Trascendencia y Schneider-Lang

Seminario de Teoría de Números

Nicolás Vilches (PUC)

Abril 20 de 2018

Números algebraicos y trascendentes

Definición

Decimos que un $\alpha \in \mathbb{C}$ *es* **algebraico** *si existe un polinomio p no-cero y con coeficientes en* $\mathbb{Q}$ *tal que* $p(\alpha) = 0$. *En caso de que no exista un polinomio de dichas características, diremos que* α *es* **trascendente**. *Denotaremos por* $\overline{\mathbb{Q}}$ *el conjunto de números algebraicos.*

Números algebraicos y trascendentes

Definición

Decimos que un $\alpha \in \mathbb{C}$ *es* **algebraico** *si existe un polinomio* p *no-cero y con coeficientes en* $\mathbb{Q}$ *tal que* $p(\alpha) = 0$*. En caso de que no exista un polinomio de dichas características, diremos que* α *es* **trascendente**. *Denotaremos por* $\overline{\mathbb{Q}}$ *el conjunto de números algebraicos.*

Observación

No es difícil notar que $\overline{\mathbb{Q}}$ *es numerable, por lo que deben existir muchos números trascendentes.*

Un poco de historia

- 1844: Liouville demuestra la existencia de números trascendentes (sin cardinalidad!), y en 1851 construye el primer ejemplo explícito

$$\sum_{i=1}^{\infty} 10^{-i!}.$$

Un poco de historia

- 1844: Liouville demuestra la existencia de números trascendentes (sin cardinalidad!), y en 1851 construye el primer ejemplo explícito

$$\sum_{i=1}^{\infty} 10^{-i!}.$$

- 1873: Hermite prueba que e es trascendente.

Un poco de historia

- 1844: Liouville demuestra la existencia de números trascendentes (sin cardinalidad!), y en 1851 construye el primer ejemplo explícito

$$\sum_{i=1}^{\infty} 10^{-i!}.$$

- 1873: Hermite prueba que e es trascendente.
- 1882: von Lindemann prueba que π es trascendente.

Un poco de historia

- 1844: Liouville demuestra la existencia de números trascendentes (sin cardinalidad!), y en 1851 construye el primer ejemplo explícito

$$\sum_{i=1}^{\infty} 10^{-i!}.$$

- 1873: Hermite prueba que e es trascendente.
- 1882: von Lindemann prueba que π es trascendente.
- 1900: Hibert plantea un problema de trascendencia en su famosa lista de problemas.

El séptimo problema de Hilbert

Proposición 1 (Séptimo problema de Hilbert)

Sean $\alpha, \beta \neq 0, 1$ *dos números algebraicos, con* β *irracional. Entonces,* α^{β} *es trascendente.*

El séptimo problema de Hilbert

Proposición 1 (Séptimo problema de Hilbert)

Sean $\alpha, \beta \neq 0, 1$ *dos números algebraicos, con* β *irracional. Entonces,* α^β *es trascendente.*

En 1934, Gelfond y Schneider de manera independiente prueban el séptimo problema de Hilbert.

El séptimo problema de Hilbert

Proposición 1 (Séptimo problema de Hilbert)

Sean $\alpha, \beta \neq 0, 1$ *dos números algebraicos, con* β *irracional. Entonces,* α^{β} *es trascendente.*

En 1934, Gelfond y Schneider de manera independiente prueban el séptimo problema de Hilbert.
Posteriormente, Lang toma las ideas de Schenider y formula una versión más general de sus métodos.

El teorema de Schneider-Lang

Teorema 1 (Schneider-Lang, 1962)

Sea K un cuerpo de números, y $f_1, \ldots, f_d$ funciones meromorfas, con orden estricto $\leq \rho$, y al menos dos algebraicamente independientes sobre K. Supongamos además que

$$\forall i, \frac{d}{dz} f_i \in K[f_1, \ldots, f_d].$$

Sean ahora $w_1, \ldots, w_m$ complejos distintos, tales que $f_i(w_k) \in K$ para todo i, k (en particular, f_i no tiene polos en los w_k). Se cumple entonces que los w_i no pueden ser muchos:

$$m \leq C\rho[K : \mathbb{Q}],$$

con C una constante universal.

¿Cuánto vale la constante C?

- En *Introduction to Trascendental Numbers* (1966), Lang da $C = 20$, pero *"no se ha hecho un gran esfuerzo por achicar la constante"*.

¿Cuánto vale la constante C?

- En *Introduction to Trascendental Numbers* (1966), Lang da $C = 20$, pero *"no se ha hecho un gran esfuerzo por achicar la constante"*.
- En *Algebra* (1971), el mismo Lang da $C = 10$.

¿Cuánto vale la constante C?

- En *Introduction to Trascendental Numbers* (1966), Lang da $C = 20$, pero *"no se ha hecho un gran esfuerzo por achicar la constante"*.
- En *Algebra* (1971), el mismo Lang da $C = 10$.
- Murty y Rath dan $C = 4$ en *Transcendental Numbers* (2014)

¿Cuánto vale la constante C?

- En *Introduction to Trascendental Numbers* (1966), Lang da $C = 20$, pero *“no se ha hecho un gran esfuerzo por achicar la constante”*.
- En *Algebra* (1971), el mismo Lang da $C = 10$.
- Murty y Rath dan $C = 4$ en *Transcendental Numbers* (2014)

Hoy vamos a hacer una demostración con $C = 4$.

Definición

Un cuerpo $K \subset \mathbb{C}$ se dice **cuerpo de números** *si es una extensión finita de $\mathbb{Q}$ (i.e. finita dimensional como espacio vectorial sobre $\mathbb{Q}$). Denotamos por $[K : \mathbb{Q}]$ su dimensión (como espacio vectorial).*

Cuerpos de números y funciones holomorfas

Definición

Un cuerpo $K \subset \mathbb{C}$ se dice **cuerpo de números** *si es una extensión finita de $\mathbb{Q}$ (i.e. finita dimensional como espacio vectorial sobre $\mathbb{Q}$). Denotamos por $[K : \mathbb{Q}]$ su dimensión (como espacio vectorial).*

Definición

Una función $f : \mathbb{C} \to \mathbb{C}$ se dice **entera** *si tiene derivada compleja en todo $\mathbb{C}$, esto es, si para todo $z_0 \in \mathbb{C}$ existe el límite*

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

Funciones meromorfas

Definición

Diremos también que una función $h : U \subset \mathbb{C} \to \mathbb{C}$ *(con* U *abierto) es* **meromorfa** *si es el cociente de dos funciones enteras,*

$$h = \frac{f}{g},$$

con g *no idénticamente cero. Equivalentemente,* h *es holomorfa si tiene derivada compleja en todo* U*, y sólo tiene singularidades del tipo polos.*

Orden de una función

Definición

Una función entera f se dice de **orden estricto** $\leq \rho$ *si existe una constante C tal que, para todo $R > 0$,*

$$|f(z)| \leq C^{R^\rho} \text{ en } |z| \leq R.$$

Orden de una función

Definición

Una función entera f se dice de **orden estricto** $\leq \rho$ *si existe una constante C tal que, para todo $R > 0$,*

$$|f(z)| \leq C^{R^\rho} \text{ en } |z| \leq R.$$

Y una función meromorfa h se dice de **orden estricto** $\leq \rho$ *si existen f, g enteras tales que $h = f/g$, con f y g ambas de orden estricto $\leq \rho$.*

Orden de una función

Definición

Una función entera f se dice de **orden estricto** $\leq \rho$ *si existe una constante C tal que, para todo $R > 0$,*

$$|f(z)| \leq C^{R^\rho} \text{ en } |z| \leq R.$$

Y una función meromorfa h se dice de **orden estricto** $\leq \rho$ *si existen f, g enteras tales que $h = f/g$, con f y g ambas de orden estricto $\leq \rho$.*

Por ejemplo, la función $f(z) = e^z$ es evidentemente de orden estricto ≤ 1. Esto prueba también que todo polinomio es de orden ≤ 1.

Alturas

Definición

Sea $\alpha \in \overline{\mathbb{Q}}$ *un número algebraico. Definimos su* **altura** $H(\alpha)$ *como el máximo de los valores absolutos de sus conjugados (de Galois).*

Alturas

Definición

Sea $\alpha \in \overline{\mathbb{Q}}$ un número algebraico. Definimos su **altura** *$H(\alpha)$ como el máximo de los valores absolutos de sus conjugados (de Galois).*

Por ejemplo, si $\alpha = \sqrt{3} - \sqrt{2}$, sus conjugados de Galois son $\sqrt{2} + \sqrt{3}, \alpha, -\alpha$ y $-\sqrt{2} - \sqrt{3}$. El mayor valor absoluto es $\sqrt{2} + \sqrt{3} = H(\alpha)$.

Lema de Siegel

Lema (Siegel)

Sea K un cuerpo de números, $n > k$, y

$$
\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\
&\vdots \\
a_{k1}x_1 + \cdots + a_{kn}x_n &= 0
\end{aligned}
$$

un sistema de ecuaciones homogéneo en K. Sea además A un número tal que $H(a_{ij}) < A$, y $d \in \mathbb{Q}^+$ un número tal que $a_{ij}d \in \mathcal{O}_K$.

Lema de Siegel

Lema (Siegel)

Sea K un cuerpo de números, $n > k$, y

$$a_{11}x_1 + \cdots + a_{1n}x_n = 0$$
$$\vdots$$
$$a_{k1}x_1 + \cdots + a_{kn}x_n = 0$$

un sistema de ecuaciones homogéneo en K. Sea además A un número tal que $H(a_{ij}) < A$, y $d \in \mathbb{Q}^+$ un número tal que $a_{ij}d \in \mathcal{O}_K$. Entonces, existe una solución no trivial $y_1, \ldots, y_n \in \mathcal{O}_K$ del sistema, tal que $H(y_i) \leq C(CndA)^{\frac{r}{n-r}}$ con C constante que depende sólo de K.

Acotando derivadas

Lema

Sea K un cuerpo de números, y $f_1, \dots, f_N$ funciones holomorfas cerca de $w \in \mathbb{C}$. Supongamos además que $f_k' \in K[f_1, \dots, f_N]$ para todo k, y que $f_k(w) \in K$ para todo k. Entonces, existe C_1 constante tal que, para todo polinomio $p \in K[T_1, \dots, T_N]$, de grado menor o igual a r, tenemos que la función $f = p(f_1, \dots, f_N)$ tiene sus derivadas acotadas por

$$H\left(\frac{d^k}{dz^k} f(w)\right) \leq H(P) k! C_1^{k+r},$$

donde $H(P)$ es la mayor altura de sus coeficientes.

Acotando derivadas

Lema

Sea K un cuerpo de números, y $f_1, \ldots, f_N$ funciones holomorfas cerca de $w \in \mathbb{C}$. Supongamos además que $f_k' \in K[f_1, \ldots, f_N]$ para todo k, y que $f_k(w) \in K$ para todo k. Entonces, existe C_1 constante tal que, para todo polinomio $p \in K[T_1, \ldots, T_N]$, de grado menor o igual a r, tenemos que la función $f = p(f_1, \ldots, f_N)$ tiene sus derivadas acotadas por

$$H\left(\frac{d^k}{dz^k} f(w)\right) \leq H(P) k! C_1^{k+r},$$

donde $H(P)$ es la mayor altura de sus coeficientes. Además, si $q \in \mathbb{Q}^+$ es un elemento tal que al multiplicar los coeficientes de p por q obtenemos sólo enteros de $\mathcal{O}_K$, entonces existe q' tal que $q' \frac{d^k}{dz^k} f(w)$ es entero algebraico, y $|q'| \leq |q|\, C_1^{k+r}$.

El teorema de Schneider-Lang

Teorema 1 (Schneider-Lang, 1962)

Sea K un cuerpo de números, y $f_1, \ldots, f_d$ funciones meromorfas, con orden estricto $\leq \rho$, y al menos dos algebraicamente independientes sobre K. Supongamos además que

$$\forall i, \frac{d}{dz} f_i \in K[f_1, \ldots, f_d].$$

Sean ahora $w_1, \ldots, w_m$ complejos distintos, tales que $f_i(w_k) \in K$ para todo i, k (en particular, f_i no tiene polos en los w_k). Se cumple entonces que los w_i no pueden ser muchos:

$$m \leq C\rho[K : \mathbb{Q}],$$

con C una constante universal.

Demostración del Teorema: Cota inferior

Sean f y g dos funciones algebraicamente independientes entre las f_i, y r un entero positivo múltiplo por $2m$. Intentaremos armar una función

$$F = \sum_{i,j=1}^{r} a_{ij} f^i g^j,$$

con muchas derivadas cero.

Demostración del Teorema: Cota inferior

Sean f y g dos funciones algebraicamente independientes entre las f_i, y r un entero positivo múltiplo por $2m$. Intentaremos armar una función

$$F = \sum_{i,j=1}^{r} a_{ij} f^i g^j,$$

con muchas derivadas cero. De hecho, ya que la condición de "tener derivada cero en w_l" se escribe como una ecuación lineal homogénea en a_{ij}, y tenemos así las mn ecuaciones

$$0 = \frac{\mathrm{d}^k}{\mathrm{d}z^k} F(w_\nu) = \sum_{i,j=1}^{r} a_{ij} \frac{\mathrm{d}^k}{\mathrm{d}z^k} (f^i g^j)(w_\nu),$$

en r^2 incógnitas.

Demostración del Teorema: Cota inferior

Tomando r tal que $r^2 = 2mn$, el lema 1 nos asegura que podemos tomar los a_{ij} en $\mathcal{O}_K$, acotados esencialmente por las derivadas de f_i. Así, obtenemos de manera explícita

$$H(a_{ij}) \leq e^{n \log n + O(n+r)}.$$

Demostración del Teorema: Cota inferior

Tomando r tal que $r^2 = 2mn$, el lema 1 nos asegura que podemos tomar los a_{ij} en $\mathcal{O}_K$, acotados esencialmente por las derivadas de f_i. Así, obtenemos de manera explícita

$$H(a_{ij}) \leq e^{n \log n + O(n+r)}.$$

Ya que f y g son algebraicamente independientes, F no es idénticamente cero. Sea s tal que las primeras $s-1$ derivadas se anulan en todos los w_i, y alguna de las s-ésimas derivadas no se anula, sin pérdida de generalidad, la s-ésima derivada en w_1, que llamaremos γ. Por supuesto, $s \geq n$. Tenemos la cota

$$H(\gamma) \leq e^{s \log s + O(s)}.$$

Demostración del Teorema: Cota inferior

Además, este número tiene un denominador acotado por $e^{s \log s + O(s)}$. Si llamamos d a dicho denominador, tenemos que $\gamma d \in \mathcal{O}_K$. Así, podemos acotar la norma de γd por

$$1 \leq \|\gamma d\| \leq |\gamma| \, e^{s \log s + O(s)} \left(e^{s \log s + O(s)} \right)^{2([K:\mathbb{Q}]-1)},$$

de donde

$$|\gamma| \geq e^{-2[K:\mathbb{Q}] s \log s + s \log s + O(s)}.$$

Demostración del Teorema: Cota superior

Sea h una función de orden $\leq \rho$ tal que fh y gh son enteras, y $h(w_1) \neq 0$. Consideramos ahora la función

$$G(z) = \frac{h(z)^{2r} F(z)}{\prod_{\nu=1}^{m} (z - w_\nu)^s} \prod_{\nu=2}^{m} (w_1 - w_\nu)^s.$$

Demostración del Teorema: Cota superior

Sea h una función de orden $\leq \rho$ tal que fh y gh son enteras, y $h(w_1) \neq 0$. Consideramos ahora la función

$$G(z) = \frac{h(z)^{2r} F(z)}{\prod_{\nu=1}^{m} (z - w_\nu)^s} \prod_{\nu=2}^{m} (w_1 - w_\nu)^s.$$

Esta función es entera, y no es difícil ver que

$$\lim_{z \to w_1} \frac{G(z)}{h(z)^{2r}} = \frac{\frac{\mathrm{d}^s}{\mathrm{d}z^s} F(w_1)}{s!},$$

ya que en torno a w_1 la función F tiene sus primeras derivadas nulas por construcción, y así su expansión es

$$F(z) = \frac{\frac{\mathrm{d}^s}{\mathrm{d}z^s}}{s!} (z - w_1)^s + \{\text{términos más grandes}\}.$$

Demostración del Teorema: Cota superior

Así, basta acotar $G(z)$ en un círculo de radio $R = s^{1/2\rho}$, de donde

$$\left| \frac{\frac{\mathrm{d}^s}{\mathrm{d}z^s} F(w_1)}{s!} \right| = \left| \lim_{z \to w_1} \frac{G(z)}{h(z)^{2r}} \right| << C^{rR^\rho} R^{-ms},$$

lo que nos da una cota

$$e^{-ms(\log s)/2\rho + s \log s + rs^{1/2} c_1} \geq |\gamma| \,.$$

Demostración del Teorema: Tiro finale

Al juntar ambas cotas obtenidas, obtenemos

$$-ms(\log s)/2\rho + s\log s + rs^{1/2}c_1 \geq -2[K:\mathbb{Q}]s\log s + s\log s + O(s),$$

o

$$0 \geq s\log s/2\rho(m - 4\rho[K:\mathbb{Q}]) + O(s) - rs^{1/2}c_1 + O(s),$$

lo que se dispara si $m > 4\rho[K:\mathbb{Q}]$. Esto nos da la cota buscada.

Algunos corolarios directos: Hermite-Lindemann

Proposición 2 (Hermite-Lindemann)

Sea $\alpha \neq 0$ número algebraico. Se tiene que e^{α} es trascendente.

Algunos corolarios directos: Hermite-Lindemann

Proposición 2 (Hermite-Lindemann)

Sea $\alpha \neq 0$ número algebraico. Se tiene que e^α es trascendente.

Proof.

Si no lo fuera, las funciones $f(z) = z, g(z) = e^{\alpha z}$ cumplirían que $f(1), f(2), f(3), \ldots$ serían elementos de K, el cuerpo de números generado por α y e^α sobre $\mathbb{Q}$. Además, $f'(z) = 1, g'(z) = \alpha e^{\alpha z}$, de donde $f', g' \in K[f, g]$.

Algunos corolarios directos: Hermite-Lindemann

Proposición 2 (Hermite-Lindemann)

Sea $\alpha \neq 0$ número algebraico. Se tiene que e^{α} es trascendente.

Proof.

Si no lo fuera, las funciones $f(z) = z, g(z) = e^{\alpha z}$ cumplirían que $f(1), f(2), f(3), \ldots$ serían elementos de K, el cuerpo de números generado por α y e^{α} sobre $\mathbb{Q}$. Además, $f'(z) = 1, g'(z) = \alpha e^{\alpha z}$, de donde $f', g' \in K[f, g]$.
Por último, ambas tienen orden estricto ≤ 1, y son algebraicamente independientes; así, el Teorema de Schneider-Lang nos da contradicción. $\square$

Trascendencia de π y e

Corolario

π, e son trascendentes.

Trascendencia de π y e

Corolario

π, e son trascendentes.

Proof.

Primero, si π fuera algebraico Hermite-Lindemann nos dice que $e^{\pi i} = -1$ es trascendente, contradicción. Además, como 1 es algebraico, $e^1 = e$ es trascendente. $\square$

El séptimo problema de Hilbert

Proposición 3

Sean $\alpha \neq 0, 1, \beta$ dos números algebraicos, con β irracional. Se tiene que α^{β} es trascendente.

El séptimo problema de Hilbert

Proposición 3

Sean $\alpha \neq 0, 1, \beta$ dos números algebraicos, con β irracional. Se tiene que α^β es trascendente.

Demostración.

Si no lo fuera, consideramos K el cuerpo generado por $\alpha, \beta, \alpha^\beta$ sobre $\mathbb{Q}$. Las funciones $f(z) = e^z, g(z) = e^{\beta z}$ son algebraicamente independientes (si fueran algebraicamente dependientes, derivando muchas veces obtendríamos un sistema de ecuaciones eventualmente inconsistente), y sus derivadas están en $K[f, g]$.

El séptimo problema de Hilbert

Proposición 3

Sean $\alpha \neq 0, 1, \beta$ dos números algebraicos, con β irracional. Se tiene que α^β es trascendente.

Demostración.

Si no lo fuera, consideramos K el cuerpo generado por $\alpha, \beta, \alpha^\beta$ sobre $\mathbb{Q}$. Las funciones $f(z) = e^z, g(z) = e^{\beta z}$ son algebraicamente independientes (si fueran algebraicamente dependientes, derivando muchas veces obtendríamos un sistema de ecuaciones eventualmente inconsistente), y sus derivadas están en $K[f, g]$. Pero ahora estas funciones asumen valores en K para $z = \log \alpha, 2 \log \alpha, 3 \log \alpha, \ldots$. $\square$

Uso en trascendencia

Corolario

Sea $\alpha \neq 0 \in \mathbb{C}$, tal que existen funciones meromorfas $f_1, \ldots, f_d$ de orden estricto $\leq \rho$; y un cuerpo de números K tal que $f_i' \in K[f_1, \ldots, f_d]$. Supongamos además que existen infinitos $w_j \in K$ tales que $f_i(\alpha w_j) \in K$. Entonces α es trascendente.

Uso en trascendencia

Corolario

Sea $\alpha \neq 0 \in \mathbb{C}$, tal que existen funciones meromorfas $f_1, \ldots, f_d$ de orden estricto $\leq \rho$; y un cuerpo de números K tal que $f_i' \in K[f_1, \ldots, f_d]$. Supongamos además que existen infinitos $w_j \in K$ tales que $f_i(\alpha w_j) \in K$. Entonces α es trascendente.

Demostración.

Si fuera algebraico, consideramos K' el cuerpo de números generado por α y K; esto nos da una contradicción directa con Schneider-Lang. $\square$