un **entero algebraico** si α es raíz de un polinomio mónico en $\mathbb{Z}[x]$.
- Ejemplos:
- Todo entero racional (es decir, todo elemento de $\mathbb{Z}$) es entero algebraico.
- $\sqrt{2}$, $\sqrt[4]{-3}$, i, $\frac{1+\sqrt{5}}{2}$ son enteros algebraicos.
- Sin embargo, ningún racional ''puro'' (es decir, ningún elemento de $\mathbb{Q}\backslash\mathbb{Z}$) es entero algebraico.

Enteros Algebraicos

- Notación: $\overline{\mathbb{Z}}$ denota al conjunto de todos los enteros algebraicos.

Enteros Algebraicos

- Notación: $\overline{\mathbb{Z}}$ denota al conjunto de todos los enteros algebraicos.
- Sea $\alpha \in \overline{\mathbb{Z}}$. El polinomio mónico en $\mathbb{Z}[x]$ de menor grado posible del cual α es raíz se denomina **polinomio mínimo** de α.

Enteros Algebraicos

- Notación: $\overline{\mathbb{Z}}$ denota al conjunto de todos los enteros algebraicos.
- Sea $\alpha \in \overline{\mathbb{Z}}$. El polinomio mónico en $\mathbb{Z}[x]$ de menor grado posible del cual α es raíz se denomina **polinomio mínimo** de α.
- El **grado** de $\alpha \in \overline{\mathbb{Z}}$ es el grado del polinomio mínimo de α.

Enteros Algebraicos

- Notación: $\overline{\mathbb{Z}}$ denota al conjunto de todos los enteros algebraicos.
- Sea $\alpha \in \overline{\mathbb{Z}}$. El polinomio mónico en $\mathbb{Z}[x]$ de menor grado posible del cual α es raíz se denomina **polinomio mínimo** de α.
- El **grado** de $\alpha \in \overline{\mathbb{Z}}$ es el grado del polinomio mínimo de α.
- Ejemplo: $\alpha = \frac{1+\sqrt{5}}{2}$ es un entero algebraico de grado 2 pues

$$f(x) = x^2 - x - 1,$$

es el polinomio mínimo de α.

Enteros Algebraicos

- A las raíces del polinomio mínimo de $\alpha \in \overline{\mathbb{Z}}$ se las denomina **conjugados** de α.

Enteros Algebraicos

- A las raíces del polinomio mínimo de $\alpha \in \overline{\mathbb{Z}}$ se las denomina **conjugados** de α.
- Aquellos enteros algebraicos α tales que α^{-1} sea entero algebraico se denominan **unidades**.

Enteros Algebraicos

- A las raíces del polinomio mínimo de $\alpha \in \overline{\mathbb{Z}}$ se las denomina **conjugados** de α.
- Aquellos enteros algebraicos α tales que α^{-1} sea entero algebraico se denominan **unidades**.
- Las unidades son enteros algebraicos cuyos polinomios mínimos tienen coeficiente constante igual a ± 1.

Enteros Algebraicos

- A las raíces del polinomio mínimo de $\alpha \in \overline{\mathbb{Z}}$ se las denomina **conjugados** de α.
- Aquellos enteros algebraicos α tales que α^{-1} sea entero algebraico se denominan **unidades**.
- Las unidades son enteros algebraicos cuyos polinomios mínimos tienen coeficiente constante igual a ± 1.
- Ejemplo: $\alpha = \frac{1+\sqrt{5}}{2}$ es una unidad pues su polinomio mínimo es

$$f(x) = x^2 - x - 1 .$$

La Conjetura de Schinzel-Zassenhaus

- Un número complejo α se dice que es una **raíz de la unidad** si α es raíz de un polinomio de la forma $x^n - 1$.

La Conjetura de Schinzel-Zassenhaus

- Un número complejo α se dice que es una **raíz de la unidad** si α es raíz de un polinomio de la forma $x^n - 1$.
- (Conjetura de Schinzel-Zassenhaus) Existe una constante positiva c tal que para cada $n \in \mathbb{N}$ y cada $0 \neq \alpha \in \overline{\mathbb{Z}}$ de grado n que no sea raíz de la unidad, se satisface la siguiente desigualdad

$$\max_{1 \leq j \leq n} |\alpha_j| \geq 1 + \frac{c}{n},$$

donde $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ son los conjugados de α.

La Conjetura de Schinzel-Zassenhaus

- Un número complejo α se dice que es una **raíz de la unidad** si α es raíz de un polinomio de la forma $x^n - 1$.
- (Conjetura de Schinzel-Zassenhaus) Existe una constante positiva c tal que para cada $n \in \mathbb{N}$ y cada $0 \neq \alpha \in \overline{\mathbb{Z}}$ de grado n que no sea raíz de la unidad, se satisface la siguiente desigualdad

$$\max_{1 \leq j \leq n} |\alpha_j| \geq 1 + \frac{c}{n},$$

donde $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ son los conjugados de α.
- Se conjetura que la constante óptima es $c = \frac{3}{2} \log \beta$ donde $\beta = 1.3247\ldots$ es la única raíz real del polinomio $x^3 - x - 1$.

La Conjetura de Schinzel-Zassenhaus

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

La Conjetura de Schinzel-Zassenhaus

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α de grado n tal que $|f(0)| \geq 2$ y sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α.

La Conjetura de Schinzel-Zassenhaus

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α de grado n tal que $|f(0)| \geq 2$ y sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α.

Escribimos $M = \max_{1 \leq j \leq n} |\alpha_j|$.

La Conjetura de Schinzel-Zassenhaus

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α de grado n tal que $|f(0)| \geq 2$ y sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α.

Escribimos $M = \max_{1 \leq j \leq n} |\alpha_j|$.

Recordemos que $\prod_{j=1}^{n} \alpha_j = (-1)^n f(0)$.

La Conjetura de Schinzel-Zassenhaus

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α de grado n tal que $|f(0)| \geq 2$ y sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α.

Escribimos $M = \max\limits_{1 \leq j \leq n} |\alpha_j|$.

Recordemos que $\prod_{j=1}^{n} \alpha_j = (-1)^n f(0)$.

Entonces $M^n \geq \prod_{j=1}^{n} |\alpha_j| = |f(0)| \geq 2$,

La Conjetura de Schinzel-Zassenhaus

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α de grado n tal que $|f(0)| \geq 2$ y sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α.

Escribimos $M = \max\limits_{1 \leq j \leq n} |\alpha_j|$.

Recordemos que $\prod_{j=1}^{n} \alpha_j = (-1)^n f(0)$.

Entonces $M^n \geq \prod_{j=1}^{n} |\alpha_j| = |f(0)| \geq 2$,

con lo cual

$$M \geq 2^{1/n},$$

- Si $\alpha \in \overline{\mathbb{Z}}$ no es una unidad, la conjetura de Schinzel-Zassenhauss es cierta con $c = \log 2$:

Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α de grado n tal que $|f(0)| \geq 2$ y sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α.

Escribimos $M = \max\limits_{1 \leq j \leq n} |\alpha_j|$.

Recordemos que $\prod_{j=1}^{n} \alpha_j = (-1)^n f(0)$.

Entonces $M^n \geq \prod_{j=1}^{n} |\alpha_j| = |f(0)| \geq 2$,

con lo cual

$$M \geq 2^{1/n},$$

y entonces $\max\limits_{1 \leq j \leq n} |\alpha_j| \geq 1 + \frac{\log 2}{n}$.

¿Cuándo todos los conjugados de α están en S^1?

- Dado $f(x) \in \mathbb{Z}[x]$ mónico, de grado n y con raíces $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, para cada $k \in \mathbb{N}_0$ se define

$$S_k(f) := \sum_{j=1}^{n} \alpha_j^k \,.$$

¿Cuándo todos los conjugados de α están en S^1?

- Dado $f(x) \in \mathbb{Z}[x]$ mónico, de grado n y con raíces $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, para cada $k \in \mathbb{N}_0$ se define

$$S_k(f) := \sum_{j=1}^{n} \alpha_j^k .$$

- (Chowla, 1966) Sea $f(x) = \sum_{m=0}^{n} a_m x^m \in \mathbb{Z}[x]$ mónico, recíproco y de grado n y sea $H := n + \sum_{m=0}^{n} |a_m|$. Existe una constante positiva c tal que si

$$|S_k(f)| \le n, \quad \text{para todo } k \in [1, H^{cn^2}],$$

entonces todas las raíces de $f(x)$ están en S^1.

- (Teorema) Sea $f(x) \in \mathbb{Z}[x]$ mónico y de grado n tal que $f(0) \neq 0$. Sea

$$k \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)}.$$

Entonces $f(x)$ tiene todas sus raíces en S^1 si y sólo si la desigualdad

$$|S_{kj}(f)| \leq |S_j(f)|,$$

se cumple para todo $1 \leq j \leq (8k)^n$.

¿Cuándo todos los conjugados de α están en S^1?

Sea

$$\phi(n) := 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)}.$$

Las siguientes afirmaciones son equivalentes:

¿Cuándo todos los conjugados de α están en S^1?

Sea

$$\phi(n) := 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)}.$$

Las siguientes afirmaciones son equivalentes:

a) Existe un entero $m \in [1, (8k)^n]$ tal que

$$|S_{km}(f)| > |S_m(f)|,$$

si $k \geq \phi(n)$.

¿Cuándo todos los conjugados de α están en S^1?

Sea

$$\phi(n) := 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)}.$$

Las siguientes afirmaciones son equivalentes:

a) Existe un entero $m \in [1, (8k)^n]$ tal que

$$|S_{km}(f)| > |S_m(f)|,$$

si $k \geq \phi(n)$.

b) Existe un número primo $p > 2n$ y $q \in \mathbb{N}$ tal que

$$S_{pq}(f) \neq S_q(f).$$

¿Cuándo todos los conjugados de α están en S^1?

Sea

$$\phi(n) := 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)}.$$

Las siguientes afirmaciones son equivalentes:

a) Existe un entero $m \in [1, (8k)^n]$ tal que

$$|S_{km}(f)| > |S_m(f)|,$$

si $k \geq \phi(n)$.

b) Existe un número primo $p > 2n$ y $q \in \mathbb{N}$ tal que

$$S_{pq}(f) \neq S_q(f).$$

c) El polinomio $f(x)$ tiene una raíz fuera del disco unitario.

¿Cuándo todos los conjugados de α están en S^1?

- Resultado clásico: si p es un número primo entonces

$$S_{pq}(f) \equiv S_q(f) \mod p\,,$$

para todo $q \in \mathbb{N}_0$.

¿Cuándo todos los conjugados de α están en S^1?

- Resultado clásico: si p es un número primo entonces
$$S_{pq}(f) \equiv S_q(f) \mod p\,,$$
para todo $q \in \mathbb{N}_0$.
- (Dobrowolski, 1978) Sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de $0 \neq \alpha \in \overline{\mathbb{Z}}$ de grado n. Si α no es una raíz de la unidad entonces
$$\max_{1 \leq j \leq n} |\alpha_j| \geq 1 + \frac{\log n}{6n^2}\,.$$

¿Cuándo todos los conjugados de α están en S^1?

`a)` $\Rightarrow$ `b): trivial.`

a) $\Rightarrow$ b): trivial.
b) $\Rightarrow$ c): Sean $p > 2n$ un número primo y $q \in \mathbb{N}_0$ tales que $S_{pq}(f) \neq S_q(f)$. Entonces

$$S_{pq}(f) = S_q(f) + tp\,,$$

para algún $t \in \mathbb{Z}\backslash\{0\}$.

¿Cuándo todos los conjugados de α están en S^1?

a) $\Rightarrow$ b): trivial.
b) $\Rightarrow$ c): Sean $p > 2n$ un número primo y $q \in \mathbb{N}_0$ tales que $S_{pq}(f) \neq S_q(f)$. Entonces

$$S_{pq}(f) = S_q(f) + tp\,,$$

para algún $t \in \mathbb{Z}\backslash\{0\}$.
Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(x)$ y sea

$$M = \max_{1 \leq j \leq n} |\alpha_j|\,.$$

Entonces $|S_k(f)| \leq nM^k$ para todo $k \in \mathbb{N}_0$.

¿Cuándo todos los conjugados de α están en S^1?

entonces

$$\begin{aligned} M^{pq} n &\geq |S_{pq}(f)| \\ &= |tp + S_q(f)| \geq |tp| - |S_q(f)| \\ &\geq p - nM^q > 2n - nM^q \geq n(2 - M^q)\,. \end{aligned}$$

entonces

$$\begin{aligned} M^{pq}n &\geq |S_{pq}(f)| \\ &= |tp + S_q(f)| \geq |tp| - |S_q(f)| \\ &\geq p - nM^q > 2n - nM^q \geq n(2 - M^q)\,. \end{aligned}$$

Esto demuestra que $M \neq 1$. Como

$$1 \leq |f(0)| = \prod_{j=1}^{n} |\alpha_j|\,,$$

no puede ser que $M < 1$.

entonces

$$\begin{aligned} M^{pq} n &\geq |S_{pq}(f)| \\ &= |tp + S_q(f)| \geq |tp| - |S_q(f)| \\ &\geq p - nM^q > 2n - nM^q \geq n(2 - M^q)\,. \end{aligned}$$

Esto demuestra que $M \neq 1$. Como

$$1 \leq |f(0)| = \prod_{j=1}^{n} |\alpha_j|\,,$$

no puede ser que $M < 1$.
Luego $M > 1$ y, por lo tanto, $f(x)$ tiene una raíz fuera del disco unitario.

¿Cuándo todos los conjugados de α están en S^1?

c) $\Rightarrow$ a). Resultado clásico de aproximación diofántica (Kronecker): Sean $\alpha_1, \ldots, \alpha_n$ números reales arbitrarios y $N \in \mathbb{N}$. Entonces existen enteros $m_1, \ldots, m_n$ y $m \in \mathbb{N}$ tales que $1 \leq m \leq N^n$ y

$$\left| \alpha_k - \frac{m_k}{m} \right| < \frac{1}{mN},$$

para $k = 1, \ldots, n$.

¿Cuándo todos los conjugados de α están en S^1?

Sean $\theta \in [0,1]$ y $a, b \in \mathbb{Z}$ tales que $|a\theta - b| < 1/8$.
Entonces

$$-\frac{\pi}{4} < 2\pi(a\theta - b) < \frac{\pi}{4}\,.$$

¿Cuándo todos los conjugados de α están en S^1?

Sean $\theta \in [0,1]$ y $a, b \in \mathbb{Z}$ tales que $|a\theta - b| < 1/8$. Entonces

$$-\frac{\pi}{4} < 2\pi(a\theta - b) < \frac{\pi}{4}\,.$$

Por lo tanto

$$\cos(2\pi(a\theta - b)) > \frac{\sqrt{2}}{2}\,.$$

¿Cuándo todos los conjugados de α están en S^1?

Sean $\theta \in [0,1]$ y $a, b \in \mathbb{Z}$ tales que $|a\theta - b| < 1/8$. Entonces

$$-\frac{\pi}{4} < 2\pi(a\theta - b) < \frac{\pi}{4}\,.$$

Por lo tanto

$$\cos(2\pi(a\theta - b)) > \frac{\sqrt{2}}{2}\,.$$

Sean $\alpha_1, \ldots, \alpha_n$ las raíces $f(x)$ y escribamos $\alpha_j = r_j\, e^{2\pi\theta_j}$. Sea

$$M := \max_{1 \le j \le n} |\alpha_j| = \max_{1 \le j \le n} r_j\,.$$

¿Cuándo todos los conjugados de α están en S^1?

Luego $M > 1$ (por hipótesis), y usando la estimación de Dobrowolski, se tiene que:

Luego $M > 1$ (por hipótesis), y usando la estimación de Dobrowolski, se tiene que:

$$\phi(n) = 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)} \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log M} .$$

¿Cuándo todos los conjugados de α están en S^1?

Luego $M > 1$ (por hipótesis), y usando la estimación de Dobrowolski, se tiene que:

$$\phi(n) = 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log\left(1 + \frac{\log n}{6n^2}\right)} \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log M}.$$

Sea $k \geq \phi(n)$. Usando el teorema de Kronecker con $N = 8k$ tenemos que existen enteros $m_1, \ldots, m_n$ y $m \in \mathbb{N}$ tales que $1 \leq m \leq N^n$ y

$$\left|\theta_j - \frac{m_j}{m}\right| < \frac{1}{mN},$$

para $1 \leq j \leq n$.

Por lo tanto $|km\theta_j - km_j| < 1/8$ y así

¿Cuándo todos los conjugados de α están en S^1?

Por lo tanto $|km\theta_j - km_j| < 1/8$ y así

$$\begin{aligned}\cos(2km\pi\theta_j) &= \cos(2\pi(km\theta_j - km_j) + 2km_j\pi) \\ &= \cos(2\pi(km\theta_j - km_j)) > \frac{\sqrt{2}}{2}.\end{aligned}$$

Entonces

¿Cuándo todos los conjugados de α están en S^1?

Por lo tanto $|km\theta_j - km_j| < 1/8$ y así

$$\begin{aligned}\cos(2km\pi\theta_j) &= \cos(2\pi(km\theta_j - km_j) + 2km_j\pi) \\ &= \cos(2\pi(km\theta_j - km_j)) > \frac{\sqrt{2}}{2}\,.\end{aligned}$$

Entonces

$$\begin{aligned}|S_{km}(f)| &= \Big|\sum_{j=1}^{n} r_j^{km}\, e^{2km\pi\theta_j}\Big| \\ &= \Big|\sum_{j=1}^{n} r_j^{km}(\cos(2km\pi\theta_j) + i\,\mathrm{sen}(2km\pi\theta_j))\Big| \\ &\geq \Big|\sum_{j=1}^{n} r_j^{km}\cos(2km\pi\theta_j)\Big| > \frac{\sqrt{2}}{2}\sum_{j=1}^{n} r_j^{km} \geq \frac{\sqrt{2}}{2}\, M^{km}\,.\end{aligned}$$

¿Cuándo todos los conjugados de α están en S^1?

Por otra parte, como

$$k \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log M} \quad \text{entonces} \quad \log M^{k-1} \geq \log \frac{2n}{\sqrt{2}}.$$

Por otra parte, como

$$k \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log M} \quad \text{entonces} \quad \log M^{k-1} \geq \log \frac{2n}{\sqrt{2}} .$$

Como $m \geq 1$ tenemos que

$$\log M^{(k-1)m} \geq m \log\left(\frac{2n}{\sqrt{2}}\right) \geq \log \frac{2n}{\sqrt{2}} .$$

¿Cuándo todos los conjugados de α están en S^1?

Por otra parte, como

$$k \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log M} \quad \text{entonces} \quad \log M^{k-1} \geq \log \frac{2n}{\sqrt{2}}\,.$$

Como $m \geq 1$ tenemos que

$$\log M^{(k-1)m} \geq m \log \left(\frac{2n}{\sqrt{2}} \right) \geq \log \frac{2n}{\sqrt{2}}\,.$$

Por lo tanto

$$\frac{\sqrt{2}}{2} M^{(k-1)m} \geq n\,,$$

Por otra parte, como

$$k \geq 1 + \frac{\log \frac{2n}{\sqrt{2}}}{\log M} \quad \text{entonces} \quad \log M^{k-1} \geq \log \frac{2n}{\sqrt{2}} \,.$$

Como $m \geq 1$ tenemos que

$$\log M^{(k-1)m} \geq m \log \left(\frac{2n}{\sqrt{2}} \right) \geq \log \frac{2n}{\sqrt{2}} \,.$$

Por lo tanto

$$\frac{\sqrt{2}}{2} M^{(k-1)m} \geq n \,,$$

y entonces

$$|S_{km}(f)| > \frac{\sqrt{2}}{2} M^{(k-1)m} M^m \geq n M^m \geq |S_m(f)| \,.$$

MUCHAS GRACIAS POR LA ATENCIÓN!!!