Tema 6.- Números trascendentes. Teorema Fundamental del Álgebra

6.1 Números trascendentes

En el tema anterior vimos que el cardinal del conjunto $\overline{\mathbb{Q}}$ de los números algebraicos es numerable, por lo que existen "muchos más" números (complejos) trascendentes que algebraicos. En esta sección vamos a demostrar que el número

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = \sum_{n=0}^{\infty}\frac{1}{n!}$$

es trascendente. La prueba original de este resultado fue dada por Hermite, y más tarde fue simplificada por Weierstrass, Hilbert, Hurwitz y Gordan.

TEOREMA 6.1.1.– El número e es trascendente.

PRUEBA: [1] Procederemos por reducción al absurdo. Supongamos que e es algebraico y sea $g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0 \in \mathbb{Q}[X]$ su polinomio mínimo, con $m \geq 1$ y $b_0 \neq 0$ pues $g(X)$ es irreducible. Quitando denominadores encontramos unos enteros $a_0, \ldots, a_m$, con $a_0, a_m \neq 0$, tales que

$$a_m e^m + \cdots + a_1 e + a_0 = 0.$$

Dado un número primo p consideremos el polinomio de grado $mp+p-1$

$$f(X) = \frac{X^{p-1}(X-1)^p\cdots(X-m)^p}{(p-1)!}$$

y pongamos

$$F(X) = f(X) + f'(X) + \cdots + f^{(mp+p-1)}(X), \quad G(X) = e^{-X}F(X).$$

Se tiene

$$\frac{dG(X)}{dX} = -e^{-X}f(X)$$

de donde

$$a_j\int_0^j e^{-X}f(X)dX = a_j\left[-e^{-X}F(X)\right]_0^j = a_jF(0) - a_je^{-j}F(j)$$

y

$$\begin{aligned}\sum_{j=0}^{m}\left(a_je^j\int_0^j e^{-X}f(X)dX\right) &= F(0)\sum_{j=0}^{m}a_je^j - \sum_{j=0}^{m}a_jF(j) = \\ &= -\sum_{j=0}^{m}\sum_{i=0}^{mp+p-1}a_jf^{(i)}(j).\end{aligned} \tag{1}$$

[1] Tomada del libro de I. Stewart, "Galois Theory".

Veamos que los $f^{(i)}(j)$ son enteros, y que son divisibles por p salvo cuando $j=0$ e $i=p-1$.

Dado un polinomio $h(X)$, pongamos $\Delta^{(k)}(h(X))=\frac{1}{k!}h^{(k)}(X)$. La fórmula de Leibnitz nos da

$$\Delta^{(i)}(f(X))=\frac{1}{(p-1)!}\sum\Delta^{(k_0)}(X^{p-1})\Delta^{(k_1)}((X-1)^p)\cdots\Delta^{(k_m)}((X-m)^p),$$

donde la suma está extendida a todas las $(m+1)$-uplas $(k_0,\ldots,k_m)$ de enteros no negativos tales que $k_0+\cdots+k_m=i$. Ahora bien, los sumandos correspondientes a índices tales que $k_0>p-1$ o $k_r>p$ para algún $r=1,\ldots,m$ se anulan, de donde obtenemos

$$\Delta^{(i)}(f(X))=\cdots=$$
$$\tfrac{1}{(p-1)!}\sum\tbinom{p-1}{k_0}(X^{p-1-k_0})\tbinom{p}{k_1}(X-1)^{p-k_1}\cdots\tbinom{p}{k_m}(X-m)^{p-k_m}$$

siendo los índices de sumación las $(m+1)$-uplas $(k_0,\ldots,k_m)$ de enteros no negativos tales que $k_0+\cdots+k_m=i$ y $k_0\le p-1$, $k_r\le p$, $r=1,\ldots,m$.

Como consecuencia, $f^{(i)}(j)=0$ para todo $j=0,\ldots,m$ y todo $i=0,\ldots,p-2$.

Para $j=0,\ldots,m$ y $p-1<i\le mp+p-1$ tenemos

$$f^{(i)}(j)=i!\Delta^{(i)}(f(X))|_{X=j}=\cdots=$$
$$\tfrac{i!}{(p-1)!}\sum\tbinom{p-1}{k_0}(j^{p-1-k_0})\tbinom{p}{k_1}(j-1)^{p-k_1}\cdots\tbinom{p}{k_{j-1}}(1)^{p-k_{j-1}}\tbinom{p}{p}$$
$$\tbinom{p}{k_{j+1}}(-1)^{p-k_{j+1}}\cdots\tbinom{p}{k_m}(j-m)^{p-k_m}$$

donde la última suma está extendida a los $k_0,\ldots,k_m\ge 0$ tales que $k_0+\cdots+k_m=i$, $k_0\le p-1, k_r\le p, r\ge 1$ y $k_j=p$. Los distintos sumandos son números enteros y como $i>p-1$ se tiene que $\frac{i!}{(p-1)!}\in\mathbb{Z}p$. Así pues $f^{(i)}(j)$ es entero y múltiplo de p, para todo $j=0,\ldots,m$ y $p-1<i\le mp+p-1$.

Para $j=0$ e $i=p-1$ el único sumando no nulo corresponde a $k_0=p-1$, $k_1=\cdots=k_m=0$ y por tanto

$$f^{(p-1)}(0)=(-1)^p\cdots(-m)^p.$$

El valor de (1) es pues $Kp+a_0(-1)^p\cdots(-m)^p$ para algún $K\in\mathbb{Z}$. Si tomamos $p>\max(m,|a_0|)$ entonces el entero $a_0(-1)^p\cdots(-m)^p$ no es divisible por p y por tanto el valor de (1) no es divisible por p. En particular es no nulo.

Para $0\le t\le m$ se tiene $|f(t)|\le m^{mp+p-1}/(p-1)!$, de donde

$$\left|\sum_{j=0}^{m}\left(a_je^j\int_0^j e^{-X}f(X)dX\right)\right|\le\sum_{j=0}^{m}|a_je^j|\int_0^j\frac{m^{mp+p-1}}{(p-1)!}dX$$
$$\le\sum_{j=0}^{m}|a_je^j|j\frac{m^{mp+p-1}}{(p-1)!}$$

que tiende a 0 cuando p tiende a infinito, lo cual es una contradicción $\square$

6.2 El teorema fundamental del Álgebra

Teorema 6.2.1.– Todo polinomio

$$f(X) = a_d X^d + \cdots + a_0 \in \mathbb{C}[X]$$

de grado $d \geq 1$ con coeficientes complejos tiene alguna raíz en $\mathbb{C}$.

Prueba: Consideremos el polinomio $f(X)$ como una función entera $f : \mathbb{C} \to \mathbb{C}$. Supongamos que $f(X)$ no tiene ninguna raíz en $\mathbb{C}$. Entonces la función $g(z) = \frac{1}{f(z)}$ es de nuevo una función entera. Ahora bien, como $d \geq 1$ (y $a_d \neq 0$) sabemos que $g(z)$ tiende a 0 cuando $|z|$ tiende a infinito. Por tanto, g es una función entera y acotada en $\mathbb{C}$ y por el teorema de Liouville, g ha de ser constante, lo que contradice que $f(X)$ sea un polinomio de grado mayor o igual que 1. $\square$