UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y TECNOLOGÍA
PROGRAMA DE MAESTRÍA EN MATEMÁTICA

EL TEOREMA DE GELFOND-SCHNEIDER

POR:

DARÍO HERRERA DÍAZ

TESIS PRESENTADA COMO REQUISITO PARCIAL PARA OPTAR POR EL TÍTULO DE MAGÍSTER EN MATEMÁTICA

PANAMÁ, REPÚBLICA DE PANAMÁ

2014

Título de la Tesis: **"EL TEOREMA DE GELFOND-SCHNEIDER"**

TESIS

Sometida para optar al título de Maestría en Matemática

Vicerrectoría de Investigación y Postgrado

Facultad de Ciencias Naturales, Exactas y Tecnología

APROBADO POR:

Doctor Jaime Gutiérrez
Presidente

Doctor Josué Ortiz
Miembro

Profesor Arsenio Cornejo
Miembro

REFRENDADO POR:

REPRESENTANTE DE LA VICERRECTORÍA
DE INVESTIGACIÓN Y POSTGRADO

FECHA: Jueves 13 de marzo de 2014

AGRADECIMIENTO

Al Doctor Jaime Gutiérrez, por sugerirme el tema de la presente investigación; la cual me permitió apreciar las relaciones entre las distintas ramas de la matemática. También le agradezco haberse tomado el tiempo en la revisión de la misma.

ÍNDICE GENERAL

Contenido Páginas
Sumario.....1
Summary.....1
Introducción.....2

CAPÍTULO N°1: El origen de La Teoría de Números Trascendentes.....4
1.1. Algunas fuentes de La Teoría de Números Trascendentes.....4
1.2. Estado de La Teoría de Números Trascendentes antes de los 23 problemas de Hilbert.....11
1.3. Los 23 problemas de David Hilbert.....25
1.4. El séptimo problema de Hilbert.....36

CAPÍTULO N°2: Preliminares a algunos resultados trascendentes.....39
2.1. Propiedades Elementales.....39
2.2. Algunas Propiedades de los Polinomios.....41
2.3. Sumas Exponenciales Conjugadas Complejas.....51
2.4. Polinomios Simétricos.....56
2.5. Algunos resultados del Álgebra Lineal.....67
2.5. Algunos resultados de La Teoría de Números Algebraicos.....72
2.6. Algunos resultados del Análisis Complejo.....82

CAPÍTULO N°3: Algunos resultados trascendentes, previos a la solución del séptimo problema de Hilbert.....84
3.1. Irracionalidad de potencias de e y su trascendencia.....84
3.2. El Teorema de Lindemann-Weierstrass.....100
3.3. Irracionalidad de e^{π}.....115

CAPÍTULO N°4: Pruebas del Teorema de Gelfond-Schneider.....125
4.1. Teorema de Gelfond-Schneider.....125
4.2. Prueba de Gelfond.....126
4.3. Prueba de Schneider.....134
4.4. Corolarios del Teorema de Gelfond-Schneider.....147
4.5. Diferencias y similitudes en las soluciones del séptimo problema de Hilbert.....148

CONCLUSIONES.....150
RECOMENDACIONES.....152
REFERENCIAS BIBLIOGRÁFICAS.....153

LISTA DE ALGUNOS SÍMBOLOS UTILIZADOS

$\mathbb{N}$ ....El conjunto de los números naturales $\{0,1,2,\ldots\}$

$\mathbb{N}^+$......................El conjunto de los números naturales positivos

$\mathbb{Z}$........................El conjunto de los números enteros

$\mathbb{Q}$........................El conjunto de los números racionales

$\mathbb{R}$........................El conjunto de los números reales

$\mathbb{C}$........................El conjunto de los números complejos

$\tilde{\mathbb{Q}}$........................El conjunto de los números algebraicos

$C(p)$....................Coeficiente principal del polinomio $p(x)$

$gr(p)$...................Grado del polinomio $p(x)$

$mgr(p)$................Multigrado de un polinomio en varias indeterminadas

$\varkappa(\alpha)$....................Altura del número algebraico α

$N_{\mathbb{Q}(\theta)}(\mu)$...............Norma del número algebraico μ en $\mathbb{Q}(\theta)$

$\|\alpha\|$......................Máximo de los valores absolutos de los conjugados de α

SUMARIO

La presente investigación pretende exteriorizar las herramientas matemáticas empleadas en la demostración del Teorema de Gelfond-Schneider; presentando, al mismo tiempo, el desarrollo histórico-matemático que lo genera. La misma la hemos dividido en cuatro capítulos, los cuales se encuentran organizados de la siguiente manera: En el capítulo n°1 presentamos el desarrollo histórico-matemático que produce el teorema de Gelfond-Schneider, el capítulo n°2 establece los conceptos matemáticos necesarios para la solución del séptimo problema de Hilbert, en el capítulo n°3 se presentan las pruebas de algunos resultados previos a la formulación de los 23 problemas de Hilbert y en el capítulo n°4 se exhiben las dos soluciones dadas, de forma independiente, del séptimo problema.

SUMMARY

This research aims to externalize the mathematical tools used in the demostration of the Gelfond-Schneider theorem, presenting at the same time, the historical and mathematical development which generated it. This work has been divided into four chapters, which are organized as follows: In the first chapter we present the historical and mathematical development that produces the Gelfond-Schneider theorem; the second chapter establishes the mathematical concepts needed for the solution of Hilbert's seventh problem; in the third chapter we present some previous results to the formulation of the Hilbert's 23 problems, and in the fourth chapter are exhibited two independent solutions given to the Hilbert's seventh problem.

INTRODUCCIÓN

Sabemos que los números reales pueden dividirse en racionales e irracionales y también que, en algunos casos, demostrar que cierto número es irracional no es tarea fácil de emprender; sin embargo otra que, posteriormente, ha llamado más la atención ha sido la división en números algebraicos y trascendentes. Los números algebraicos son infinitos numerables y los trascendentes infinitos no numerables, por ende se puede concluir que hay más números trascendentes que algebraicos; no obstante generar números trascendentes o demostrar la trascendencia de cierto número, es aún más complicado (al cabo de todo, primero tiene que ser irracional).

En 1900, en el Segundo Congreso Internacional de Matemáticos celebrado en Paris; David Hilbert propone veintitrés problemas, que en su opinión deberían ocuparse los matemáticos durante el siglo XX. En el séptimo problema conjeturó que: "α^{β} sería trascendente si α es un número algebraico diferente de 0 ó 1 y si β es un número algebraico irracional"; además proporcionó ejemplos como $2^{\sqrt{2}}$.

En 1929, el matemático ruso Alexander Gelfond presentó un primer adelanto de la solución del séptimo problema de Hilbert, la diferencia radicó en tomar a β como un número cuadrático imaginario irracional. Después, Kuzmin (1930) extiende este resultado a los β irracionales reales cuadráticos. No fue hasta 1934 cuando, de forma independiente, Gelfond y Theodor Schneider solucionan por completo el séptimo problema de Hilbert; conocido hoy día como teorema de Gelfond-Schneider.

En vista de que el teorema de Gelfond-Schneider resuelve el séptimo problema planteado por Hilbert y nos ayuda a demostrar, por ejemplo, que e^{π} es trascendente; es de vital importancia reconocer y comprender los conceptos matemáticos usados en su demostración, para poderlo emplear con confianza; de aquí que decidimos realizar la presente investigación.

CAPÍTULO N°1

EL ORIGEN DE LA TEORÍA DE NÚMEROS TRASCENDENTES

La Teoría de Números Trascendentes es un área de la Teoría de Números que es formulada, con sus propios métodos, a partir del siglo XX; no obstante florece a partir de fuentes diversas como los son: el problema clásico de la cuadratura del círculo, las investigaciones de Liouville y Cantor, las investigación de Hermite sobre la función exponencial y el séptimo problema de Hilbert (de su famosa lista de 23 problemas de los cuales debían ocuparse los matemáticos en el siglo XX).

En el presente capítulo presento el desarrollo-histórico matemático que suscita la solución del séptimo problema de Hilbert; el cual, posteriormente, será conocido como Teorema de Gelfond-Shneider. También se presenta la evolución de la Teoría de Número Trascendente, antes de la formulación de los 23 problemas de Hilbert; culminando con la enunciación de estos últimos y su estado actual.

1.1. Algunas fuentes de La Teoría de Números Trascendentes.

Los principales problemas de la Teoría de Números Trascendentes son probar la irracionalidad, la independencia lineal, la trascendencia y la independencia algebraica de ciertos números. Unas cuantas definiciones serán necesaria para definir el concepto de número trascendente, al tiempo que revisamos sus fuentes de origen.

Definición 1.1: Sea D un anillo. La colección $D[x]$, definida por:

$$D[x] = \{\sum_{i=0}^{n} a_i x^i \,/\, n \in \mathbb{N} \ y \ a_i \in D, \forall i = 0, \dots, n\}$$

la llamaremos anillo de los polinomios sobre D en la indeterminada x.

Observación 1.1: Algunas características o propiedades que posee el anillo D son conservadas por el anillo de polinomios $D[x]$, como lo son:

1. Si D es conmutativo, entonces $D[x]$ también los es.
2. Si 1 es la unidad de D, entonces 1 también es la unidad de $D[x]$.
3. Si D es un dominio entero (D no tiene divisores de cero), entonces $D[x]$ también lo es.
4. Si D es un cuerpo, entonces $D[x]$ es un Dominio Euclidiano y por ende es válido el algoritmo de la división en $D[x]$.

Ejemplo 1.1.

1. $\mathbb{Z}[x]$ es el anillo de los polinomios en la indeterminada x con coeficientes enteros.
2. $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ son anillos de polinomios en x con coeficientes racionales, reales y complejos; respectivamente. Además; como $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ forman cada uno un cuerpo, se tiene que $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ son dominios euclidianos, donde es válido el algoritmo de la división.

Definición 1.2: Sea $p(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$

1. Si $a_n \neq 0$ diremos que a_n es el coeficiente principal de $p(x)$ y lo denotaremos C(p); y que el grado de $p(x)$ es n , el cual denotaremos por $gr(p)$.
2. Diremos que un polinomio es una constante si es de grado 0 o es el polinomio cero.

Definición 1.3: Un número complejo α se dice que es raíz de un polinomio $p(z) \in \mathbb{Q}[z]$, si $p(\alpha) = 0$.

El descubrimiento de los números irracionales se le atribuye a los pitagóricos hacia mediado del siglo V a.C; específicamente a Hipaso de Metaponto, quien presumiblemente demostró que $\sqrt{2}$ era irracinnal usando aproximaciones geométricas. Una prueba de la irracionalidad de $\sqrt{2}$ la encontramos en los Elementos de Euclides, convirtiéndose esto en un teorema incipiente, junto con su prueba, de la Teoría de Números Trascendentes. En la actualidad hay muchas pruebas de la irracionalidad de $\sqrt{2}$, la que presentamos a continuación nos ayudará a comprender los argumentos empleados en la demostración de la trascendencia de ciertos números.

Teorema 1.1: El número $\sqrt{2}$ no es racional.

Prueba:

Supongamos que $\sqrt{2} \in \mathbb{Q}$, es decir $\sqrt{2} = \frac{r}{s}$. Donde $r, s \in \mathbb{N}^+ = \{1,2,3, \dots\}$

Definamos dos sucesiones $\{a_n\}$ y $\{b_n\}$ en forma recurrente, mediante las condiciones:

$$a_0 = 0 \quad a_1 = 1 \qquad a_n = 2a_{n-1} + a_{n-2} \quad n \geq 2$$

$$b_0 = 1 \qquad b_1 = 1 \qquad b_n = 2b_{n-1} + b_{n-2} \quad n \geq 2$$

Ahora consideremos los polinomios en $\mathbb{Z}[z]$, definidos por

$$P_n(z) = a_n^2 z^2 - b_n^2 \qquad , \quad n \in \mathbb{N}$$

Claramente

$$P_n(\sqrt{2}) \in \mathbb{Z} \quad y \quad P_n(\sqrt{2}) \neq 0, \qquad para\, n \geq 1$$

Es más, para $n \geq 1$ se tiene que:

(1.1) $$2a_n^2 - b_n^2 = (-1)^{n+1} \qquad y \qquad 2a_{n-1}a_n - b_{n-1}b_n = (-1)^n$$

Probemos esta última afirmación por inducción.

Para $n = 1$, obtenemos que:

$$2a_1^2 - b_1^2 = 2(1)^2 - 1 = 2 - 1 = 1 = (-1)^2 = (-1)^{1+1}$$

$$2a_{1-1}a_1 - b_{1-1}b_1 = 2a_0a_1 - b_0b_1 = 0 - 1(1) = -1 = (-1)^1$$

Si suponemos que (1.1) es válido para un particular n (Hipótesis de Inducción, H.I), se tiene que para $n + 1$:

$$2a_{n+1}^2 - b_{n+1}^2 = 2(2a_{n+1-1} + a_{n+1-2})^2 - (2b_{n+1-1} + b_{n+1-2})^2$$

$$= 2(2a_n + a_{n-1})^2 - (2b_n + b_{n-1})^2$$

$$= 2(4a_n^2 + 4a_n a_{n-1} + a_{n-1}^2) - (4b_n^2 + 4b_n b_{n-1} + b_{n-1}^2)$$

$$= 4(2a_n^2 - b_n^2) + 4(2a_n a_{n-1} - b_n b_{n-1}) + (2a_{n-1}^2 - b_{n-1}^2)$$

$$= 4(-1)^{n+1} + 4(-1)^n + (-1)^n \qquad \text{por la} \quad \text{H.I}$$

$$= (-1)^n$$

$$= (-1)^n(-1)^2$$

$$= (-1)^{n+2}$$

$$= (-1)^{(n+1)+1}$$

De manera análoga;

$$2a_{(n+1)-1}a_{n+1} - b_{(n+1)-1}b_{n+1} = 2a_n a_{n+1} - b_n b_{n+1}$$

$$= 2a_n(2a_n + a_{n-1}) - b_n(2b_n + b_{n-1})$$

$$= 2(2a_n^2 - b_n^2) + (2a_{n-1}a_n - b_{n-1}b_n)$$

$$= 2(-1)^{n+1} + (-1)^n \qquad \text{por H.I}$$

$$= (-1)^{n+1} + (-1)^{n+1} + (-1)^n$$

$$= (-1)^{n+1}$$

De (1.1) se deduce que para todo $n \geq 1, |P_n(\sqrt{2})| = 1$.

En vista de la definición de los P_n y nuestra suposición de que $\sqrt{2} = \frac{r}{s}$, podemos dar otra expresión para $|P_n(\sqrt{2})|$, a saber:

$$1 = |P_n(\sqrt{2})| = |2a_n^2 - b_n^2|$$

$$= |(\sqrt{2}a_n - b_n)(\sqrt{2}a_n + b_n)|$$

$$= \left|\left(a_n\tfrac{r}{s} - b_n\right)\left(a_n\tfrac{r}{s} + b_n\right)\right|$$

$$= |a_n r - b_n s| \left(\frac{a_n r + b_n s}{s^2}\right)$$

De esta última igualdad podemos inferir que $a_n r - b_n s$ es un entero satisfaciendo:

$$0 < |a_n r - b_n s| = \frac{s^2}{a_n r + b_n s}$$

Por otro lado, $\{a_n\}$ *y* $\{b_n\}$ son estrictamente crecientes. Veamos esto para $\{a_n\}$.

Por definición; $a_0 < a_1$ $\quad a_1 = 1 < 2 = a_2$ $\quad$ y para $n \geq 2$

$$a_{n+1} - a_n = 2a_{(n+1)-1} + a_{(n+1)-2} - a_n = 2a_n + a_{n-1} - a_n = a_n + a_{n-1} > 0$$

De forma análoga se prueba que $\{b_n\}$ es estrictamente creciente para $n \geq 2$, de donde se sigue que la sucesión $\{a_n r + b_n s\}$ también es estrictamente creciente; por lo tanto existe un entero ñ tal que

$$s^2 < a_{ñ} r + b_{ñ} s$$

Al considerar el polinomio auxiliar $P_{\tilde{n}}(z)$, obtenemos un entero $a_{\tilde{n}}r - b_{\tilde{n}}s$ que satisface la relación:

$$0 < |a_{\tilde{n}}r - b_{\tilde{n}}s| < 1$$

lo cual es imposible, pues no hay enteros entre 0 y 1. Así nuestra suposición inicial es falsa y $\sqrt{2}$ es irracional.□

Al suponer, en la demostración anterior, que $\sqrt{2} = \frac{r}{s} \in \mathbb{Q}$; alegamos que $\sqrt{2}$ es raíz de un polinomio de grado uno en $\mathbb{Z}[z]$. Por ende, podemos adoptar la siguiente definición:

Definición 1.4: Los números irracionales son aquellos números complejos que no son raíces de ningún polinomio de grado uno en $\mathbb{Z}[z]$.

El problema de la cuadratura del círculo fue lo que dio origen en el siglo XIX a las investigaciones sobre números trascendentes; dicho problema lo encontramos desde tiempos antiguos en el papiro Rhind, cuando el escriba Ahmes hacia el año 1650 a.C da una regla para construir un cuadrado de área "casi" igual a la del círculo.

La palabra "trascendente" fue utilizada por primera vez por Euler o Leibniz; algunos autores afirman que fue Leibniz quien la utilizo en 1704, otros como Yandell (2002) afirman que fue Euler alrededor de 1740 quien conjeturo que tales números existían y los llamó "trascendentes", ya que estos, según el propio Euler, "trascienden al poder de los métodos algebraicos". En este momento es oportuno presentar la definición de número algebraico y la de número trascendente.

Definición 1.5: Un número $\alpha \in \mathbb{C}$ se dice que es algebraico, si existe un polinomio $p(x) \in \mathbb{Z}[x]$ no nulo tal que $p(\alpha) = 0$.

Definición 1.6: Los números complejos que no son algebraicos se llaman trascendentes.

Observación 1.2. Al conjunto formado por los números algebraicos lo denotaremos por $\widetilde{\mathbb{Q}}$.

A continuación presentamos una cronología del estado de la Teoría de Números Trascendente antes del reto de Hilbert, la prueba de algunos de estos acontecimientos se presentan en el Capítulo N°3.

1.2. Estado de la Teoría de Números Trascendentes antes de los 23 problemas de Hilbert.

En **1727** el matemático suizo Leonhard Paul Euler utilizó por primera vez, de forma escrita, el símbolo e para un número y; posteriormente en **1737** demostró que este es irracional. En **1748** publica *Introductio in analysin infinitiorum* y; entre los hechos o resultados más sobresalientes que encontramos en esta publicación, podemos mencionar:

- Prueba que e^2 es irracional, utilizando su expansión en fracciones continuas.
- Obtiene la relación $e^{i\pi} = -1$
- Deriva la fórmula $e^{ix} = cos(x) + isen(x)$

- Calcula dieciocho dígitos de e
- Formula una conjetura para números trascendentes.

Conjetura de Euler: Para cualesquiera números racionales $a \neq 1$ y b;

$$log_a b = \frac{\ln b}{\ln a}$$

es trascendente si $\frac{\ln b}{\ln a}$ no es racional.

Posteriormente excluye casos triviales como $log_2 4$

Recordemos la definición moderna de la función logarítmica, para obtener una versión exponencial de esta conjetura.

Definición 1.7: La función logarítmica con base $a > 0, a \neq 1$, se define por

$$log_a b = y \quad si\ y\ sólo\ si \qquad a^y = b$$

Conjetura de Euler (Versión Exponencial): Suponga que a y b son números racionales distintos de cero, tales que

$$a^\beta = b$$

Entonces, si β no es racional, debe ser trascendente.

En esta versión se deduce que $2^{\sqrt{2}}$ es irracional, pues en caso contrario $\sqrt{2}$ sería trascendente; lo cual sabemos es falso, pues $\sqrt{2}$ es raíz del polinomio $p(x) = x^2 - 2 \in \mathbb{Z}[x]$.

Motivado por el problema de la cuadratura del círculo, Johann Lambert probó en **1766** que π es irracional. En **1815** Jospeh Fourier dió una prueba alternativa de la irracionalidad de e, la cual se convertiría en fuente para los métodos de demostración empleados en la Teoría de Números Trascendentes. Veamos esta prueba.

Teorema 1.2: El número e es irracional.

Prueba:

Supongamos que $e = \frac{r}{s}$, con $r, s \in \mathbb{Z}$ $y\, s \geq 1$.

Como $e = \sum_{n=0}^{\infty} \frac{1}{n!}$. Si consideramos $\sum_{n=0}^{s} \frac{1}{n!}$, se tiene que:

$$\frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}$$

es un número positivo; luego:

$$s!\left(\frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}\right) = s!\left(e - \sum_{n=0}^{s} \frac{1}{n!}\right) \in \mathbb{Z}^{+}$$

Denotemos esta última expresión por N. Al realizar algunas operaciones, se sigue que:

$$N = s!\left(e - \sum_{n=0}^{s} \frac{1}{n!}\right) = s!\left(\sum_{n=0}^{\infty} \frac{1}{n!} - \sum_{n=0}^{s} \frac{1}{n!}\right)$$

$$= s!\left(\sum_{n=s+1}^{\infty} \frac{1}{n!}\right)$$

$$= s!\left(\frac{1}{(s+1)!} + \frac{1}{(s+2)!} + \cdots\right)$$

$$N = \frac{1}{s+1} + \frac{1}{(s+2)(s+1)} + \frac{1}{(s+3)(s+2)(s+1)} + \cdots$$

En vista de que $s \geq 1$, $s + 1 \geq 2$; se sigue que:

$$\frac{1}{s+1} \leq \frac{1}{2}, \ \frac{1}{(s+2)(s+1)} < \frac{1}{2^2}, \ldots$$

Así,

$$N = \frac{1}{s+1} + \frac{1}{(s+2)(s+1)} + \frac{1}{(s+3)(s+2)(s+1)} + \cdots < \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots$$

$$= \sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n$$

$$= \sum_{n=1}^{\infty} \left(\frac{1}{2}\right)\left(\frac{1}{2}\right)^{n-1}$$

Luego,

$$N < 1$$

De esta forma hemos obtenido un entero N con la propiedad

$$0 < N < 1$$

lo cual es imposible, por lo tanto e es irracional.□

Aunque se había especulado que los números trascendentes existían, hasta 1844 no se había exhibido un número que fuese de esta clase. Fue entonces cuando Liouville demuestra que los números algebraicos irracionales no podían aproximarse a través de números racionales, a menos que los denominadores de estos últimos fuesen muy grandes. De este hallazgo se sigue que si un número irracional puede aproximarse mediante números racionales con denominadores relativamente pequeños, este debe ser trascendente. Antes de presentar el teorema, veamos una definición y un teorema preliminar.

Definición 1.8: Sea $\alpha \epsilon \bar{\mathbb{Q}}$. Un polinomio $f(x)$ *en* $\mathbb{Z}[x]$ se denomina un polinomio mínimo para α, si

$$gr(f) = min\{gr(g)/\ g(x) \in \mathbb{Z}[x] - \{0\}\ y\ g(\alpha) = 0\}$$

Si el máximo común divisor de los coeficientes de f es 1, entonces f se denomina el polinomio mínimo para α.

Definición 1.9: Sea $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo para un número algebraico α de grado n. Se dice entonces que α es un número algebraico de grado n o que el grado del número algebraico α es n; y lo denotaremos por $gr(\alpha) = n$, es decir, $gr(\alpha) = gr(f)$.

Definición 1.10: Sea $D[x]$ un anillo de polinomios sobre un dominio entero D. Un polinomio no constante $f(x) \in D[x]$ es irreducible sobre D, si siempre que $f(x) = g(x)h(x)$ con $g(x), h(x) \in D[x]$, entonces $gr(g) = 0$ ó $gr(h) = 0$

Lema 1.1: Si $f(x) \in \mathbb{Z}[x]$ es un polinomio mínimo para un número algebraico α, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Lema 1.2: Sea $f(z) \in \mathbb{Q}[z]$ y $\frac{p}{q} \in \mathbb{Q}$. Entonces;

$$f\left(\frac{p}{q}\right) = 0 \; sii \; f(z) = (qz - p)g(z)\text{ , para algún } g(z) \in \mathbb{Q}[z].$$

Del lema anterior se deduce que si $f(z) \in \mathbb{Q}[z]$ es irreducible de grado mayor que 1, $f\left(\frac{p}{q}\right) \neq 0 \;\; \forall \frac{p}{q} \in \mathbb{Q}$.

Teorema 1.3: (Teorema de Liouville).

Supóngase que α es un número algebraico de grado $d > 1$. Entonces existe una constante positiva $c(\alpha)$ tal que para todo número racional $\frac{p}{q}$,

$$\frac{c}{q^d} \leq \left|\alpha - \frac{p}{q}\right|$$

Prueba:

<u>CASO REAL</u>

Sean $\alpha \epsilon \mathbb{R}$ y $\frac{p}{q} \in \mathbb{Q}, q > 0$

Supongamos que $1 < \left|\alpha - \frac{p}{q}\right|$. En vista de que $q \geq 1$ se tiene que $\frac{1}{q} \leq 1$; de donde se sigue:

$$\frac{1}{q^d} < \frac{1}{q} \leq 1 < \left|\alpha - \frac{p}{q}\right|$$

Así, si tomamos $c \leq 1$, obtenemos la desigualdad;

$$\frac{c}{q^d} < \left|\alpha - \frac{p}{q}\right|$$

Supongamos ahora que $\left|\alpha - \frac{p}{q}\right| \leq 1$.

Sea $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \epsilon \mathbb{Z}[x]$, el polinomio mínimo para α.

$$f\left(\frac{p}{q}\right) = a_d \frac{p^d}{q^d} + a_{d-1}\frac{p^{d-1}}{q^{d-1}} + \cdots + a_1 \frac{p}{q} + a_0$$

$$= \frac{a_d p^d + a_{d-1}p^{d-1}q + \cdots + a_1 p q^{d-1} + a_0 q^d}{q^d}$$

Como f es irreducible y $gr(f) \geq 2$, por el lema 1.2. $f\left(\frac{p}{q}\right) \neq 0$

Luego;

$$\left|f\left(\frac{p}{q}\right)\right| = \frac{|N|}{q^d}$$

Donde $|N| \geq 1$, lo que implica que:

$$\frac{1}{q^d} \leq \left|f\left(\frac{p}{q}\right)\right|$$

En vista de que $f(\alpha) = 0$, podemos reescribir la desigualdad anterior como sigue:

$$\frac{1}{q^d} \leq \left|f(\alpha) - f\left(\frac{p}{q}\right)\right| \tag{1.2}$$

Ya que $\alpha \epsilon \mathbb{R}$ y, $y = f(x)$ es una función diferenciable; por el Teorema del Valor Medio existe φ entre α y $\frac{p}{q}$ tal que:

$$f(\alpha) - f\left(\frac{p}{q}\right) = f'(\varphi)\left(\alpha - \frac{p}{q}\right)$$

$$\left|f(\alpha) - f\left(\frac{p}{q}\right)\right| = |f'(\varphi)|\left|\alpha - \frac{p}{q}\right| \tag{1.3}$$

Ahora como φ está entre α y $\frac{p}{q}$, y $\left|\alpha - \frac{p}{q}\right| \leq 1$ se tiene que $|\alpha - \varphi| \leq 1$. De donde,

$$-\alpha - 1 \leq -\varphi \leq 1 - \alpha$$

$$\alpha - 1 \leq \varphi \leq 1 + \alpha$$

En vista de que f' es una función continua, y por lo tanto $|f'|$ también lo es; por el Teorema del Valor Extremo,

$$|f'(\varphi)| \leq max\{|f'(\theta)|/\theta \in [\alpha - 1, \alpha + 1]\}$$

Como $f'(\varphi) \neq 0$, pues en caso contrario $f\left(\frac{p}{q}\right) = 0$; se sigue que:

$$max\{|f'(\theta)|/\theta \epsilon [\alpha - 1, \alpha + 1]\} = M > 0 \tag{1.4}$$

Luego (1.2), (1.3) y (1.4) nos lleva a las desigualdades

$$\frac{1}{q^d} \leq |f'(\varphi)|\left|\alpha - \frac{p}{q}\right| \leq M\left|\alpha - \frac{p}{q}\right|$$

$$\frac{M^{-1}}{q^d} \leq \left|\alpha - \frac{p}{q}\right|$$

Si en esta ocasión tomamos $c = mín\{1, M^{-1}\}$, completamos la prueba del Teorema de Liouville para $\alpha \epsilon \mathbb{R}$.

CASO NO REAL

Sea $\alpha = a + bi \ (b \neq 0)$ y $\frac{p}{q} \in \mathbb{Q} \ (q > 0)$

$$\frac{|Im(\alpha)|}{q^d} \leq |Im(\alpha)| = |b| \leq \left|\left(a - \frac{p}{q}\right) + bi\right| = \left|(a + bi) - \frac{p}{q}\right| = \left|\alpha - \frac{p}{q}\right|$$

En este caso basta tomar $c = |Im(\alpha)|$, para obtener la desigualdad de Liouville.□

Corolario 1.1: El número $£ = \sum_{n=1}^{\infty} 10^{-n!}$ es trascendente.

Prueba:

Supongamos que $£ \in \tilde{\mathbb{Q}}$ y $gr(£) = d$.

Para aplicar el Teorema de Liouville debemos establecer que £ es irracional, es decir, $d > 1$. Veamos la expansión decimal de £.

$$£ = \sum_{n=1}^{\infty} 10^{-n!} = \frac{1}{10} + \frac{1}{100} + \frac{1}{1000000} + \frac{1}{1000000000000000000000000} + \cdots$$

$$= 0.11\underbrace{000}_{3\ ceros}1\underbrace{00000000000000000}_{17\ ceros}1\underbrace{000\ldots00}_{95\ ceros}1000\ldots$$

En vista de que la sucesión de los ceros consecutivos en la expansión decimal de £ crece sin límite, esta no puede ser eventualmente periódica; por lo tanto £ debe ser irracional.

Por el Teorema de Liouville, existe $c > 0$ tal que:

$$\frac{c}{q^d} \leq \left| £ - \frac{p}{q} \right| \tag{1.5}$$

para todo racional $\frac{p}{q}$.

Vamos a construir una sucesión de números racionales que se aproximen a £ y que contradice la desigualdad (1.5). En efecto, para un entero positivo N, sea

$$r_N = \sum_{n=1}^{N} 10^{-n!}$$

Ya que r_N tiene una expansión decimal finita, $r_N \in \mathbb{Q}$; el cual podemos definir por

$$r_N = \frac{p_N}{q_N}, \qquad \text{donde } p_N = 10^{N!} \sum_{n=1}^{N} 10^{-n!} \text{ y } q_N = 10^{N!}$$

Así,

$$r_1 = 10^{-1!} = \frac{1}{10} = 0.1$$

$$r_2 = \sum_{n=1}^{2} 10^{-n!} = \frac{1}{10} + \frac{1}{100} = 0.1 + 0.01 = 0.11$$

$$r_3 = \sum_{n=1}^{3} 10^{-n!} = \frac{1}{10} + \frac{1}{100} + \frac{1}{1000000} = 0.1 + 0.01 + 0.000001 = 0.110001$$

Luego cada truncamiento de la expansión decimal de £ se da antes de cada sucesión de ceros.

Se tiene que

$$\left|£ - \frac{p_N}{q_N}\right| = \sum_{n=1}^{\infty} 10^{-n!} - \sum_{n=1}^{N} 10^{-n!} = \sum_{n=N+1}^{\infty} 10^{-n!}$$

En vista de que

$$\sum_{n=N+1}^{\infty} 10^{-n!} = 10^{-(N+1)!} + 10^{-(N+2)!} + 10^{-(N+3)!} + \cdots$$

$$= (10^{-1})^{(N+1)!} + (10^{-1})^{(N+2)!} + (10^{-1})^{(N+3)!} + \cdots$$

Al compararla con la serie geométrica

$$\sum_{n=(N+1)!}^{\infty} 10^{-n} = 10^{-(N+1)!} + 10^{-[(N+1)!+1]} + 10^{-[(N+1)!+2]} + \cdots$$

$$= (10^{-1})^{(N+1)!} + (10^{-1})^{(N+1)!+1} + (10^{-1})^{(N+1)!+2} + \cdots$$

$$= \left(\frac{1}{10}\right)^{(N+1)!} + \left(\frac{1}{10}\right)^{(N+1)!+1} + \left(\frac{1}{10}\right)^{(N+1)!+2} + \cdots$$

$$= \sum_{n=1}^{\infty} \left(\frac{1}{10}\right)^{(N+1)!} \left(\frac{1}{10}\right)^{n-1}$$

$$= \frac{\left(\frac{1}{10}\right)^{(N+1)!}}{\frac{9}{10}} = \frac{10}{9}\, 10^{-(N+1)!}$$

Es evidente que

$$\sum_{n=N+1}^{\infty} 10^{-n!} < \sum_{n=(N+1)!}^{\infty} 10^{-n}$$

Lo que implica

$$\left|\pounds - \frac{p_N}{q_N}\right| < \frac{10}{9}\, 10^{-(N+1)!}$$

Aplicando (1.5) y reemplazando $q_N = 10^{N!}$ se tiene

$$\frac{c}{(q_N)^d} < \frac{10}{9}\, 10^{-(N+1)!}$$

$$\frac{c}{10^{dN!}} < \frac{10}{9}\, 10^{-(N+1)!}$$

$$c10^{-dN!} < \frac{10}{9}\, 10^{-(N+1)!}$$

De donde

$$0 < \frac{9}{10}c < 10^{dN!-(N+1)!}$$

$$0 < 9 < \left(\frac{10}{c}\right) 10^{dN!-(N+1)!}$$

Para $N \geq d,\ dN! - (N+1)! < 0$ y si N es relativamente grande obtenemos la desigualdad

$$0 < 9 < 1$$

Lo que es una contradicción. De donde nuestra suposición de que £ es algebraico es falsa; por lo tanto debe ser trascendente.□

En **1873** el matemático francés Charles Hermite demostró que e es trascendente, la demostración aparece en su memoria titulada: "Sobre la función exponencial", publicada en Comptes Rendus (Vol 77), y en la misma utiliza la representación en serie para el número $e^n = \sum_{k=0}^{\infty} \frac{n^k}{k!}$.

En **1874** el matemático alemán George Cantor demostró que la "mayoría" de los números reales eran trascendentes. Veamos una prueba de este resultado.

Teorema 1.4: El conjunto de los números algebraicos es numerable.

Prueba:

Si α es algebraico, satisface alguna ecuación polinomial de la forma

(1.6) $$p(x) = a_0 + a_1 x + \cdots + a_n x^n = 0 \qquad (n \geq 1)$$

Donde $p(x) \in \mathbb{Z}[x]$ y $a_n \neq 0$.

A cada ecuación de la forma (1.6) le podemos asociar el entero positivo

(1.7) $$|a_n| + |a_{n-1}| + \cdots + |a_0| + n = m$$

Ya que $|a_n| \geq 1$ y $n \geq 1$, $m \geq 2$ para cualquier ecuación de la forma (1.6). Sea $J \subset \mathbb{N}^+ \times (\mathbb{N}^+ - \{1\})$ el conjunto de pares de enteros (n, m) para los cuales se da (1.7) y definamos $P_{(n,m)}$ como sigue:

$$P_{(n,m)} = \{p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] / |a_n| + |a_{n-1}| + \cdots + |a_0| + n = m\}$$

Es claro que $P_{(n,m)}$ es finito; por lo tanto

$$\wp = \bigcup_{(n,m)\in J} P_{(n,m)}$$

es numerable, por ser la unión numerable de conjuntos finitos, es decir, que el conjunto de las ecuaciones polinomiales de la forma (1.6) es numerable.

De igual manera definamos para cada par de enteros $(n, m) \in J$ los conjuntos:

$$A_{(n,m)} = \{\alpha : p(\alpha) = 0 \; y \; p(x) \in P_{(n,m)}\}$$

Como todo polinomio de grado n no puede tener más de n raíces, $A_{(n,m)}$ es finito para todo$(n, m) \in J$; por consiguiente,

$$\widetilde{\mathbb{Q}} = \bigcup_{(n,m)\in J} A_{(n,m)}$$

es numerable□

Corolario 1.2: La "mayoría" de los números reales son trascendentes.

Prueba:

Como el conjunto de todos los números reales no es numerable, se sigue que el conjunto de los números reales trascendentes, $\mathbb{R} - \widetilde{\mathbb{Q}}$,no es numerable y por lo tanto, la "mayoría" de los números reales son trascendentes□

En **1882,** Ferdinand von Lindemann usa la representación en serie de e^z, la fórmula de Euller y algunos resultados sobre números algebraicos para probar que $i\pi$ es trascendente y por lo tanto π también es trascendente; incluso llego a probar que e^α es trascendente cuando α es un número algebraico no nulo. Este último resultado se conoce como Teorema de Hermite-Lindemann.

En **1884,** el matemático alemán Carl Weierstras generaliza el Teorema de Hermite-Lindemann al probar que $a_1e^{\alpha_1} + a_2e^{\alpha_2} + \cdots + a_le^{\alpha_l}$ es trascendente siempre que $\alpha_1, \alpha_2, \ldots, \alpha_l$ sean números algebraicos no nulos y distintos, al tiempo que $a_1, a_2, \ldots, a_l$ sean números algebraicos no nulos.

1.3. Los 23 problemas de David Hilbert.

El 8 de agosto de 1900, en el Segundo Congreso Internacional de Matemáticos, celebrado ea París, el matemático alemán David Hilbert planteó, originalmente, 10 problemas sin resolver que él pensaba marcarían el avance de la matemática durante el siglo XX. El artículo impreso de la conferencia de Hilbert contiene 23 problemas, así como una serie de argumentos acerca de por qué los matemáticos deberían enfrentarse a éstos, procurando llegar a teorías que arrojasen luz sobre el problema en cuestión, y sobre temas próximos. Entre tales argumentos está el problema de la braquistocrona de 1696, originalmente planteado por el matemático Johann Bernouilli, que pregunta por la curva que une dos puntos en un plano vertical y a lo largo de la cual una partícula deslizaría desde un punto al otro en el tiempo más corto. Los matemáticos presentes en la conferencia; si bien sabían que este problema había sido resuelto por varios matemáticos, entre los cuales estaba el

Inglés Issac Newton; también sabían que este había generado un variado conjunto de problemas similares y que la teoría en la cual se encuadraba el problema seguía llena de vida.

Hilbert nació el 23 de enero de 1862 en Kônigsberg, una pequeña ciudad en la Prusia Oriental. Ingreso en la Universidad de Kônigsberg en 1880 y fue allí donde tuvo contacto con Hermann Minkowski, un prodigio en matemática; quien le aconsejó no responder al discurso de Poincaré en el Primer Congreso Internacional de Matemáticos celebrado en Zurich, en el año 1897. Minkowski le escribe a Hilbert el 5 de enero de 1900, lo siguiente:

"Más atractivo sería el intento de mirar al futuro, en otras palabras, de hacer una caracterización de los problemas a los que los matemáticos deberían orientarse en el futuro. Con esto, podrías tener a gente hablando de tu charla incluso durante décadas a partir de ahora. Por supuesto, la profecía es realmente un asunto difícil" (Rûdenberg y Zassenhaus, 1973; citado por Gray, 2003, p.70)

Siguiendo el consejo de su amigo Minkowski, Hilbert presentó los problemas que desafiaron a la Matemática en los inicios del siglo XX; los cuales se describen, brevemente, a continuación:

1. El problema de Cantor del número cardinal del continuo.

Pide demostrar un teorema que se deriva de las investigaciones de Cantor sobre los cardinales infinitos. Cantor había probado en 1873 que el cardinal del conjunto de los números naturales era menor que el cardinal del conjunto de los números reales, el continuo denotado por *c*; posteriormente propone que el cardinal de cada subconjunto infinito de $\mathbb{R}$ es igual al de los números naturales, o bien al del continuo.

El teorema en cuestión establece que el continuo de los números reales es el conjunto infinito más pequeño estrictamente mayor que un conjunto numerable, por tal razón al primer problema se le conoce como la Hipótesis del Continuo.

Entre 1939 y 1940, Kurt Gôdel demostró que la hipótesis del continuo no puede refutarse en la teoría axiomática de Zermelo-Frankel-Axioma de Elección, es decir, que puede construirse una teoría de conjunto consistente donde la hipótesis del continuo sea cierta. Por otro lado, entre 1963 y 1964 Paul Cohen demuestra que al añadir el contario de la hipótesis del continuo al sistema de Zermelo-Frankel-Axioma de Elección; también puede construirse una teoría de conjunto consistente.

2. La compatibilidad de los axiomas de la Aritmética.

Pide demostrar que los axiomas de la Aritmética son consistentes, es decir, que un número finito de pasos lógicos basados en ellos no puede llevar a resultados contradictorios.

En 1931, Gôdel demuestra que tal como se formula habitualmente la aritmética es incompleta e indecidible.

3. La igualdad de los volúmenes de dos tetraedros de la misma base y la misma altura.

Consiste en disponer de dos sólidos de igual volumen, tal que ninguno de los dos pueda dividirse en número finito de piezas que puedan reordenarse para formar el otro.

En 1902, un estudiante de Hilbert, Max Dehn, demostró que un tetraedro y un cubo del mismo volumen no pueden fragmentarse y recomponerse de una forma diferente de modo que cada uno de ellos se trasforme en el otro. Dehn menciona en sus notas que Bricard en 1896 y Sforza en 1897 dieron ejemplos de poliedros que no pueden transformarse uno en otro por corte y pegado, pero sus argumentos eran insuficientes.

4. El problema de la línea recta como la distancia más corta entre dos puntos.

Los investigadores han encontrado este problema bastante vago, trata de manera general de imaginarse geometrías desde puntos de vistas sugestivos que permanezcan próximas a la geometría euclídea. Así, el problema es un programa de investigación y Herbert Busemann contribuyó notablemente al desarrollo de este, alrededor de 1966; seguido por Aleksei Pogorelov en 1973 y Z.I. Szabó en 1986.

5. El concepto de Lie de grupo continuo de transformaciones sin la hipótesis de la diferenciabilidad de las funciones que definen el grupo.

En este problema Hilbert pregunta si la hipótesis de la diferenciabilidad de las funciones que definen el grupo, por medio del cual Lie establece un sistema de axiomas geométricos, puede ser ignorada y posteriormente deducida de los demás axiomas geométricos y del mismo concepto de grupo.

Andrew Gleason, Deane Montgomery y Leo Zippin; dieron soluciones positivas en 1952.

6. Tratamiento matemático de los axiomas de la Física.

Plantea tratar por medio de axiomas, tal como se hizo con la geometría, aquellas ciencias físicas en las que las matemáticas juegan un papel importante. El problema no ha sido resuelto del todo matemáticamente; sin embargo: La mecánica clásica fue axiomatizada por Hamel en 1903, la termodinámica por Carathéodory en 1909, la relatividad especial por Robb 1914 y Carathéodory en 1924 (de forma independiente), la teoría de la probabilidad fue axiomatizada por Kolmogorov en 1930 y la teoría cuántica de campos fue axiomatizada por Wightman a finales de los años cincuenta del siglo XX.

7. Irracionalidad y trascendencia de ciertos números.

Hilbert sugiere una investigación completa del hecho de que ciertas funciones trascendentes especiales tomen valores algebraicos para ciertos argumentos algebraicos. Pide una demostración del hecho de que la expresión α^{β} , para una base algebraica y un exponente algebraico irracional representa siempre un número trascendente o al menos un número irracional.

En 1934, Alexander Gelfond y Theodor Schneider, de manera independiente, solucionaron este séptimo problema. Al final del capítulo volveremos a hacer otros comentarios de este problema y su solución.

8. Problemas de números primos.

Surge de un artículo de Riemann. El problema plantea demostrar que los ceros de la función $\varsigma(s)$ definida por la serie

$$\varsigma(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

tienen todos parte real $\frac{1}{2}$, excepto los bien conocidos ceros reales enteros negativos. Si se estableciese esta demostración, se estaría en condición, según Hilbert, de: comprobar con más exactitud la serie infinita de Riemann para el número de primos por debajo de un número dado, alcanzar la solución rigurosa del problema de Goldbach, atacar la cuestión de si existe un número infinito de pares de números primos que difieren en dos, etc.

Este problema, conocido como La hipótesis de Riemann, aún no ha sido resuelto.

9. Demostración de la ley de reciprocidad más general en cualquier campo de números.

Pide un teorema de reciprocidad para potencias arbitrarias en cualquier campo de números.

En 1927, Emil Artin conjeturó un resultado que daba todas las leyes de reciprocidad conocidas cuando se hacía explícito; el mismo que llevo a Kurt Hensel a definir un símbolo residuo de norma generalizado y completar la solución del 9° problema.

10. Determinación de la resolubilidad de la ecuación diofántica.

Pide determinar en un número finito de operaciones si una ecuación diofántica con cualquier número de incógnitas y con coeficientes numéricos enteros racionales es resoluble en enteros racionales.

En 1970, Yuri Matiyasevich demostró que no existe un algoritmo para resolver las ecuaciones diofánticas de este décimo problema.

11. Formas cuadráticas con coeficientes numéricos algebraicos cualesquiera.

Plantea resolver una ecuación cuadrática dada con coeficientes numéricos algebraicos en cualquier número de variables por números enteros o fraccionarios pertenecientes al dominio de racionalidad algebraico determinado por los coeficientes.

Parcialmente resuelto: En 1930, Carl Siegel lo resuelve sobre los números enteros y, entre 1923 y 1924 Helmut Hasse lo hace sobre los números racionales.

12. Extensión del teorema de Kronecker sobre campos abelianos a cualquier dominio de racionalidad algebraico.

Los expertos han señalado varios errores en la formulación de este problema; no obstante, lo importante es que ha generado un programa de investigación que permanece abierto; ya que depende del cuerpo algebraico particular con que se inicie.

13. La imposibilidad de la solución de la ecuación general de 7º grado por medio de funciones de sólo dos argumentos.

En este problema Hilbert plantea que la raíz de la ecuación de séptimo grado es una función de sus coeficientes que no pertenecen a la clase de funciones susceptibles de construcción nomográfica, es decir, que no pueden construirse por un número finito de inserciones de funciones de dos argumentos.

Resuelto en sentido negativo por Andrei Kolmogorov y su estudiante Vladimir Arnlo'd en 1957.

14. Demostración de la finitud de ciertos sistemas completos de funciones.

Hilbert pide demostrar que todas las funciones relativamente enteras de cualquier dominio de racionalidad dado constituye siempre un campo de integridad finito. Así pues, él está interesado en saber si el anillo que forman las funciones racionales tiene una base finita.

En 1962, Masayoshi Nagata produce un contraejemplo a lo planteado en este problema.

15. Fundamentación rigurosa del cálculo enumerativo de Schubert.

El problema consiste en:

"Establecer rigurosamente y con una determinación exacta de los límites de su validez aquellos números geométricos que Schubert en especial ha determinado sobre la base del denominado principio de posición especial, o conservación del número, por medio del cálculo enumerativo por él desarrollado" (Hilbert, 1900; citado por Gray, 2003, p.294 y Yandell, 2002, p.269)

Una teoría rigurosa se debe a Bartel Leendert van der Waerden en 1930, le sigue André Weil en 1946 con la publicación de su Fundamentos de la Geometría Algebraica.

16. Problema de la topología de curvas y superficies algebraica.

La primera parte del problema pregunta por el número de lazos que puede tener una curva algebraica real de un grado dado, y cómo pueden estar dispuestos. La segunda parte por el número máximo y la posición de los ciclos límites de Poincaré para una ecuación diferencial de primer orden, bajo ciertas condiciones.

Los mejores resultados sobre la topología de curvas se deben a Ilia Itenberg y Oleg Viro en 1996. De igual forma, encontramos resultados parciales para los ciclos límites de flujos dados por polinomios debidos a Yuri Ilyashenko y Écalle a principios de los noventa.

17. Expresión de formas definidas por cuadrados.

Pide, esencialmente, demostrar que toda forma definida no puede expresarse como un cociente de sumas de cuadrados de formas.

En 1927, Emil Artin y Otto Schreier resuelve el problema para campos cerrados reales. La cota superior sobre el número de formas requeridas se debe a Pfister en 1967 y la solución negativa en general se debe a Du Bois en el mismo año.

18. Construcción del espacio a partir de poliedros congruentes.

El problema se divide en tres partes, a saber:

i. Determinar si el número de grupos cristalográficos en los espacios euclídeos de grandes dimensiones es finito.
ii. Determinar si se puede llenar el espacio con regiones fundamentales idénticas que no estén asociadas con un grupo cristalográfico.
iii. Determinar la manera más eficiente de llenar el espacio con varios sólidos regulares.

La primera parte fue resuelta en 1910 por Ludwig Bieberbach, la segunda fue respondida afirmativamente en 1928 por K. Reinhardt en dimensión 3 y por Heesch en 1932 en dimensión 2. La tercera sigue sin resolver; no obstante, hay una respuesta elaborada por Thomas Hale en el 2000 que está siendo revisada.

19. ¿Son siempre necesariamente analíticas las soluciones de problemas regulares en el cálculo de variaciones?

En este problema Hilbert conjeturó que las soluciones de las denominadas ecuaciones "lagrangianas" serían siempre regulares.

La solución a esta conjetura la da el matemático Serge Bernstein en 1904. Desde entonces existen diversas variaciones de este problema, dependiendo del número de ecuaciones o de variables involucradas; dando origen a un programa de investigación.

20. El problema general de los valores de contorno.

Pide condiciones bajo las que una gran clase de ecuaciones tienen soluciones particularmente regulares, y teoremas regulares que garanticen la existencia de soluciones.

Por la generalidad del problema es considerado un programa de investigación, donde han intervenido un sin número de matemáticos e incluso se ha fusionado con el problema anterior.

21. Demostración de la existencia de ecuaciones diferenciales lineales que tienen prescrito un grupo monodrómico.

Pide demostrar que siempre existe una ecuación diferencial lineal de la clase fuchsiana, con puntos singulares y grupo monodrómico dado. Generalmente se denomina el problema de Riemann-Hilbert y fue resuelto en sentido negativo por Anosov y Bolibruch en 1994.

22. Uniformización de relaciones analíticas por medio de funciones automorfas.

Poincaré había demostrado que era posible uniformizar cualquier relación algebraica entre dos variables a través del uso de funciones automorfas de una variable. A raíz de lo demostrado por Poincaré, Hilbert plantea lo siguiente:

"No está demostrado si las dos funciones univaluadas de la nueva variable puede escogerse de modo que, mientras esta variable recorre el dominio regular de

dichas funciones; se alcanza y representan realmente todos los puntos regulares del campo analítico dado" (Hilbert, 1900; citado por Gray, 2003, p.303)

Hilbert también pidió que el teorema de uniformización se extendiera a funciones de tres o más variables.

Este problema fue resuelto por Jules Henri Poincaré y Paul Koebe, de manera independiente, en 1907.

23. Desarrollo adicional de los métodos del cálculo de variaciones.

Hilbert hace una presentación extensa de este "problema" y pide, principalmente, desarrollar los métodos del cálculo de variaciones; por ende ha sido catalogado como un programa de investigación.

1.4. El séptimo problema de Hilbert.

Ya se ha planteado en la sección anterior que en el séptimo problema, en su formulación original, Hilbert pide hacer un estudio general de qué sucede cuando ciertas funciones trascendentes toman valores algebraicos; él especula que si $f(z)$ es una función trascendental, entonces $f(\alpha)$ es un número trascendente siempre que α sea un número algebraico no nulo. Esta interrogante surge de los problemas resueltos por Hermite y Lindemann sobre la función exponencial; pero lo que se convirtió en imperativo fue probar que $2^{\sqrt{2}}$ y e^{π} representaban números trascendentes o al menos números irracionales y de manera general que:

La expresión α^{β}, para una base algebraica y un exponente algebraico irracional β representa siempre un número trascendente o al menos un número irracional.

Si comparamos la conjetura de Euler de 1748 con la de Hilbert de 1900 podemos apreciar que la diferencia estriba en la naturaleza aritmética de los números en consideración.

En 1929 el alemán Carl Ludwig Siegel demostró que la función de Bessel $J_0(x)$ toma valores trascendentes para argumentos algebraicos y en la prueba enuncia un lema, lema de Siegel, que permite construir ciertas funciones auxiliares; afirmando que tales funciones serían útiles, como en efecto lo fue, en la prueba del séptimo problema.

La solución de casos especiales del séptimo problema de Hilbert fue dada, por primera vez, por el Ruso Alexander Osipovich Gelfond en 1929 y aparecieron en Comptes Rendu. Lo primero que prueba Gelfond es que e^{π} es trascendente y seguidamente que $2^{\sqrt{-2}}$ también los es, empleando resultados de 1914 de George Pólya sobre funciones enteras.

La trascendencia del número de Hilbert, $2^{\sqrt{2}}$, fue probada en 1930 por el matemático ruso de nombre R.O. Kuzmin.

De forma independiente, la solución general del séptimo problema fue dada por Gelfond, el 1 de abril de 1934 y por un estudiante de Siegel, el alemán Theodor

Schneider, el 28 de mayo de 1934 y; a partir de la fecha se conoce como el Teorema de Gelfond-Schneider.

CAPITULO N° 2

PRELIMINARES A ALGUNOS RESULTADOS TRASCENDENTES

Una vez conocido el origen de la Teoría de Números Trascendentes; en este capítulo se presentan las herramientas matemáticas necesarias para la solución de séptimo problema de Hilbert y para la prueba de algunos resultados sobresalientes de esta teoría, descritos en el capítulo n°1.

2.1. Propiedades Elementales

Propiedad 2.1. Para enteros $N \geq n \geq k \geq 1$, se tiene que:

(a) $\frac{N!}{(N+n)!} \leq \frac{1}{n!}$

(b) $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

Propiedad 2.2: Dados dos enteros cualesquiera, su suma y su diferencia tienen la misma paridad.

Propiedad 2.3. Sea $K, r \in \mathbb{Z}^+$, con $r \geq 2$; entonces existe un entero $T_0 = T_0(K)$ tal que para todo $T > T_0$, se tiene que

$$(4KT)^2\left(16Kr^{2K^{\frac{3}{2}}}\right)^T < T^{\frac{T}{2}}$$

Prueba:

Sea $T > r^{(16K)^8}$ Entonces:

$$(16)^8 < r^{(16K)^8} < T$$

$$(16)^8 < T$$

$$[(16)^8]^T < T^T$$

$$[(16)^T]^8 < T^T$$

(2.1) $$(16)^T < T^{\frac{T}{8}}$$

$$K^8 < r^{(16K)^8} < T$$

$$K^8 < T$$

$$(K^8)^T < T^T$$

$$(K^T)^8 < T^T$$

(2.2) $$K^T < T^{\frac{T}{8}}$$

$$r^{16K^{\frac{3}{2}}} < r^{(16K)^8} < T$$

$$r^{16K^{\frac{3}{2}}} < T$$

$$\left(r^{16K^{\frac{3}{2}}}\right)^T < T^T$$

$$\left(r^{2K^{\frac{3}{2}}T}\right)^8 < T^T$$

(2.3) $$r^{2K^{\frac{3}{2}}T} < T^{\frac{T}{8}}$$

$$4K < r^{8K} = r^{2(4K)}$$

$$4KT < (r^{8K})^T$$

$$(4KT)^{16} < (r^{8KT})^{16}$$

$$(4KT)^{16} < (r^{16K})^{8T}$$

$$(4KT)^{\frac{16}{T}} < (r^{16K})^8 < T$$

$$(4KT)^{\frac{16}{T}} < T$$

$$(2.4) \qquad (4KT)^2 < T^{\frac{T}{8}}$$

Luego por (2.1), (2.2), (2.3), y (2.4);

$$(4KT)^2\left(16Kr^{2K^{\frac{3}{2}}}\right)^T = (4KT)^2(16)^T K^T \left(r^{2K^{\frac{3}{2}}}\right)^T$$

$$< T^{\frac{T}{8}}T^{\frac{T}{8}}T^{\frac{T}{8}}T^{\frac{T}{8}}$$

$$= T^{\frac{T}{2}}\square$$

2.2. Algunas Propiedades de los Polinomios.

Lema 2.1. Sea $f(z) = \sum_{N=j}^{k} c_N z^N \in \mathbb{Z}[z]$, para enteros j y k satisfaciendo $1 \leq j \leq k$; pruebe que:

$$\sum_{n=1}^{j} f^n(z) = \sum_{N=j}^{k}\left(N!\,c_N \sum_{n=N-j}^{N-1} \frac{z^n}{n!}\right) = \sum_{l=1}^{L}\left(K_{N_l} \sum_{n=N_l-p+1}^{N_l-1} \frac{z^n}{n!}\right)$$

Prueba:

$$\sum_{n=1}^{j} f^n(z) = f^1(z) + f^2(z) + f^3(z) + \cdots + f^j(z)$$

$$= \sum_{N=j}^{k} N c_N z^{N-1} + \sum_{N=j}^{k} N(N-1)c_N z^{N-2}$$

$$+ \sum_{N=j}^{k} N(N-1)(N-2)c_N z^{N-3} + \cdots$$

$$+ \sum_{N=j}^{k} N(N-1)(N-2)\ldots(N-j+1)c_N z^{N-j}$$

$$\sum_{n=1}^{j} f^n(z) = \sum_{N=j}^{k} N!\,c_N\left(\frac{z^{N-1}}{(N-1)!} + \frac{z^{N-2}}{(N-2)!} + \frac{z^{N-3}}{(N-3)!} + \cdots + \frac{z^{N-j}}{(N-j)!}\right)$$

$$= \sum_{N=j}^{k}\left(N!\,c_N \sum_{n=N-j}^{N-1} \frac{z^n}{n!}\right)$$

$$\sum_{n=1}^{j} f^n(z) = \sum_{N=j-(j-1)}^{k-(j-1)} \left([N+(j-1)]!\, c_{N+(j-1)} \sum_{n=N+(j-1)-j}^{N+(j-1)-1} \frac{z^n}{n!}\right)$$

$$= \sum_{N=1}^{k-j+1} \left((N+j-1)!\, c_{N+j-1} \sum_{n=(N+j-1)-(j+1)+1}^{(N+j-1)-1} \frac{z^n}{n!}\right)$$

$$= \sum_{l=1}^{k-j+1} (l+j-1)!\, c_{l+j-1} \sum_{n=l+(j-1)-(j+1)+1}^{l+(j-1)-1} \frac{z^n}{n!}$$

Reescribiendo

$$L = k - j + 1$$

$$N_l = l + (j-1)$$

$$K_{N_l} = (l+j-1)!\, c_{l+j-1}$$

$$p = j + 1$$

Se tiene que:

$$\sum_{n=1}^{j} f^n(z) = \sum_{l=1}^{L} \left(K_{N_l} \sum_{n=N_l-p+1}^{N_l-1} \frac{z^n}{n!}\right)$$

Lo que completa la prueba. □

Lema 2.2: Sean $g(z), h(z) \in D[z]$, entonces

$$(g(z)h(z))^n = \sum_{k=0}^{n} \binom{n}{k} g^{n-k}(z) h^k(z)$$

Prueba: (Por inducción).

Para $n = 1$

Sean $g(z) = \sum_{i=0}^{m} a_i x^i$ y $h(z) = \sum_{i=0}^{s} b_i x^i$. Entonces

$$g'(z) = \sum_{i=0}^{m-1}(i+1)a_{i+1}x^i \quad \text{y} \quad h'(z) = \sum_{i=0}^{s-1}(i+1)b_{i+1}x^i$$

$$(g(z)h(z))' = g'(z)h(z) + g(z)h'(z)$$

$$(g(z)h(z))' = \left(\sum_{i=0}^{m-1}(i+1)a_{i+1}x^i\right)h(z) + g(z)\left(\sum_{i=0}^{s-1}(i+1)b_{i+1}x^i\right)$$

$$(g(z)h(z))' = \left(\sum_{i=0}^{m-1}(i+1)a_{i+1}x^i\right)\left(\sum_{i=0}^{s}b_ix^i\right)$$

$$+\left(\sum_{i=0}^{m}a_ix^i\right)\left(\sum_{i=0}^{s-1}(i+1)b_{i+1}x^i\right)$$

$$= (a_1b_0 + b_1a_0) + (2a_1b_1 + 2a_2b_0 + 2b_2a_0)x + \cdots$$

$$+(m+s)(a_0b_{m+s} + a_1b_{m+s-1} + a_2b_{m+s-2+} \cdots +$$

$$a_{m+s}b_0)$$

$$= \sum_{j=0}^{m+s-1} d_jx^j$$

Donde $d_j = (j+1)\sum_{i=0}^{j+1} a_ib_{j+1-i}$

Por otra parte

$$g(z)h(z) = \left(\sum_{i=0}^{m} a_ix^i\right)\left(\sum_{i=0}^{s} b_ix^i\right)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_0b_{n+s} + a_1b_{n+s-1} + \cdots +$$

$$a_{n+s}b_0)x^{n+s}$$

$$= \sum_{j=0}^{n+s} c_jx^j$$

Donde $c_j = \sum_{i=0}^{j} a_ib_{j-i}$

Luego

$$(g(z)h(z))' = \sum_{j=0}^{m+s-1}(j+1)c_{j+1}x^j$$

$$= \sum_{j=0}^{m+s-1}\left((j+1)\sum_{i=0}^{j+1}a_i b_{j+1-i}\right)x^j$$

$$= \sum_{j=0}^{m+s-1}d_j x^j$$

Por lo tanto,

$$(g(z)h(z))' = g'(z)h(z) + g(z)h'(z)$$

$$= \binom{1}{0}g^{1-0}(z)h(z) + \binom{1}{1}g(z)h^1(z)$$

$$= \sum_{k=0}^{1}\binom{1}{k}g^{1-k}(z)h^k(z)$$

Supongamos que se tiene para n , Hipótesis de Inducción (H.I). Veámoslo para $n+1$.

En efecto:

$$\left(g(z)h(z)\right)^{n+1} = \left[\left(g(z)h(z)\right)^n\right]'$$

$$= \left[\sum_{k=0}^{n}\binom{n}{k}g^{n-k}(z)h^k(z)\right]' \text{ Por H.I.}$$

$$= \sum_{k=0}^{n}\binom{n}{k}\left(g^{n-k}(z)h^k(z)\right)'$$

$$= \sum_{k=0}^{n}\binom{n}{k}\left(g^{n-k+1}(z)h^k(z) + g^{n-k}(z)h^{k+1}(z)\right)$$

$$\left(g(z)h(z)\right)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} g^{n-k+1}(z)h^{k}(z) + \sum_{k=0}^{n} \binom{n}{k} g^{n-k}(z)h^{k+1}(z)$$

$$= \sum_{k=0}^{n} \binom{n}{k} g^{n+1-k}(z)h^{k}(z) + \sum_{k=1}^{n+1} \binom{n}{k-1} g^{n-k+1}(z)h^{k}(z)$$

$$= g^{n+1}(z)h^{0}(z) + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k}\right] g^{n+1-k}(z)h^{k}(z)$$

$$+g^{0}(z)h^{n+1}(z)$$

$$= g^{n+1}(z)h(z) + \sum_{k=1}^{n} \binom{n+1}{k} g^{n+1-k}(z)h^{k}(z) + g(z)h^{n+1}(z)$$

La última expresión se obtiene por (b), propiedad 2.1.

Finalmente se tiene que,

$$\left(g(z)h(z)\right)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} g^{n+1-k}(z)h^{k}(z) \square$$

Lema 2.3. Sean a, j enteros positivos y $f(z) = z^{j}(z-a)^{j+1} \in \mathbb{Z}[z]$, entonces,

$(a) f(z) = \sum_{n=j}^{2j+1} c_n z^n$

$(b) \sum_{n=1}^{j} f^{n}(a) = 0$

Prueba: Parte (a)

$$f(z) = z^{j}(z-a)^{j+1}$$

$$= z^{j} \sum_{n=0}^{j+1} \binom{j+1}{n} z^{j+1-n}(-a)^{n}$$

$$= z^{j}\left[\binom{j+1}{0} z^{j+1} + \binom{j+1}{1} z^{j}(-a) + \binom{j+1}{2} z^{j-1}(-a)^{2}\right.$$

$$\left. + \binom{j+1}{3} z^{j-2}(-a)^{3} + \cdots + \binom{j+1}{j+1}(-a)^{j+1}\right]$$

$$f(z) = \binom{j+1}{0} z^{2j+1} + \binom{j+1}{1} z^{2j}(-a) + \binom{j+1}{2} z^{2j-1}(-a)^2 + \cdots$$

$$+ \binom{j+1}{j+1} z^{j}(-a)^{j+1}$$

$$f(z) = \binom{j+1}{j+1} z^{j}(-a)^{j+1} + \binom{j+1}{j} z^{j+1}(-a)^{j} + \cdots + \binom{j+1}{2} z^{2j-1}(-a)^2$$

$$+ \binom{j+1}{1} z^{2j}(-a) + \binom{j+1}{0} z^{2j+1}$$

$$f(z) = \sum_{n=j}^{2j+1} \binom{j+1}{2j+1-n} z^{n}(-a)^{2j+1-n}$$

$$= \sum_{n=j}^{2j+1} c_n z^n$$

Donde $c_n = \binom{j+1}{2j+1-n}(-a)^{2j+1-n}$, lo que prueba la parte (a)

Parte (b)

Si $z = a$ se tiene que:

$$\sum_{n=1}^{j} f^{n}(a) = f^{1}(a) + f^{2}(a) + \cdots + f^{j}(a)$$

Ahora como $f(z) = z^j(z-a)^{j+1}$. Al tomar $g(z) = z^j$ y $h(z) = (z-a)^{j+1}$, por el lema 2.2:

$$\sum_{n=1}^{j} f^{n}(a) = \sum_{k=0}^{1} \binom{1}{k} g^{1-k}(a)h^{k}(a) + \sum_{k=0}^{2} \binom{2}{k} g^{2-k}(a)h^{k}(a) + \cdots$$

$$+ \sum_{k=0}^{j} \binom{j}{k} g^{j-k}(a)h^{k}(a)$$

$$\sum_{n=1}^{j} f^{n}(a) = \binom{1}{0} g^{1}(a)h(a) + \binom{1}{1} g(a)h^{1}(a) + \binom{2}{o} g^{2}(a)h(a)$$

$$+ \binom{2}{1} g^{1}(a)h^{1}(a) + \binom{2}{2} g(a)h^{2}(a) + \cdots$$

$$+ \binom{j}{0} g^{j}(a)h(a) + \binom{j}{1} g^{j-1}(a)h^{1}(a) + \cdots$$

$$+ \binom{j}{j} g(a)h^{j}(a)$$

$$\textstyle\sum_{n=1}^{j} f^{n}(a) = \binom{1}{0} ja^{j-1}(a-a)^{j+1} + \binom{1}{1} a^{j}(j+1)(a-a)^{j}$$

$$+ \binom{2}{0} j(j-1)a^{j-2}(a-a)^{j+1} + \binom{2}{1} ja^{j-1}(j+1)(a-a)^{j}$$

$$+ \binom{2}{2} a^{j}(j+1)j(a-a)^{j-1} + \cdots + \binom{j}{0} [j(j-1)(j-2)\ldots 1](a-a)^{j+1}$$

$$+ \binom{j}{1} [j(j-1)(j-2)\ldots 2]a(j+1)(a-a)^{j} + \cdots$$

$$+ \binom{j}{j} a^{j}[(j+1)j(j-1)\ldots 2](a-a)$$

Por lo tanto;

$$\textstyle\sum_{n=1}^{j} f^{n}(a) = 0 \square$$

OBSERVACIÓN 2.1: El resultado del Lema 2.3 lo podemos generalizar, es decir, si $f(z) = z^{p-1}(z-1)^p(z-2)^p \dots (z-d)^p$, entonces; empleando reiteradamente el Teorema del Binomio de Newton se demuestra que:

$$f(z) = \sum_{N=p-1}^{(d+1)p-1} c_N z^N$$

Y utilizando el Lema 2.2 obtenemos que para $t = 1,2,3,\dots,d$

$$\sum_{n=1}^{p-1} f^n(t) = 0$$

Lema 2.4. Dado $f(z) = z^{p-1}(z-a)^p = \sum_{N=p-1}^{2p-1} c_N z^N$, donde $a \in \mathbb{Z}^+$:

$$\sum_{N=p-1}^{2p-1} |c_N| = (1+a)^p$$

Prueba:

$$f(z) = z^{p-1}(z-a)^p$$

$$= z^{p-1}\left[\binom{p}{0} z^p + \binom{p}{1} z^{p-1}(-a) + \cdots + \binom{p}{p}(-a)^p\right]$$

$$= \binom{p}{0} z^{2p-1} + \binom{p}{1} z^{2p-2}(-a) + \binom{p}{2} z^{2p-3}(-a)^2 + \cdots + \binom{p}{p} z^{p-1}(-a)^p$$

$$= \binom{p}{p}(-a)^p z^{p-1} + \binom{p}{p-1}(-a)^{p-1} z^p + \cdots + \binom{p}{1}(-a) z^{2p-2} + \binom{p}{0} z^{2p-1}$$

$$= \binom{p}{0}(-a)^p z^{p-1} + \binom{p}{1}(-a)^{p-1} z^p + \cdots + \binom{p}{p-1}(-a) z^{2p-2} + \binom{p}{p} z^{2p-1}$$

Luego,

$$\sum_{N=p-1}^{2p-1}|c_N| = |c_{p-1}| + |c_p| + \cdots + |c_{2p-1}|$$

$$= \left|\binom{p}{0}(-a)^p\right| + \left|\binom{p}{1}(-a)^{p-1}\right| + \cdots + \left|\binom{p}{p}(-a)^0\right|$$

$$\sum_{N=p-1}^{2p-1}|c_N| = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p}a^0$$

$$= \sum_{k=0}^{p}\binom{p}{k}a^{p-k}$$

$$= (a+1)^p \ \square$$

Lema 2.5. Sea $(z-t)^p = \sum_{n=0}^{p}\binom{p}{n}(-t)^{p-n}z^n$ para enteros $t = 1,2,3,\dots,d$

Pruebe que:

(a) $\max\limits_{n=0,1,\dots,p}\left\{\left|\binom{p}{n}(-t)^{p-n}\right|\right\} \le t^p\sum_{n=0}^{p}\binom{p}{n} = (2t)^p$

(b) $\prod_{t=1}^{d}\left(\max\limits_{n=0,1,\dots,p}\left\{\left|\binom{p}{n}(-t)^{p-n}\right|\right\}\right) \le \prod_{t=1}^{d}(2t)^p$

Prueba:

Parte (a).

$$\max_{n=0,1,\dots,p}\left\{\left|\binom{p}{n}(-t)^{p-n}\right|\right\} = max\left\{\left|\binom{p}{0}(-t)^p\right|, \left|\binom{p}{1}(-t)^{p-1}\right|, \dots, \left|\binom{p}{p}(-t)^0\right|\right\}$$

$$= max\left\{\binom{p}{o}t^p, \binom{p}{1}t^{p-1}, \dots, \binom{p}{p}\right\}$$

$$\le t^p\sum_{n=0}^{p}\binom{p}{n}$$

Ahora del Binomio de Newton

$$(x+y)^p = \sum_{n=0}^{p} \binom{p}{n} x^{p-n} y^n$$

Si $x = y = 1$

$$2^p = \sum_{n=0}^{p} \binom{p}{n}$$

Por lo tanto,

$$\max_{n=0,1,\ldots,p} \left\{ \left| \binom{p}{n} (-t)^{p-n} \right| \right\} \leq t^p \sum_{n=0}^{p} \binom{p}{n} = (2t)^p$$

La parte (b) se deduce de (a)□

Lema 2.6: Sea $\mathcal{P}(z) \in \mathbb{Z}[z]$ y $gr(\mathcal{P}) = d$. Entonces,

$$\mathcal{P}\left(\sqrt{\frac{a}{b}}\right) + \mathcal{P}\left(-\sqrt{\frac{a}{b}}\right)$$

es un número racional, que puede escribirse con denominador b^d.

Prueba:

Sea $\mathcal{P}(z) = \sum_{n=0}^{d} r_n z^n \in \mathbb{Z}[z]$, $r_d \neq 0$ y d par. Entonces,

$$\mathcal{P}\left(\sqrt{\frac{a}{b}}\right) = r_0 + r_1\sqrt{\frac{a}{b}} + r_2\left(\sqrt{\frac{a}{b}}\right)^2 + r_3\left(\sqrt{\frac{a}{b}}\right)^3 + \cdots + r_{d-1}\left(\sqrt{\frac{a}{b}}\right)^{d-1} + r_d\left(\sqrt{\frac{a}{b}}\right)^d$$

$$\mathcal{P}\left(-\sqrt{\frac{a}{b}}\right) = r_0 - r_1\sqrt{\frac{a}{b}} + r_2\left(\sqrt{\frac{a}{b}}\right)^2 - r_3\left(\sqrt{\frac{a}{b}}\right)^3 + \cdots - r_{d-1}\left(\sqrt{\frac{a}{b}}\right)^{d-1} + r_d\left(\sqrt{\frac{a}{b}}\right)^d$$

Luego,

$$\mathcal{P}\left(\sqrt{\frac{a}{b}}\right)+\mathcal{P}\left(-\sqrt{\frac{a}{b}}\right)=2r_0+2r_2\left(\sqrt{\frac{a}{b}}\right)^2+\cdots+2r_d\left(\sqrt{\frac{a}{b}}\right)^d$$

$$=2r_0+2r_2\frac{a}{b}+\cdots+2r_d\frac{a^{\frac{d}{2}}}{b^{\frac{d}{2}}}$$

$$2r_0+2r_2\frac{a}{b}+\cdots+2r_d\frac{a^{\frac{d}{2}}}{b^{\frac{d}{2}}}=\frac{2r_0(b)^{\frac{d}{2}}+2r_2a(b)^{\frac{d}{2}-1}+\cdots+2r_{d-2}(a)^{\frac{d-2}{2}}b+2r_d(a)^{\frac{d}{2}}}{(b)^{\frac{d}{2}}}$$

$$=\frac{2r_0b^d+2r_2a(b)^{d-1}+\cdots+2r_{d-2}(a)^{\frac{d-2}{2}}(b)^{\frac{d+2}{2}}+2r_d(a)^{\frac{d}{2}}(b)^{\frac{d}{2}}}{b^d}\in\mathbb{Q}$$

Por la propiedad 2.2.

Si d es impar

$$\mathcal{P}\left(\sqrt{\frac{a}{b}}\right)+\mathcal{P}\left(-\sqrt{\frac{a}{b}}\right)=2r_0+2r_2\left(\sqrt{\frac{a}{b}}\right)^2+\cdots+2r_{d-1}\left(\sqrt{\frac{a}{b}}\right)^{d-1}$$

$$=\frac{2r_0(b)^{\frac{d-1}{2}}+2r_2a(b)^{\frac{d-3}{2}}+\cdots+2r_{d-1}(a)^{\frac{d-1}{2}}}{(b)^{\frac{d-1}{2}}}$$

$$=\frac{2r_0(b)^d+2r_2a(b)^{d-1}+\cdots+2r_{d-1}(a)^{\frac{d-1}{2}}(b)^{\frac{d+1}{2}}}{b^d}\in\mathbb{Q}$$

De nuevo por la propiedad 2.2.□

2.3. Sumas Exponenciales Conjugadas Completas

Definición 2.1: Conjugados

Sea α un número algebraico. Las raíces del polinomio mínimo para α son llamados los conjugados de α.

Ejemplo 2.1:

$\alpha_1 = \sqrt{1+\sqrt{3}}$ es algebraico, con polinomio mínimo $p(x) = x^4 - 2x^2 - 2$. Luego los conjugados de α_1 son:

$$\alpha_1 = \sqrt{1+\sqrt{3}}, \qquad \alpha_2 = -\sqrt{1+\sqrt{3}}, \qquad \alpha_3 = i\sqrt{-1+\sqrt{3}},$$

$$\alpha_4 = -i\sqrt{-1+\sqrt{3}}$$

Definición 2.2: *Conjunto completo de conjugados.*

Se dice que un conjunto finito de números algebraicos S es *un conjunto completo de conjugados* si para todo $\alpha \in S$, S contiene todos los conjugados de α y en caso de que α aparezca *m-veces, también* cada uno de sus conjugados debe aparecer *m-veces.*

Ejemplo 2.2:

$\left\{\sqrt{1+\sqrt{3}}, -\sqrt{1+\sqrt{3}}, i\sqrt{-1+\sqrt{3}}, -i\sqrt{-1+\sqrt{3}}\right\}$, por el ejemplo anterior es un conjunto de conjugados, por lo tanto es un *conjunto completo de conjugados.*

Ejemplo 2.3:

$\{2\sqrt{2}, -2\sqrt{2}, 2\sqrt{3}, -2\sqrt{3}\}$ es un *conjunto completo de conjugados.* Vemos que $2\sqrt{2}, -2\sqrt{2}$ son conjugados, con polinomio mínimo $p(x) = x^2 - 8$; y $2\sqrt{3}, -2\sqrt{3}$ también son conjugados, con polinomio mínimo $q(x) = x^2 - 12$.

Ejemplo 2.4

$\{2\sqrt{2}, -2\sqrt{2}, 2\sqrt{3}, -2\sqrt{3}, -2\sqrt{2}\}$ no es un *conjunto completo de conjugados.* Vemos que $-2\sqrt{2}$ aparece dos veces, sin embargo su conjugado $2\sqrt{2}$ sólo una vez.

Definición 2.3: Una suma finita de términos exponenciales $e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_L}$ se dice que es una suma exponencial conjugada completa si la colección de los exponentes $\{\alpha_1, \alpha_2, \ldots, \alpha_L\}$ es un ***conjunto completo de conjugados.***

Lema 2.7: Sea $\rho_1, \rho_2, \ldots, \rho_L, \tau_1, \tau_2, \ldots, \tau_M$ números complejos distintos y sea $r_1, r_2, \ldots, r_L, t_1, t_2, \ldots, t_M$ números complejos no nulos. Si el producto

$$(\textstyle\sum_{l=1}^{L} r_l e^{\rho_l})(\sum_{m=1}^{M} t_m e^{\tau_m})$$

Es expandido e iguales términos exponenciales son combinados, entonces el resultado es una expresión de la forma

$$\textstyle\sum_{n=1}^{N} s_n e^{\omega_n},$$

para algún entero positivo *N*, distintos exponentes de la forma $\omega_n = \rho_l + \tau_m$ y números complejos s_n, donde al menos uno de estos números complejos s_n es distinto de cero.

Prueba:

Es claro que:

(2.5) $$(\textstyle\sum_{l=1}^{L} r_l e^{\rho_l})(\sum_{m=1}^{M} t_m e^{\tau_m}) = \sum_{\substack{1\le l\le L \\ 1\le m\le M}} r_l t_m e^{\rho_l+\tau_m}$$

Sea $H = \{\rho_l + \tau_m \,/ 1 \le l \le L, 1 \le m \le M\}$. Entonces H tiene más de un elemento, luego podemos escribir

$$H = \{\omega_1, \omega_2, \ldots, \omega_N\}$$

Para distintos $\omega_n \in \mathbb{C}$ y algún $N \in \mathbb{N}$.

Si $s_n = \sum r_l t_m$; l, m tal que $\rho_l + \tau_m = \omega_n$. Entonces podemos escribir (2.5) como sigue

$$\left(\sum_{l=1}^{L} r_l e^{\rho_l}\right)\left(\sum_{m=1}^{M} t_m e^{\tau_m}\right) = \sum_{n=1}^{N} s_n e^{\omega_n}$$

Donde al menos uno de los s_n no es cero. Para probar esta afirmación sea $\rho_l = a_l + ib_l$, $l = 1,2, \dots, L$ y consideremos:

$$\{\rho_{l_1}, \dots, \rho_{l_K}\} \subset \{\rho_1, \rho_2, \dots, \rho_L\}$$

el subconjunto con parte real máxima, es decir,

$$\rho_{l_k} = a + ib_{l_k}, 1 \leq k \leq K \quad \text{y},$$

$$a \geq a_l, l = 1,2, \dots, L$$

Tomemos ahora $b = máx\{b_{l_k}, 1 \leq k \leq K\}$. Entonces para un l_φ, $1 \leq \varphi \leq K$, $\rho_{l_\varphi} = a + ib$ es único, pues en particular los ρ_{l_k} son distintos.

Si procedemos de forma análoga para $\{\tau_1, \dots, \tau_M\}$ se tiene que hay un único $\tau_{m_\theta} = c + id \in \{\tau_{m_1}, \dots, \tau_{m_J}\} \subset \{\tau_1, \dots, \tau_M\}$

Ahora se tiene que $\omega_n = \rho_{l_\varphi} + \tau_{m_\theta}$ se obtiene de manera única de la suma de ρ_{l_φ} y τ_{m_θ}; pues si hay algún ρ_l y algún τ_m distintos de ρ_{l_φ} y τ_{m_θ}, respectivamente, tal que $\omega_n = \rho_l + \tau_m$, entonces

$$Re\left(\rho_{l_\varphi} + \tau_{m_\theta}\right) = Re(\rho_l + \tau_m)$$

$$Im\left(\rho_{l_\varphi} + \tau_{m_\theta}\right) = Im(\rho_l + \tau_m)$$

Lo cual contradice la condición de parte real e imaginaria máxima de ρ_{l_φ} y τ_{m_θ}. De donde $e^{\rho_{l_\varphi}+\tau_{m_\theta}}$ tiene un coeficiente único $s_{l_\varphi,m_\theta} = r_{l_\varphi} t_{m_\theta}$, el cual es distinto de cero por hipótesis.□

Lema 2.8: El conjunto $\{\alpha_1, \alpha_2, \dots, \alpha_L\}$ es *un conjunto completo de conjugados* si y sólo si el polinomio $(z-\alpha_1)(z-\alpha_2)\dots(z-\alpha_L)$ tiene coeficientes racionales.

Prueba:

Sea $\{\alpha_1, \alpha_2, \dots, \alpha_L\}$ un conjunto completo de conjugados. Reagrupemos los conjuntos de conjugados

$$\alpha_{11}, \alpha_{12}, \dots, \alpha_{1M_1}, \qquad \alpha_{21}, \dots, \alpha_{2M_2}, \qquad \dots\dots, \qquad \alpha_{L1}, \dots, \alpha_{LM_L}$$

Sea $f_l(z) = (z-\alpha_{l1})(z-\alpha_{l2})\dots(z-\alpha_{lM_l}), l = 1,2,\dots L$. Entonces f_l es el polinomio mínimo para el conjunto de conjugados $\{\alpha_{l1}, \alpha_{l2}, \dots, \alpha_{lM_l}\}$, luego $f_l(z) \in \mathbb{Q}[z]$. Por lo tanto,

$$\prod_{l=1}^{L} f_l(z) = (z-\alpha_1)(z-\alpha_2)\dots(z-\alpha_L) \in \mathbb{Q}[z]$$

Supongamos ahora que

$$f(z) = (z-\alpha_1)(z-\alpha_2)\dots(z-\alpha_L) \in \mathbb{Q}[z]$$

Si algún o algunos α_l son racionales, estos formarán un conjunto completo de conjugados, digamos $\{\alpha_l / K+1 \le l \le L\}$. Entonces,

$$(2.6) \qquad f(z) = \underbrace{(z-\alpha_1)(z-\alpha_2)\dots(z-\alpha_K)}_{g(z)}(z-\alpha_{K+1})\dots(z-\alpha_L)$$

Es claro que $g(z)=(z-\alpha_1)(z-\alpha_2)\dots(z-\alpha_K)\in\mathbb{Q}[z]$. Si g es irreducible, entonces es el polinomio mínimo para $\alpha_1,\dots,\alpha_K$ y por ende $\{\alpha_1,\dots,\alpha_K\}$ es un conjunto completo de conjugados. Luego $\{\alpha_1,\dots,\alpha_K\}\cup\{\alpha_l/K+1\leq l\leq L\}$ es un conjunto completo de conjugados.

Si g es reducible, entonces:

$$g=p_1^{i_1}\dots p_J^{i_J}$$

donde cada $p_j\in\mathbb{Q}[z]$ es irreducible y $i_j\geq 1$. Por (2.6)

$$p_j(z)=(z-\alpha_{j1})(z-\alpha_{j2})\dots\left(z-\alpha_{jK_j}\right)$$

Se tiene que $p_j\in\mathbb{Q}[z]$ es el polinomio mínimo para $\alpha_{j1},\dots,\alpha_{jK_j}$, luego $\left\{\alpha_{j1},\dots,\alpha_{jK_j}\right\}$ es un conjunto completo de conjugados.

Como

$$\{\alpha_1,\dots,\alpha_K\}=\bigcup_{j=1}^{J}\bigcup_{\mu=1}^{i_J}\{\alpha_{j1},\dots,\alpha_{Kj}\}$$

Se tiene que $\{\alpha_1,\dots,\alpha_K\}$ es un conjunto completo de conjugados, por ser la unión de conjuntos completos de conjugados; y por la misma razón

$\{\alpha_1,\dots,\alpha_K\}\cup\{\alpha_l/K+1\leq l\leq L\}$ es un conjunto completo de conjugados.□

2.4. Polinomios Simétricos.

Antes de presentar algunos resultados sobre polinomios simétricos, es necesario generalizar la definición 1.1 a varias indeterminadas.

Definición 2.4: Sean $L \in \mathbb{Z}^+$, $\check{n}' = (n'_1, n'_2, \dots, n'_L)$ y $\check{n} = (n_1, n_2, \dots, n_L)$ elementos de $\mathbb{N}^L$. Diremos que $\check{n}' < \check{n}$, si para la primera l tal que $n'_l \neq n_l$, se tiene que $n'_l < n_l$.

Observación 2.2: Para cualesquiera $\check{n}, \check{n}' \in \mathbb{N}^L$, se tiene que $\check{n} = \check{n}', \check{n} < \check{n}'$, o $\check{n}' < \check{n}$, por lo tanto $(\mathbb{N}^L, \leq)$ está totalmente ordenado. También por simple inspección se tiene que para $\check{n}, \check{n}', \check{n}'' \in \mathbb{N}^L$; si

$$\check{n} < \check{n}' \Rightarrow \check{n} + \check{n}'' < \check{n}' + \check{n}''$$

Definición 2.5: Llamaremos anillo de los polinomios sobre $\mathbb{Q}$ (ò $\mathbb{Z}$) en las indeterminadas $z_1, z_2, \dots, z_L$ y lo denotaremos $\mathbb{Q}[z_1, z_2, \dots, z_L]$ (ó $\mathbb{Z}[z_1, z_2, \dots, z_L]$) a la colección

$$\sum_{n_1=0}^{\varepsilon_1} \cdots \sum_{n_L=0}^{\varepsilon_L} c_{(n_1,n_2,\dots,n_L)} z_1^{n_1} \dots z_L^{n_L}$$

Donde:

(i) $z_i^0 = 1, \forall i = \{1,2, \dots, L)$

(ii) $\varepsilon_l \in \mathbb{Z}^+, \forall l = \{1,2, \dots, L)$

(iii) $c_{(n_1,\dots,n_L)} \in \mathbb{Q}$ (o $\mathbb{Z}$, respectivamente); $\forall, 0 \leq n_l \leq \varepsilon_l$

(iv) Si $f(z_1, z_2, \dots, z_L) = \sum_{n_1=0}^{\varepsilon_1} \cdots \sum_{n_L=0}^{\varepsilon_L} c_{(n_1,\dots,n_L)} z_1^{n_1} \dots z_L^{n_L}$, con $c_{(\varepsilon_1,\dots,\varepsilon_L)} \neq 0$

$g(z_1, z_2, \dots, z_L) = \sum_{n'_1=0}^{\mu_1} \cdots \sum_{n'_L=0}^{\mu_L} b_{(n'_1,\dots,n'_L)} z_1^{n'_1} \dots z_L^{n'_L}$, con $b_{(\mu_1,\dots,\mu_L)} \neq 0$

Son elementos de $\mathbb{Q}[z_1, z_2, \dots, z_L]$ (ó $\mathbb{Z}[z_1, z_2, \dots, z_L]$), entonces $f = g$, si y solo si, $\varepsilon_l = \mu_l$, $\forall l = \{1, \dots, L\}$; y $c_{(n_1,\dots,n_L)} = b_{(n'_1,\dots,n'_L)}$, $\forall 0 \leq n_l \leq \varepsilon_l$, $\forall 0 \leq n'_l \leq \mu_l$

Observación 2.3: En algunos casos simplificaremos $p(z_1, z_2, \dots, z_L)$ por simplemente p y

$p(z_1, z_2, \dots, z_L) = \sum_{n_1=0}^{\varepsilon_1} \cdots \sum_{n_L=0}^{\varepsilon_L} c_{(n_1,\dots,n_L)} z_1^{n_1} \dots z_L^{n_L}$ por $p = \sum_{\check{n}} c_{\check{n}} Z^{\check{n}}$, donde $Z^{\check{n}} = z_1^{n_1} \dots z_L^{n_L}$ para $\check{n} = (n_1, n_2, \dots, n_L)$.

Definición 2.6: Sea $p(z_1, z_2, \dots, z_L) = \sum_{n_1=0}^{\varepsilon_1} \cdots \sum_{n_L=0}^{\varepsilon_L} c_{(n_1,\dots,n_L)} z_1^{n_1} \dots z_L^{n_L}$ un polinomio no nulo en $\mathbb{Q}[z_1, z_2, \dots, z_L]$. Entonces,

(i) El multigrado de p, denotado por $mgr(p)$, está dado por

$$mgr(p) = max\{(n_1, \dots, n_L) \in \mathbb{N}^L / \, c_{(n_1,\dots,n_L)} \neq 0\}$$

(ii) El coeficiente principal de p, denotado por $C(p)$, está dado por

$$C(p) = c_{mgr(p)} \in \mathbb{Q}$$

(iii) El monomio principal de p, denotado por $M(p)$, está dado por

$$M(p) = Z^{mgr(p)}$$

(iv) El término principal de p, denotado por $T(p)$, está dado por

$$T(p) = C(p)M(p)$$

Definición 2.7: Un polinomio $f(z_1, z_2, \dots, z_L) \in \mathbb{Q}[z_1, z_2, \dots, z_L]$ es simétrico si

$$f(z_{\tau(1)}, \dots, z_{\tau(L)}) = f(z_1, \dots, z_L)$$

Para todas las posibles permutaciones $z_{\tau(1)}, \dots, z_{\tau(L)}$; de las variables $z_1, \dots, z_L$.

Definición 2.8: (Orden monomial en $\mathbb{Q}[z_1, z_2, \dots, z_L]$)

Supongamos que $\mathcal{M} = c z_1^{n_1} \dots z_L^{n_L}$ y $\mathcal{M}' = c' z_1^{n_1'} \dots z_L^{n_L'}$ son dos monomios en $\mathbb{Q}[z_1, z_2, \dots, z_L]$,con la posibilidad de que todos o algunos de los exponentes son iguales. Se dice que el monomio $\mathcal{M}'$ es menor que el monomio $\mathcal{M}$ (o que $\mathcal{M}$ es superior a $\mathcal{M}'$) y lo denotaremos $\mathcal{M}' < \mathcal{M}$ si: $(n_1', n_2', \dots, n_L') < (n_1, n_2, \dots, n_L)$.

Definición 2.9: Dadas las variables $z_1, \dots, z_L$. Se definen los polinomios $\sigma_1, \sigma_2, \dots, \sigma_L \in \mathbb{Q}[z_1, z_2, \dots, z_L]$ por:

$$\sigma_1(z_1, \dots, z_L) = z_1 + z_2 + \cdots + z_L$$

$$\sigma_2(z_1, \dots, z_L) = z_1z_2 + z_1z_3 + \cdots + z_1z_L + z_2z_3 + \cdots + z_2z_L + \cdots + z_{L-1}z_L$$

$$\vdots$$

$$\sigma_l(z_1, \dots, z_L) = \sum_{\tau(1)<\cdots<\tau(l)} z_{\tau(1)} \dots z_{\tau(l)}$$

$$\vdots$$

$$\sigma_L(z_1, \dots, z_L) = z_1z_2 \dots z_L$$

Observación 2.4: De la definición anterior se desprende que σ_l es un polinomio simétrico para todo $l = 1, \dots, L$; y diremos que $\{\sigma_1, \dots, \sigma_L\}$ son los polinomios simétricos elementales de $\mathbb{Q}[z_1, \dots, z_L]$.

Ejemplo 2.5: Dado el ordenamiento de monomios, $M(\sigma_l) = z_1 \dots z_l$; ya que de la definición 2.6.

$$mgr(\sigma_1) = \Big(1, \underbrace{0,0 \dots 0}_{L-1}\Big), \qquad mgr(\sigma_2) = \Big(1,,1, \underbrace{0,\dots,0}_{L-2}\Big), \dots, \qquad mgr(\sigma_l) = \Big(\underbrace{1,\dots,1}_{l-veces}, \underbrace{0,\dots,0}_{L-l}\Big), \dots, mgr(\sigma_L) = \Big(\underbrace{1,1,\dots,1}_{L-veces}\Big)$$

Por lo tanto $\quad M(\sigma_l) = z_1 \dots z_l \quad$ y $C(\sigma_l) = 1$.

Lema 2.9: Para polinomios no nulos $f, g \in \mathbb{Q}[z_1, z_2, \dots, z_L]$.

$$mgr(fg) = mgr(f) + mgr(g) \quad \text{y}$$

$$C(fg) = C(f)C(g)$$

Prueba:

Supongamos que $mgr(f) = \check{n}$ y $mgr(g) = \check{n}'$, es decir,

$$f = c_{\check{n}} Z^{\check{n}} + \textstyle\sum_{i<\check{n}} c_i Z^i \quad \text{con } c_{\check{n}} \neq 0$$

$$g = c'_{\check{n}'} Z^{\check{n}'} + \textstyle\sum_{j<\check{n}'} c_j Z^j \quad \text{con } c'_{\check{n}'} \neq 0$$

Multiplicando término a término, fg tiene un término no nulo

$$c_{\check{n}} c'_{\check{n}'} Z^{\check{n}+\check{n}'}$$

Todos los otros términos tienen multigrado de la forma.

$$\check{n} + j, i + \check{n}' \text{ ó } i + j$$

Como $i < \check{n}$ y $j < \check{n}'$, todos estos términos tienen multigrado menor que $\check{n} + \check{n}'$

Luego

$$mgr(fg) = mgr(f) + mgr(g) \quad \text{y} \quad C(fg) = C(f)C(g)$$

Lema 2.10: Sea $p(z_1, z_2, \dots, z_L)$ un polinomio simétrico. Si $\mathcal{M} = cz_1^{n_1} \dots z_L^{n_L}$ es el término principal de p, entonce

$$n_L \leq n_{L-1} \leq \cdots \leq n_2 \leq n_1$$

Prueba:

Sea $\check{n} = (n_1, n_2, \dots, n_L)$ el multigrado de $\mathcal{M}$, como p es simétrico $\mathcal{M}' = c z_{\tau(1)}^{n_1} z_{\tau(2)}^{n_2} \dots z_{\tau(L)}^{n_L}$ es un término de p, de donde $\left(n_{\tau(1)}, n_{\tau(2)}, \dots n_{\tau(l)}\right)$ es el multigrado de algún monomio no cero de p. Ya que $(n_1, n_2, \dots, n_L)$ es el máximo de los multigrado de todos los monomios de p; $(n_1, n_2, \dots, n_L)$ es el máximo en $\mathbb{N}^L$, para todas las permutaciones no triviales, de donde,

$$n_L \leq n_{L-1} \leq \cdots \leq n_2 \leq n_1$$

Lema 2.11: $T\left(\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_L^{n_L}\right) = z_1^{n_1+n_2+\cdots+n_L} z_2^{n_2+n_3+\cdots+n_L} \dots z_L^{n_L}$

Prueba:

Del ejemplo 2.5 y el lema 2.9, para enteros no negativos $n_1, \dots, n_L$

$mgr\left(\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_L^{n_L}\right) = (n_1 + n_2 + \cdots + n_L, n_2 + n_3 + \cdots + n_L, \dots, n_L)$ y

$$C\left(\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_L^{n_L}\right) = 1$$

Por lo tanto,

$$T\left(\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_L^{n_L}\right) = z_1^{n_1+n_2+\cdots+n_L} z_2^{n_2+n_3+\cdots+n_L} \dots z_L^{n_L}$$

Teorema 2.1: Todo polinomio simétrico en $\mathbb{Q}[z_1, z_2, \dots, z_L]$, es un polinomio en los polinomios simétricos elementales con coeficientes racionales. Esto es; si $p(z_1, z_2, \dots, z_L) \in \mathbb{Q}[z_1, z_2, \dots, z_L]$ es un polinomio simétrico, entonces existe un polinomio f con coeficientes racionales tal que:

$$p(z_1, z_2, \dots, z_L) = f(\sigma_1, \sigma_2, \dots, \sigma_L)$$

Y $mgr(f) \leq mgr(p)$

Prueba:

La prueba será por inducción en el multigrado del polinomio.

Un polinomio en $\mathbb{Q}[z_1, z_2, ..., z_L]$ con multigrado $(0,0,...,0)$está en $\mathbb{Q}$, y $\mathbb{Q} \subset \mathbb{Q}[\sigma_1, \sigma_2, ..., \sigma_L]$.

Sea $\check{n} = (n_1, n_2, ..., n_L) \neq (0,0,...,0)$ en $\mathbb{N}^L$ y supongamos que el lema es válido para todo polinomio simétrico con multigrado menor que $\check{n}$.

Si $p(z_1, z_2, ..., z_L) \in \mathbb{Q}[z_1, z_2, ..., z_L]$ es un polinomio simétrico tal que $mgr(p) = \check{n}$, entonces

$$p = c_{\check{n}} z_1^{n_1} \dots z_L^{n_L} + \sum_{\check{n}' < \check{n}} c_{\check{n}'} Z^{\check{n}'}$$

Donde $c_{\check{n}} \neq 0$.

Consideremos

$$p - c_{\check{n}} \sigma_1^{n_1 - n_2} \sigma_2^{n_2 - n_3} \dots \sigma_{L-1}^{n_{L-1} - n_L} \sigma_L^{n_L} \tag{2.7}$$

Por el lema 2.11, $T\left(c_{\check{n}} \sigma_1^{n_1 - n_2} \sigma_2^{n_2 - n_3} \dots \sigma_{L-1}^{n_{L-1} - n_L} \sigma_L^{n_L}\right) = c_{\check{n}} z_1^{n_1} \dots z_L^{n_L}$, el cual se simplifica con el término superior de p.

Si $p = c_{\check{n}} \sigma_1^{n_1 - n_2} \dots \sigma_L^{n_L}$, no hay nada que probar. En caso contario (2.7) es simétrico, ya que ambos términos en la diferencia son simétricos y

$$mgr\left(p - c_{\check{n}} \sigma_1^{n_1 - n_2} \dots \sigma_L^{n_L}\right) < \check{n}.$$

Por la hipótesis de inducción

$$p - c_{\check{n}} \sigma_1^{n_1 - n_2} \dots \sigma_L^{n_L} \in \mathbb{Q}[\sigma_1, \sigma_2, ..., \sigma_L]$$

Luego existe $g(\sigma_1, \sigma_2, ..., \sigma_L) \in \mathbb{Q}[\sigma_1, \sigma_2, ..., \sigma_L]$, tal que

$$p - c_{\check{n}}\sigma_1^{n_1-n_2}\dots\sigma_L^{n_L} = g(\sigma_1, \sigma_2, \dots, \sigma_L)$$

$$p = g(\sigma_1, \sigma_2, \dots, \sigma_L) + c_{\check{n}}\sigma_1^{n_1-n_2}\dots\sigma_L^{n_L}$$

$$p = f(\sigma_1, \sigma_2, \dots, \sigma_L)$$

Donde $$mgr(f) \leq mgr(p)\square$$

Observación 2.5: En vista de que en la prueba del teorema 2.1 no se llegó a dividir entre los elementos de $\mathbb{Q}$, el teorema es válido si se reemplaza $\mathbb{Q}$ por $\mathbb{Z}$.

El siguiente lema generaliza el lema 2.6

Lema 2.12: Sea $G(z) \in \mathbb{Z}[z]$ dado por $G(z) = \sum_{l=0}^{L} a_l z^l$ y; $\alpha_1, \alpha_2, \dots, \alpha_L$ las raíces de $G(z)$. Sea $\mathcal{P}(z)$ un polinomio con coeficientes enteros. Entonces,

$$\mathcal{P}(\alpha_1) + \mathcal{P}(\alpha_2) + \cdots + \mathcal{P}(\alpha_L)$$

es un número racional con denominador igual a ${a_L}^{gr(\mathcal{P})}$.

Prueba:

Sea

$$P(x_1, x_2, \dots, x_L) = \mathcal{P}(x_1) + \mathcal{P}(x_2) + \cdots + \mathcal{P}(x_L)$$

Es claro que P es simétrico; entonces, por el Teorema 2.1, podemos escribirlo en término de los polinomios simétricos elementales $\sigma_1, \sigma_2, \dots, \sigma_L$ en $x_1, x_2, \dots, x_L$; es decir

$$P(x_1, x_2, \dots, x_L) = F(\sigma_1, \sigma_2, \dots, \sigma_L)$$

Donde F es un polinomio con coeficientes enteros. Luego $P(\alpha_1, \alpha_2, \dots, \alpha_L)$ es un polinomio en

(2.8) $\quad \alpha_1 + \alpha_2 + \cdots + \alpha_L,\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{L-1}\alpha_L,\ \dots,\ \alpha_1\alpha_2\dots\alpha_L$

Ahora

$$\begin{aligned} G(z) &= a_L z^L + a_{L-1}z^{L-1} + \cdots + a_1 z + a_0 \\ &= a_L\left(z^L + \frac{a_{L-1}}{a_L}z^{L-1} + \cdots + \frac{a_1}{a_L}z + \frac{a_0}{a_L}\right) \\ &= a_L \prod_{i=1}^{L}(z-\alpha_i) \\ &= a_L(z^L - (\alpha_1 + \alpha_2 + \cdots + \alpha_L)z^{L-1} \\ &\quad +(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{L-1}\alpha_L)z^{L-2} + \cdots \\ &\quad\quad +(-1)^L(\alpha_1\alpha_2 \ldots \alpha_L)) \end{aligned}$$

De donde (2.8) son los coeficientes de $\frac{G(z)}{a_L}$, los cuales son racionales. Por lo tanto

$$P(\alpha_1, \alpha_2, \ldots, \alpha_L) = \mathcal{P}(\alpha_1) + \mathcal{P}(\alpha_2) + \cdots + \mathcal{P}(\alpha_L)$$

es un número racional.

Ahora $a_L\alpha_1, a_L\alpha_2, \ldots, a_L\alpha_L$ son las raíces de

$$a_L^{L-1}G\left(\frac{z}{a_L}\right) = z^L + a_{L-1}z^{L-1} + a_L a_{L-2}z^{L-2} + \cdots + a_L^{L-1}a_0$$

De donde los polinomios simétricos elementales en $a_L\alpha_1, a_L\alpha_2, \ldots, a_L\alpha_L$ son enteros.

Si $p(x_1, x_2, \ldots, x_L)$ es un polinomio simétrico homogéneo de grado $r \leq gr(P) = gr(\mathcal{P})$ con coeficientes enteros, entonces:

$$a_L^r p(\alpha_1, \alpha_2, \ldots, \alpha_L) = p(a_L\alpha_1, a_L\alpha_2, \ldots, a_L\alpha_L)$$

Así $a_L^r p(\alpha_1, \alpha_2, \ldots, \alpha_L)$ es un entero.

Expresando P como una suma de polinomios homogéneos se llega a que:

$$a_L{}^{gr(\mathcal{P})} P(\alpha_1, \alpha_2, \ldots, \alpha_L) \in \mathbb{Z}.$$

Por lo tanto, $\mathcal{P}(\alpha_1) + \mathcal{P}(\alpha_2) + \cdots + \mathcal{P}(\alpha_L)$ se puede escribir como un número racional con denominador $a_L{}^{gr(\mathcal{P})}$.□

Lema 2.13: Sea $\{\alpha_1, \alpha_2, \dots, \alpha_L\}$ un conjunto completo de conjugados y $P(x_1, \dots, x_L) \in \mathbb{Q}[x_1, \dots, x_L]$ un polinomio simétrico. Entonces $P(\alpha_1, \dots, \alpha_L)$ es una combinación lineal racional de los coeficientes de P.

Prueba:

Por el Teorema 2.1, $P(x_1, \dots, x_L)$ es un polinomio sobre $\mathbb{Q}$ en $\sigma_1, \dots, \sigma_L$. Luego $P(\alpha_1, \dots, \alpha_L)$ es un polinomio en

(2.9) $$\alpha_1 + \alpha_2 + \cdots + \alpha_L, \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{L-1}\alpha_L, \dots, \alpha_1\alpha_2 \dots \alpha_L.$$

Ahora por el Lema 2.8, $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_L) \in \mathbb{Q}[x]$ y (2.9) son sus coeficientes, los cuales están en $\mathbb{Q}$. □

Lema 2.14: Si $\{\gamma_1, \gamma_2, \dots, \gamma_J\}$ es un conjunto de números algebraicos arbitrarios y $f(x_1, x_2, \dots, x_J) = a_1x_1 + a_2x_2 + \cdots + a_Jx_J \in \mathbb{Z}[x_1, x_2, \dots, x_J]$. Entonces

$$\{f(\tau_1, \tau_2, \dots, \tau_J) / \ \tau_j \ es\ conjugado\ de\ \gamma_j, \forall j = 1,2, \dots, J\}$$

es un conjunto completo de conjugados.

Prueba:

Por el lema 2.8, es suficiente probar que

$$p(z) = \prod_{\substack{\tau_j conjugado\ de\ \gamma_j \\ j=1,2,\dots J}} \left(z - f(\tau_1, \tau_2, \dots, \tau_J)\right) \in \mathbb{Q}[z]$$

Reescribiendo $p(z)$ como

$$p(z) = \prod_{\substack{\tau_j conjugado\ de\ \gamma_j \\ j=2,\dots J}} \left(\prod_{\tau_1 conjugado\ de\ \gamma_1} \left(z - f(\tau_1, \tau_2, \dots, \tau_J)\right) \right)$$

Se tiene que

$$h(z) = \prod_{\tau_1 \, conjugado \, de \, \gamma_1} \left(z - f(\tau_1, \tau_2, \dots, \tau_j)\right)$$

es una función polinomial simétrica en los conjugados de γ_1. En efecto,

Si los conjugados de γ_1 son $\gamma_{11}, \gamma_{12}, \dots \gamma_{1n}$; $f(\gamma_{1i}, \gamma_2, \dots, \gamma_j) = a_1\gamma_{1i} + a_2\gamma_2 + \cdots + a_j\gamma_j$. Entonces,

$$h(z) = \left(z - f(\tau_{11}, \tau_2, \dots, \tau_j)\right) \dots \left(z - f(\tau_{1n}, \tau_2, \dots, \tau_j)\right)$$

$$= \prod_{i=1}^{n} \left(\underbrace{z - a_2\tau_2 - \cdots - a_j\tau_j}_{y} - a_1\gamma_{1i} \right)$$

$$= \prod_{i=1}^{n} (y - a_1\gamma_{1i})$$

$$= y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} - \cdots + (-1)^n \sigma_n$$

Donde los σ_i son polinomios simétricos elementales de los conjugados de γ_1 y por ende todos son racionales, por lo tanto

$$h(z) \in \mathbb{Q}[z, \tau_2, \dots, \tau_j]$$

Empleando el mismo argumento para cada $\tau_j, j = 2, \dots, J$; se tiene que

$$p(z) \in \mathbb{Q}[z]$$

Por el Lema 2.8,

$$\{f(\tau_1, \tau_2, \dots, \tau_j) / \ \tau_j \ es \ conjgado \ de \ \gamma_j, \forall j = 1,2, \dots, J\}$$

es un *conjunto completo de conjugados*.□

Ejemplo 2.6.

$\{\sqrt{2}, \sqrt{3}\}$ es un conjunto de números algebraicos.

Si $f(x_1, x_2) = 2x_1 + 3x_2$, entonces

$$\{f(\sqrt{2}, \sqrt{3}), f(-\sqrt{2}, \sqrt{3}), f(\sqrt{2}, -\sqrt{3}), f(-\sqrt{2}, -\sqrt{3})\}$$

Viene dado por $\{2\sqrt{2}+3\sqrt{3}, -2\sqrt{2}+3\sqrt{3}, 2\sqrt{2}-3\sqrt{3}, -2\sqrt{2}-3\sqrt{3}\}$ y $2\sqrt{2}+3\sqrt{3}, -2\sqrt{2}+3\sqrt{3}, 2\sqrt{2}-3\sqrt{3}, -2\sqrt{2}-3\sqrt{3}$; es un conjunto de conjugados, por ser los ceros del polinomio $p(z) = z^4 - 70z^2 + 361$, por lo tanto es un *conjunto completo de conjugados*.

Lema 2.15: El producto de dos sumas exponenciales conjugadas completas es una suma exponencial conjugada completa.

Prueba:

Sean $e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_L}$ y $e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_M}$ dos sumas exponenciales conjugadas completas. Es claro que:

(2.10) $$\left(e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_L}\right)\left(e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_M}\right) = \sum_{\substack{1\le l\le L \\ 1\le m\le M}} e^{\alpha_l+\beta_m}$$

Si aplicamos el Lema 2.14 al polinomio $f(x_1, x_2) = x_1 + x_2$, se tiene que

$$\{\alpha_l + \beta_m : 1 \le l \le L, 1 \le m \le M\}$$

es un conjunto completo de conjugados; por lo tanto, (2.10) es una suma exponencial conjugada completa.□

En las tres secciones que siguen se presentan resultados del álgebra y del análisis complejo que necesitaremos para pruebas subsiguientes; algunos solo serán enunciados, en vista de que la mayoría de la literatura que trata de estos temas, presentan las pruebas completas y claras de estos hechos.

2.5. Algunos resultados del Álgebra Lineal

Las pruebas de los dos siguientes Lemas pueden encontrase, por ejemplo, en Burgos, 2006, páginas 81 y 102.

Lema 2.16: Considérese cualquier sistema de ecuaciones lineales que sea homogéneo.

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0$$

(2.11)

$$a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = 0$$

Entonces, (2.11) tendrá alguna solución no nula si, y sólo si, $det[a_{ij}] = 0$

Lema 2.17: (Determinante de Vandermonde)

Si $x_1, x_2, \dots x_n$ son números, entonces:

$$\begin{vmatrix} 1 & 1 & 1 \dots & 1 \\ x_1 & x_2 & x_3 \dots & x_n \\ & & \vdots & \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} \dots & x_n^{n-1} \end{vmatrix} = \prod_{i<j}(x_j - x_i)$$

Lema 2.18:(Lema de Siegel 1929)

Sea

$$a_{11}x_1 + a_{12}x_2 + \cdots a_{1N}x_N = 0$$

(2.12)

$$a_{M1}x_1 + a_{M2}x_2 + \cdots a_{MN}x_N = 0$$

M ecuaciones en *N* incógnitas tal que:

$$0 < M < N,$$

$$a_{mn} \in \mathbb{Z}; \quad 1 \le m \le M, \quad 1 \le n \le N \quad \text{y}$$

$$|a_{mn}| \le A, \quad A \in \mathbb{Z}$$

Entonces existe una solución no trivial $(x_1, x_2, \dots, x_N) \in \mathbb{Z}^N$ tal que:

$$|x_n| < 1 + (NA)^{\frac{M}{N-M}} \qquad , \quad n = 1,2, \dots N$$

Prueba:

Escribamos

$$a_{m1}x_1 + \cdots + a_{mN}x_N = y_m \qquad m = 1,2, \dots, M$$

Es decir,

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots a_{1N}x_N &= y_1 \\ &\qquad (2.13) \\ a_{M1}x_1 + a_{M2}x_2 + \cdots a_{MN}x_N &= y_M \end{aligned}$$

Así a cada $X = (x_1, x_2, \dots, x_N)$, (2.13) lo envía a $Y = (y_1, y_2, \dots, y_N)$

Sea $q \in \mathbb{Z}^+$

Si $N = 2$, entonces en el cuadrado bidimensional de vértices $(-q, q), (q, q), (q, -q)\ y(-q, -q)$ hay $2q + 1$ enteros en el eje x y $2q + 1$ enteros en el eje y; por lo tanto hay $(2q + 1)^2$ retículos enteros.

Si $N = 3$, hay $(2q + 1)^3$ retículos enteros

De manera general, para N arbitrario; hay $(2q + 1)^N$ retículos enteros en el cubo $N - dimensional$, para $|x_n| \leq q$. Luego los correspondientes valores y_m satisfacen

$$|y_m| = \left|\sum_{n=1}^{N} a_{mn}x_n\right| \leq \sum_{n=1}^{N} |a_{mn}||x_n| \leq NAq$$

Así, si las coordenadas de los puntos reticulares X están en el rango de $(2q + 1)^N$; las coordenadas correspondientes de los puntos reticulares Y están entre $2NAq + 1$ valores: $0, \pm 1, \pm 2, \dots, \pm NAq$. Luego, los puntos reticulares Y tienen a los más $(2NAq + 1)^M$ localizaciones; por lo tanto se tiene que

(2.14) $$(2q+1)^N > (2NAq+1)^M$$

Para demostrar esta última afirmación escójase un entero q tal que $2q$ es el único entero par en el intervalo de longitud 2 definido por

(2.15) $$(NA)^{\frac{M}{N-M}} - 1 \le 2q < (NA)^{\frac{M}{N-M}} + 1$$

La primera parte de la desigualdad (2.15) implica que:

$$(NA)^{\frac{M}{N-M}} - 1 \le 2q$$

$$(NA)^{\frac{M}{N-M}} \le 2q + 1$$

$$(NA)^M \le (2q+1)^{N-M}$$

De donde se sigue que;

$$\begin{aligned}(2NAq+1)^M &= (NA)^M\left(2q + \tfrac{1}{NA}\right)^M \\ &< (NA)^M(2q+1)^M \\ &\le (2q+1)^{N-M}(2q+1)^M \\ &= (2q+1)^N\end{aligned}$$

Como X recorre los $(2q+1)^N$ puntos reticulares definido por $|x_n| \le q$, los correspondientes puntos reticulares Y no son todos distintos, es decir, que existe por lo menos un punto Y correspondiente a

$X' = (x_1', \dots, x_N')$ y $X'' = (x_1'', \dots, x_N'')$

Entonces,

$X''' = (x_1' - x_1'', \dots, x_N' - x_N'')$ da la solución no trivial a (2.12)

Además

$$|x_n' - x_n''| \le |x_n'| + |x_n''| \le q + q = 2q < (NA)^{\frac{N}{N-M}} + 1 \square$$

Ejemplo 2.7:

Sean $D, K, T, r, s \in \mathbb{Z}^{+}, s < r$

Para cada k, t tal que $1 \leq k \leq K$ y $0 \leq t \leq T-1$; consideremos

(2.16) $$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} Re[(m+ni)^t]r^{km}s^{k(D-1-m)}(-1)^{kn}x_{mn} = 0$$

(2.17) $$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} Im[(m+ni)^t]r^{km}s^{k(D-1-m)}(-1)^{kn}x_{mn} = 0$$

Entonces (2.16) y (2.17) dan lugar a KT ecuaciones, respectivamente, con coeficientes enteros en D^2 variables x_{mn} desconocidas; es decir, que obtenemos un sistema homogéneo en $2KT$ ecuaciones en D^2 incógnitas con coeficientes enteros.

Para cada m, n tal que $0 \leq m \leq D-1,\ 0 \leq n \leq D-1$ se tiene que

$$|(m+ni)^t| = \left|\sum_{\theta=0}^{t}\binom{t}{0} m^{t-\theta}(ni)^{\theta}\right| \leq 2^t m^t n^t$$

Como $(m+ni)^t$ tiene $t+1$ términos, de los cuales no más de $\frac{t+1}{2}$ son complejos

$$|Re(m+ni)^t| \leq \frac{t+1}{2}(2mn)^t$$

Luego

$$\left|Re(m+ni)^t r^{km}s^{k(D-1-m)}(-1)^{kn}\right| \leq \frac{t+1}{2}(2mn)^t r^{km}s^{k(D-1-m)}$$

$$\leq \frac{T+1}{2}(2D^2)^T r^{KD} r^{K(D-1-D)}$$

$$\leq \frac{T+1}{2}(2D^2)^T r^{KD} r^{-K}$$

$$\leq \frac{T+1}{2}(2D^2)^T r^{KD}$$

$$\left|Re(m+ni)^t r^{km} s^{k(D-1-m)}(-1)^{kn}\right| \leq 4^{\frac{T+1}{2}}(2D^2)^T r^{KD}$$

$$\leq 2(T+1)(2D^2)^T r^{KD}$$

$$\leq (T+1)(2D)^{2T} r^{KD}$$

De manera análoga se tiene que:

$$\left|Im(m+ni)^t r^{km} s^{k(D-1-m)}(-1)^{kn}\right| \leq (T+1)(2D)^{2T} r^{KD} \in \mathbb{Z}$$

Si $2KT < D^2$, por el Lema de Siegel existe una solución no trivial

$$\left(x_{00}, \dots, x_{0(D-1)}, x_{10}, \dots, x_{1(D-1)}, \dots, x_{(D-1)0}, \dots, x_{(D-1)(D-1)}\right) \in \mathbb{Z}^{D^2}$$

Tal que:

$$|x_{mn}| < 1 + (D^2(T+1)(2D)^{2T} r^{KD})^{\frac{2KT}{D^2-2KT}}$$

2.5. Algunos resultados de La Teoría de Números Algebraicos

Definición 2.10. Un número algebraico α se dice que es un entero algebraico si su polinomio mínimo es mónico.

Definición 2.11. Sea $[\mathbb{Q}(\theta):\mathbb{Q}] = n$ y $\alpha = \sum_{i=0}^{n-1} c_i\theta^i = r(\theta) \in \mathbb{Q}(\theta)$

Si $\theta_1, \theta_2, \dots, \theta_n$ son los conjugados de θ. Entonces los números $\alpha_j = r(\theta_j)$, $j = 1, \dots, n$; son llamados los conjugados de α en $\mathbb{Q}(\theta)$.

Lema 2.19. Sean α, β números algebraicos en $\mathbb{Q}(\theta)$, $[\mathbb{Q}(\theta):\mathbb{Q}] = h$; $\alpha = \alpha_1, \alpha_2, \dots, \alpha_h$; $\beta = \beta_1, \beta_2, \dots, \beta_h$ los conjugados de α y β en $\mathbb{Q}(\theta)$, respectivamente. Entonces los conjugados de $\alpha + \beta$ y $\alpha\beta$ en $\mathbb{Q}(\theta)$ son, respectivamente:

$$\alpha_1 + \beta_1, \dots, \alpha_h + \beta_h \qquad \text{y} \qquad \alpha_1\beta_1, \dots, \alpha_h\beta_h$$

Prueba:

Como $\alpha, \beta \in \mathbb{Q}(\theta)$; los podemos expresar como sigue

$$\alpha = \sum_{i=0}^{h-1} c_i\theta^i = r(\theta) \text{ y } \quad \beta = \sum_{i=0}^{h-1} b_i\theta^i = s(\theta)$$

Sean $r(x) = \sum_{i=0}^{h-1} c_i x^i, s(x) = \sum_{i=0}^{h-1} b_i x^i \in \mathbb{Q}[x]$ y $\theta_1, \theta_2, \dots, \theta_h$ los conjugados de θ con polinomio mínimo $\mathrm{p}(x)$. Por el algoritmo de la división en $\mathbb{Q}[x]$,

$$r(x)s(x) = q(x)p(x) + t(x) \qquad \text{con } 0 \leq gr(t) \leq h-1$$

En vista de que para $1 \leq j \leq h$, $p(\theta_j) = 0$; se tiene que

$$\alpha_j\beta_j = r(\theta_j)s(\theta_j) = t(\theta_j)$$

Por lo tanto, $\alpha_j\beta_j$ son los conjugados de $\alpha\beta$ en $\mathbb{Q}(\theta)$, $j = 1,2,\dots,h$

Por otro lado,

$$\alpha + \beta = r(\theta) + s(\theta) = \sum_{i=0}^{h-1} c_i\theta^i + \sum_{i=0}^{h-1} b_i\theta^i = \sum_{i=0}^{h-1}(c_i + b_i)\theta^i \qquad \text{y}$$

$$\alpha_i + \beta_i = r(\theta_i) + s(\theta_i) = \sum_{i=0}^{h-1}(c_i + b_i)\theta_i^i. \square$$

La prueba de los siguiente lemas se puede encontrar, por ejemplo, en Pollar & Diamond, 1998.

Lema 2.20. Si α es un número algebraico, entonces existe un entero positivo r tal que $r\alpha$ es un entero algebraico.

Lema 2.21: Si $\alpha_1, \alpha_2, \dots, \alpha_L \in \tilde{\mathbb{Q}}$, entonces existe un entero algebraico $\theta \in \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_L)$ tal que $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_L) = \mathbb{Q}(\theta)$.

Definición 2.12. Si $[\mathbb{Q}(\theta): \mathbb{Q}] = n$ y $\alpha_1, \alpha_2, \dots, \alpha_n$ una base para $\mathbb{Q}(\theta)$. Entonces el discriminante del conjunto $\alpha_1, \alpha_2, \dots, \alpha_n$ está definido por:

$$\Delta[\alpha_1, \alpha_2, \dots, \alpha_n] = \left|\alpha_j^i\right|^2,$$

donde $\left|\alpha_j^i\right|$ es el determinante

$$\begin{vmatrix} \alpha_1^1 & \alpha_2^1 \dots \alpha_n^1 \\ & \cdot \\ & \cdot \\ & \cdot \\ \alpha_1^n & \alpha_2^n \dots \alpha_n^n \end{vmatrix} \quad \text{y}$$

$\alpha_j^i, i = 1,2, \dots n$ son los conjugados de α_j en $\mathbb{Q}(\theta)$.

Lema 2.22. Si $[\mathbb{Q}(\theta):\mathbb{Q}] = h$. Entonces existe una base para $\mathbb{Q}(\theta)$ compuesta por enteros algebraicos $\beta_1, \beta_2, \dots, \beta_h$ tal que todo entero algebraico en $\mathbb{Q}(\theta)$ se puede expresar de forma única como $a_1\beta_1 + a_2\beta_2 + \cdots + a_h\beta_h$; donde $a_i \in \mathbb{Z}, i = 1,2, \dots h$. Además $\Delta[\beta_1, \beta_2, \dots, \beta_h] \in \mathbb{Z} - \{0\}$.

Definición 2.13. Si $[\mathbb{Q}(\theta):\mathbb{Q}] = h$ y α es un número algebraico en $\mathbb{Q}(\theta)$. La norma de α en $\mathbb{Q}(\theta)$ denotada por $N_{\mathbb{Q}(\theta)}(\alpha)$ está definida por $N_{\mathbb{Q}(\theta)}(\alpha) = \alpha_1\alpha_2 \dots \alpha_h$: Donde α_i $(i = 1,2, \dots h)$ son los conjugados de α en $\mathbb{Q}(\theta)$.

Lema 2.23. Si $[\mathbb{Q}(\theta):\mathbb{Q}] = h$ y α, β números algebraico en $\mathbb{Q}(\theta)$, entonces:

i) $N_{\mathbb{Q}(\theta)}(\alpha\beta) = (N_{\mathbb{Q}(\theta)}(\alpha))(N_{\mathbb{Q}(\theta)}(\beta))$

ii) $N_{\mathbb{Q}(\theta)}(\alpha) = 0$ si y sólo si $\alpha = 0$

iii) Si α es un entero algebraico, entonces $N_{\mathbb{Q}(\theta)}(\alpha) \in \mathbb{Z}$

iv) Si α es racional, entonces $N_{\mathbb{Q}(\theta)}(\alpha) = \alpha^h$

Lema 2.24: Sea $\theta \in \widetilde{\mathbb{Q}}$ de grado h. Consideremos p ecuaciones en q incógnitas, con $0 < p < q$.

$$\begin{aligned} \alpha_{11}\xi_1 + \alpha_{12}\xi_2 + \cdots + \alpha_{1q}\xi_q &= 0 \\ &\vdots \\ \alpha_{p1}\xi_1 + \alpha_{p2}\xi_2 + \cdots + \alpha_{pq}\xi_q &= 0 \end{aligned} \tag{2.18}$$

Donde α_{ij} son enteros algebraicos en $\mathbb{Q}(\theta)$ tal que $\|\alpha_{ij}\| \leq A$; para $A \geq 1$, $i = 1,2,..p;\quad j = 1,2,..q$

Entonces existe una constante positiva c que depende de $\mathbb{Q}(\theta)$ e independiente de los α_{ij}, p y q tal que (2.18) tiene una solución no trivial $\xi_1, \xi_2, \dots, \xi_q$ en enteros algebraicos en $\mathbb{Q}(\theta)$; tal que:

$$\|\xi_k\| < c + c(cqA)^{\frac{p}{q-p}} \qquad k = 1,2,\dots q$$

Prueba:

Sea $\beta_1, \beta_2, \dots, \beta_h$ una base de enteros algebraicos para $\mathbb{Q}(\theta)$, la cual está garantizada por el Lema 2.22.

Si α es un entero algebraico en $\mathbb{Q}(\theta)$, entonces

$$\alpha = g_1\beta_1 + g_2\beta_2 + \cdots + g_h\beta_h \quad , g_i \in \mathbb{Z} \quad i = 1,2,\dots,h \tag{2.19}$$

Denotemos los conjugados de α y β_j $(j = 1,\dots,h)$ en $\mathbb{Q}(\theta)$, respectivamente, por:

$$\alpha = \alpha^1, \alpha^2, \dots, \alpha^h$$

$$\beta_j = \beta_j^1, \beta_j^2, \dots, \beta_j^h$$

Tomando conjugados en (2.19), por el Lema 2.19 se tiene que:

$$\alpha^1 = g_1\beta_1^1 + g_2\beta_2^1 + \cdots + g_h\beta_h^1$$

$$\alpha^2 = g_1\beta_1^2 + g_2\beta_2^2 + \cdots + g_h\beta_h^2$$

$$\vdots$$

$$\alpha^h = g_1\beta_1^h + g_2\beta_2^h + \cdots + g_h\beta_h^h$$

Por el lema 2.22, $|\beta_j^i| \neq 0$; por lo tanto podemos resolver estas ecuaciones para los g_j como una combinación lineal de los α^i cuyos coeficientes dependen únicamente de la base.

Luego,

(2.20) $$|g_j| < c_1\|\alpha\| \quad j = 1,2,\dots,h$$

Donde la constante positiva c_1 depende de $\mathbf{Q}(\theta)$, pero es independiente de α.

Si (2.18) tiene una solución en enteros algebraicos en $\mathbf{Q}(\theta)$, los podemos escribir como sigue:

(2.21) $$\xi_i = \sum_{j=1}^{h} x_{ij}\beta_j \qquad i = 1,2,\dots,q;\ x_{ij} \in \mathbb{Z}$$

Luego (2.18) la podríamos reducir a

(2.22) $$\sum_{i=1}^{q} \alpha_{ki}\xi_i = \sum_{i=1}^{q} \alpha_{ki}\left(\sum_{j=1}^{h} x_{ij}\beta_j\right) = \sum_{i=1}^{q}\sum_{j=1}^{h} \alpha_{ki}\beta_j x_{ij} = 0$$

$$k = 1,2,\dots,p$$

El problema se reduce en hallar enteros x_{ij} que satisfagan (2.22). Ahora los enteros algebraicos $\alpha_{ki}\beta_j$ pueden expresarse en término de la base de enteros algebraicos, es decir;

(2.23) $$\alpha_{ki}\beta_j = \sum_{r=1}^{h} m_{kijr}\beta_r$$

Donde $k = 1, \dots, p; i = 1, \dots, q; j = 1, \dots, h$ y $m_{kijr} \in \mathbb{Z}$.

Reescribiendo (2.22),

$$\sum_{i=1}^{q}\sum_{j=1}^{h}\sum_{r=1}^{h} m_{kijr}x_{ij}\beta_r = 0 \qquad k = 1,2, \dots, p$$

Como los β_r son linealmente independiente sobre los números racionales.

(2.24) $$\sum_{i=1}^{q}\sum_{j=1}^{h} m_{kijr}x_{ij} = 0 \qquad k = 1, \dots, p; r = 1, \dots, h$$

Se tienen ph ecuaciones en qh incógnitas x_{ij} y en vista de que $0 < p < q$, $0 < ph < qh$.

A partir de (2.23), obtenemos de (2.20),

$$|m_{kijr}| < c_1\|\alpha_{ki}\beta_j\| \leq c_1\|\alpha_{ki}\|\|\beta_j\|$$

$$\leq c_1 A\|\beta_j\|$$

$$\leq c_2 A$$

Donde $c_2 \geq c_1\|\beta_j\|, \forall j = 1,2, \dots h$; tal que $c_2 A \in \mathbb{Z}^+$

Ahora podemos aplicar el Lema de Siegel a (2.24), es decir, que existe una solución no trivial de (2.24) tal que:

$$|x_{ij}| < 1 + (qhc_2A)^{\frac{ph}{qh-ph}} = 1 + (hc_2qA)^{\frac{p}{q-p}}$$

Luego de (2.21)

$$\|\xi_i\| < h\left(max\|\beta_j\|\right)\left[1 + (hc_2qA)^{\frac{p}{q-p}}\right]$$

$$< c + c(cqA)^{\frac{p}{q-p}}$$

Donde $c \geq máx\{hc_2, h\|\beta_j\|\}, j = 1,2,\dots,h$; además, es claro que c depende del cuerpo $\mathbf{Q}(\theta)$ y es independiente de α_{ij}, p y q.

Como al menos uno de los x_{ij} no es nulo, se sigue de (2.21) que al menos uno de los $\xi_i$es una solución no nula ya que los β_j son $\mathbf{Q}$ −linealmente independientes. □

Ejemplo 2.8:

Sean α, β números algebraicos, con $\alpha \neq 0,1$ y $\beta \notin \mathbf{Q}$ y consideremos;

(2.25) $$\sum_{i=1}^{q}\sum_{j=1}^{q}(i + \beta j)^a e^{(i+\beta j)b(log\alpha)}\xi_{ij} = 0$$

Donde $a = 0,1, \dots, n-1; b = 1,2, \dots, m$.

Reescribiendo (2,25),

$$\sum_{i=1}^{q}\sum_{j=1}^{q}(i + \beta j)^a (e^{log\alpha})^{ib}\left(e^{\beta log\alpha}\right)^{jb}\xi_{ij} = 0$$

(2.26) $$\sum_{i=1}^{q}\sum_{j=1}^{q}(i + \beta j)^a (\alpha)^{ib}(\gamma)^{jb}\xi_{ij} = 0$$

Donde $\gamma = \alpha^{\beta}$.

Sea $\theta \in \tilde{\mathbf{Q}}$ y supongamos que $\gamma \in \tilde{\mathbf{Q}}$ tal que $\alpha, \beta, \gamma \in \mathbf{Q}(\theta)$. Además como $1, \beta$ son linealmente independientes, los $i + \beta j$ son distintos. Luego de (2.26) se obtienen mn ecuaciones lineales en q^2 incógnitas ξ_{ij} cuyos coeficientes son números algebraicos distintos en $\mathbf{Q}(\theta)$, de la forma $(i + \beta j)^a(\alpha)^{ib}(\gamma)^{jb}$.

Escojamos m, n, q de tal forma que $q > 4m^2$, q^2 sea múltiplo de $2m$, $n = \frac{q^2}{2m}$ y q un cuadrado perfecto; entonces, es claro que $mn < q^2$. Procedamos a acotar los coeficientes de (2.26).

$$(i+\beta j)^a(\alpha)^{ib}(\gamma)^{jb} = \left[\sum_{k=0}^{a}\binom{a}{k} i^{a-k}(j\beta)^k\right]\alpha^{ib}\gamma^{jb}$$

$$= \left[i^a + \frac{a!}{(a-1)!} i^{a-1}(j\beta)^1 + \frac{a!}{2!(a-2)!} i^{a-2}(j\beta)^2 + \cdots + (j\beta)^a\right]\alpha^{ib}\gamma^{jb}$$

En esta última expresión aparecen monomios en α, β, y γ con grado a lo sumo

$$ib + jb + a \le qm + qm + n - 1 = n - 1 + 2mq < n + 2mq$$

Por el Lema 2.20, existe un entero $c_1 > 0$ tal que: $c_1\alpha, c_1\beta, c_1\gamma$ son enteros algebraicos; luego,

$$\text{(2.27)} \qquad c_1^{n+2mq}(i+j\beta)^a\alpha^{ib}\gamma^{jb} \qquad a = 0,1,\ldots,n-1;\ b = 1,2,\ldots,m$$

Son enteros algebraicos.

Por otro lado, ya que $\|i + j\beta\| \le \|i\| + \|j\|\|\beta\| \le q + q\|\beta\| = q(1 + \|\beta\|)$. Si $c_2 = \text{máx}\{\|\alpha\|, \|\gamma\|, 1 + \|\beta\|\}$, entonces para cada entero algebraico en (2.27) y sus conjugados se tiene la siguiente cota.

$$\left|c_1^{n+2mq}(i+j\beta)^a\alpha^{ib}\gamma^{jb}\right| \le c_1^{n+2mq}(qc_2)^n c_2^{qb} c_2^{qb}$$

$$< c_1^{n+2mq}(qc_2)^n c_2^{2qm}$$

$$= (c_1c_2)^n[(c_1c_2)^{2m}]^q q^n$$

$$= (c_1c_2)^n[(c_1c_2)^{2m}]^q\left(\sqrt{2mn}\right)^n$$

$$\left|c_1^{n+2mq}(i+j\beta)^a\alpha^{ib}\gamma^{jb}\right| < (c_1c_2)^n[(c_1c_2)^{2m}]^q\left(\sqrt{2m}\right)^n n^{\frac{n}{2}}$$

$$< (c_1c_2)^n[(c_1c_2)^{2m}]^n\left(\sqrt{2m}\right)^n n^{\frac{n}{2}}$$

$$= [(c_1c_2)^{2m+1}]^n\left(\sqrt{2m}\right)^n n^{\frac{n}{2}}$$

$$= c_3^n n^{\frac{n}{2}}$$

Donde $c_3 = (c_1c_2)^{2m+1}\sqrt{2m}$ y es claro que c_3, c_1, c_2, m son independientes de n.

Ahora podemos aplicar el Lema 2.24 a (2.25), con $A = c_3^n n^{\frac{n}{2}}$. Luego, existe una solución no trivial de enteros algebraicos ξ_{ij} tal que

$$\|\xi_{ij}\| < c + c\left[c(2mn)c_3^n n^{\frac{n}{2}}\right]^{\frac{mn}{2mn-mn}}$$

$$= c + 2c^2mnc_3^n n^{\frac{n}{2}}$$

$$< 3c^2mnc_3^n n^{\frac{n}{2}}$$

$$< 3c^2 4^n c_3^n n^{\frac{n}{2}}$$

$$< 3^n(c^2)^n 4^n c_3^n n^{\frac{n}{2}}$$

$$= c_4^n n^{\frac{n}{2}}$$

Donde $c_4 = 12c^2c_3$ y es claro que es independiente de n.

Definición 2.14. Sea α un número algebraico de grado d con polinomio mínimo $p(x) = \sum_{j=0}^{d} c_j x^j \in \mathbb{Z}[x]$. Se define la altura de α, denotada por $\varkappa(\alpha)$, como la altura de su polinomio mínimo; es decir,

$$\varkappa(\alpha) = \varkappa(p) = max\{|c_0|, |c_1|, \ldots, |c_d|\}$$

Lema 2.25: Sea α un número algebraico de grado d con polinomio mínimo $p(x) = \sum_{j=0}^{d} c_j x^j \in \mathbb{Z}[x]$. Entonces los números $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ son linealmente independientes sobre $\mathbb{Q}$. Además, para cada entero $n, n \geq d$, la cantidad α^n puede expresarse como una combinación lineal racional de $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$. Esto es, existen números racionales $c_{0,n}, c_{1,n}, \dots, c_{d-1,n}$ tal que

$$\alpha^n = c_{0,n} + c_{1,n}\alpha + c_{2,n}\alpha^2 + \cdots + c_{d-1,n}\alpha^{d-1} \qquad \text{y}$$

$$\max_{0 \leq j \leq d-1} \{|c_{j,n}|\} \leq \left(1 + \varkappa(\alpha)\right)^{n+1-d}$$

y además cada número racional $c_{j,n}$ puede expresarse como una fracción con denominador igual a c_d^{n+1-d}

Lema 2.26: Sean $\beta_1, \beta_2, \dots, \beta_L \in \mathbb{Q}(\theta)$, donde θ es un entero algebraico de grado d y altura $\varkappa(\theta)$. Si para cada $l = 1,2, \dots, L$,

$$\beta_l = r_{l1} + r_{l2}\theta + \cdots + r_{ld}\theta^{d-1}$$

Con $r_{lj} \in \mathbb{Q}$, tal que $|r_{lj}| \leq B_l, j = 1,2, \dots, d$; para alguna constante B_l. Entonces

$$\beta_1\beta_2 \dots \beta_L = r_1 + r_2\theta + \cdots + r_d\theta^{d-1} \qquad \text{y}$$

$r_j \in \mathbb{Q}$, satisfaciendo

$$\max_{1 \leq j \leq d} \{|r_j|\} \leq d^L B_1 B_2 \dots B_L \left(2\varkappa(\theta)\right)^{dL}$$

Más aún, si $den(\beta_l)$ denota el mínimo común múltiplo de los denominadores de los coeficientes racionales $r_{l1}, r_{l2}, \dots, r_{ld}$; entonces cada número racional r_j puede expresarse con denominador de la forma

$$den(\beta_1)den(\beta_2) \dots den(\beta_L)$$

2.7. Algunos resultados del Análisis Complejo.

Los siguientes resultados del análisis complejo pueden ser consultados en Churchill & Brown, 2004.

Lema 2.27. Si una función es analítica en un punto, admite derivadas de todo orden en ese punto y las derivadas son funciones analíticas en ese punto.

Lema 2.28. (Principio del Módulo Máximo)

Si $f(z)$ es analítica en un dominio D y en su frontera C, donde C es una curva cerrada simple, entonces $|f(z)|$ alcanza su máximo en la frontera C, y no en su interior, a no ser que $f(z)$ sea constante.

Lema 2.29. Una función f analítica en z_0 tiene un cero de orden m en z_0 si, y sólo si, existe una función g, analítica y no nula en z_0 tal que $f(z) = (z - z_0)^m g(z)$

Definición 2.15. Sea F una función y $R \in \mathbb{R}^+$. Definimos el conjunto

$$Z(F,R) = \{z \in \mathbb{C}: F(z) = 0, |z| \leq R\}$$

con la condición de que, si $z_0 \in Z(F,R)$ es un cero de F con multiplicidad m, entonces z_0 aparece m veces en el conjunto $Z(F,R)$. El cardinal del conjunto $Z(F,R)$ lo denotaremos por $card\big(Z(F,R)\big)$.

Lema 2.30. Sea F una función entera y supóngase que existe un número real k tal que para todo número real suficientemente grande R,

$$\max_{|z|\leq R}\{|F(z)|\} = |F|_R \leq e^{R^k}$$

Si existe un $\epsilon > 0$ y una sucesión creciente no acotada de números reales $R_1, R_2, \ldots$ tal que

$$R_n^{k+\epsilon} < card\big(Z(F,R)\big),$$

para todo $n = 1,2,\dots$; entonces F es idénticamente nula.

CAPÍTULO N° 3

ALGUNOS RESULTADOS TRASCENDENTES, PREVIOS A LA SOLUCIÓN DEL SÉPTIMO PROBLEMA DE HILBERT

Tal como lo anunciamos en el capítulo n°1, esta sección está dedicada a presentar las pruebas de algunos resultados previos a la formulación de los 23 problemas de Hilbert y a la solución del séptimo problema planteado por él.

3.1. Irracionalidad de potencias de e y su trascendencia.

Teorema 3.1. e^a es irracional para todo entero $a \geq 1$.

Prueba:

Supongamos que $e^a = \frac{r}{s} \in \mathbf{Q}$, entonces

$$r - se^a = 0$$

(3.1) $$r - s\sum_{n=0}^{\infty}\frac{a^n}{n!} = r - s\left(\sum_{n=0}^{N-p}\frac{a^n}{n!} + \sum_{n=N-p+1}^{N-1}\frac{a^n}{n!} + \sum_{n=N}^{\infty}\frac{a^n}{n!}\right) = 0,$$

$N, p \in \mathbb{Z}$

Sea $f(z) = z^{p-1}(z-a)^p = \sum_{N=p-1}^{2p-1} c_N z^N \in \mathbb{Z}[z]$, por la parte (a) del Lema 2.3

Al multiplicar (3.1) por $\sum_{N=p-1}^{2p-1} N!\, c_N$, se tiene que

$$r\sum_{N=p-1}^{2p-1} N!\, c_N = s\sum_{N=p-1}^{2p-1}\left(N!\, c_N \sum_{n=0}^{N-p}\frac{a^n}{n!}\right) + s\sum_{N=p-1}^{2p-1}\left(N!\, c_N \sum_{n=N-p+1}^{N-1}\frac{a^n}{n!}\right)$$

$$+s\sum_{N=p-1}^{2p-1}\left(N!\, c_N \sum_{n=N}^{\infty}\frac{a^n}{n!}\right)$$

Por el Lema 2.1 y la parte (b) del Lema 2.3:

$$\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=N-p+1}^{N-1}\frac{a^n}{n!}\right)=0$$

Luego,

$$(3.2)\quad r\sum_{N=p-1}^{2p-1}N!\,c_N=s\left(\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{a^n}{n!}\right)+\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=N}^{\infty}\frac{a^n}{n!}\right)\right)$$

Definamos:

$\mathcal{P}_p(z)=\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{z^n}{n!}\right)$, Polinomio de aproximación

$\mathcal{T}_p(z)=\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=N}^{\infty}\frac{z^n}{n!}\right)$, Cola de la serie

Podemos reescribir (3.2) como sigue

$$r\sum_{N=p-1}^{2p-1}N!\,c_N=s\mathcal{P}_p(a)+s\mathcal{T}_p(a)$$

Así;

$$\left|r\sum_{N=p-1}^{2p-1}N!\,c_N-s\mathcal{P}_p(a)\right|=\left|s\mathcal{T}_p(a)\right|$$

Vamos a obtener una cota superior para $\mathcal{T}_p(a)$

$$\mathcal{T}_p(a)=\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=N}^{\infty}\frac{a^n}{n!}\right)$$

$$=\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=0}^{\infty}\frac{a^{n+N}}{(n+N)!}\right)$$

$$\sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=0}^{\infty}\frac{a^{n+N}}{(n+N)!}\right)=\sum_{N=p-1}^{2p-1}\left(c_N\sum_{n=0}^{\infty}\frac{N!\,a^{n+N}}{(n+N)!}\right)$$

$$=\sum_{N=p-1}^{2p-1}\left(c_N\sum_{n=0}^{\infty}\frac{N!\,a^{n}a^{N}}{(n+N)!}\right)$$

$$=\sum_{N=p-1}^{2p-1}\left(c_N a^N\sum_{n=0}^{\infty}\frac{N!\,a^{n}}{(n+N)!}\right)$$

$$\leq\sum_{N=p-1}^{2p-1}\left(c_N a^N\sum_{n=0}^{\infty}\frac{a^{n}}{n!}\right);\quad \text{por (a), propiedad 2.1.}$$

Así,

$$\left|\mathcal{T}_p(a)\right|\leq\left|\sum_{N=p-1}^{2p-1}\left(c_N a^N\sum_{n=0}^{\infty}\frac{a^{n}}{n!}\right)\right|$$

$$=\left|\sum_{N=p-1}^{2p-1}(c_N a^N e^a)\right|$$

$$\leq e^a a^{2p-1}\left|\sum_{N=p-1}^{2p-1}c_N\right|$$

$$\leq e^a a^{2p-1}\sum_{N=p-1}^{2p-1}|c_N|$$

$$=e^a a^{2p-1}(1+a)^p,\quad \text{por el Lema 2.4}$$

$$=e^a a^{2p}a^{-1}(1+a)^p$$

$$=e^a\frac{1}{a}[a^2(1+a)]^p$$

$$=K_1{K_2}^p$$

Donde $K_1=\frac{e^a}{a}$ y $K_2=a^2(1+a)$.

Concluimos que:

$$\left|r\sum_{N=p-1}^{2p-1} N!\,c_N - s\mathcal{P}_p(a)\right| = \left|s\mathcal{T}_p(a)\right| \le sK_1K_2{}^p$$

$$\left|r\sum_{N=p-1}^{2p-1} N!\,c_N - s\mathcal{P}_p(a)\right| \le sK_1K_2{}^p \tag{3.3}$$

El lado izquierdo de la desigualdad anterior es un entero positivo que tiene como factor a $(p-1)!$. En efecto;

Sabemos que $f(z) = \sum_{N=p-1}^{2p-1} c_N z^N \in \mathbb{Z}[z]$, por ende $c_N \in \mathbb{Z}$.

Así,

$$r\sum_{N=p-1}^{2p-1} N!\,c_N \in \mathbb{Z}$$

y, evidentemente tiene a $(p-1)!$ como factor.

Por otro lado,

$$\mathcal{P}_p(a) = \sum_{N=p-1}^{2p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{a^n}{n!}\right)$$

$$= \sum_{N=p}^{2p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{a^n}{n!}\right)$$

$$= p!\,c_p\sum_{n=0}^{p-p}\frac{a^n}{n!} + (p+1)!\,c_{p+1}\sum_{n=0}^{1}\frac{a^n}{n!} + (p+2)!\,c_{p+2}\sum_{n=0}^{2}\frac{a^n}{n!} + \cdots$$

$$+(2p-1)!\,c_{2p-1}\sum_{n=0}^{p-1}\frac{a^n}{n!}$$

$$\mathcal{P}_p(a) = p!\,c_p + (p+1)!\,c_{p+1}[1+a] + (p+2)!\,c_{p+2}\left[1+a+\frac{a^2}{2!}\right] + \cdots \tag{3.4}$$

$$+(2p-1)!\,c_{2p-1}\left[1+a+\frac{a^2}{2!}+\cdots+\frac{a^{p-1}}{(p-1)!}\right] \in \mathbb{Z}$$

y también tiene como factor a $(p-1)!$

Por lo tanto,

$$r\sum_{N=p-1}^{2p-1} N!\,c_N - s\mathcal{P}_p(a)$$

es un entero que tiene como factor a $(p-1)!$

Al dividir (3.3) entre $(p-1)!$, obtenemos la desigualdad:

(3.5) $$\left|\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!\,c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a)\right| \le sK_1\frac{K_2{}^p}{(p-1)!}$$

cuyo lado izquierdo sigue siendo un entero; es más, es distinto de cero. Para ver esta afirmación probaremos que:

(3.6) $$\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!\,c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a) \not\equiv 0 \; mod\; p$$

Por (3.4)

$$\frac{s}{(p-1)!}\mathcal{P}_p(a) \equiv 0 \; mod\; p$$

Sin embargo,

$$\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!\,c_N \not\equiv 0 \; mod\; p$$

Pues en caso contrario, al escoger un primo p tal que $p > máx\{a, r\}$ se tendría que si:

$$p/\left(\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!\, c_N\right)$$

Entonces, como $p > r$

$$p/[c_{p-1} + pc_p + (p+1)pc_{p+1} + \cdots + (2p-1)(2p-2)\ldots pc_{2p-1}]$$

Luego,

$$p/c_{p-1}$$

Y en vista de que

$$|c_{p-1}| = |a^p| \neq 0$$

Se tiene que

$$p/a$$

Lo cual es imposible, pues $p > a$. Así completamos la prueba de (3.6)

Como p es arbitrario, al escoger un p relativamente grande, es decir $p \to \infty$, se tendría en vista de que K_1 y K_2 no dependen de p y de (3.6) que:

$$0 < \left|\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!\, c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a)\right| < 1$$

Lo cual es imposible, pues no hay enteros entre 0 y 1; luego nuestra suposición es falsa y e^a tiene que ser irracional.□

Corolario 3.1: Para todo número racional $\frac{a}{b}$ distinto de cero, $e^{\frac{a}{b}}$ es irracional.

Prueba:

Supongamos que $\exists \frac{a}{b} \in \mathbb{Q}$ no nulo tal que,

$$e^{\frac{a}{b}} \in \mathbb{Q}, \text{ es decir, } e^{\frac{a}{b}} = \frac{p}{q};\ p,q \in \mathbb{Z},\ q \neq 0$$

Sin pérdida de generalidades, supongamos que $a \geq 1$. Luego,

$$e^{\frac{a}{b}} = (e^{a})^{\frac{1}{b}} = \frac{p}{q}$$

Elevando a la potencia b.

$$e^{a} = \left(\frac{p}{q}\right)^{b} \in \mathbb{Q}$$

Lo que contradice el Teorema anterior; por lo tanto nuestra suposición es falsa y $e^{\frac{a}{b}}$ es irracional□

Teorema 3.2. El número e es trascendente.

Prueba:

Supongamos que e es algebraico, entonces existen enteros $r_0, r_1, \ldots, r_d$ con $r_d \neq o$ tal que

(3.7) $$r_0 + r_1 e + r_2 e^2 + \cdots + r_d e^d = 0$$

Construyamos un polinomio $\mathcal{P}_p(z)$ tal que:

$\mathcal{P}_p(1)$ se aproxime a e

$\mathcal{P}_p(2)$ se aproxime a e^2

$$\mathcal{P}_p(d) \quad \text{se aproxime a } e^d$$

Para tal efecto, definamos:

$$f(z) = z^{p-1}(z-1)^p(z-2)^p \dots (z-d)^p$$

Rescribiéndolo (ver observación 2.1)

$$f(z) = \sum_{N=p-1}^{(d+1)p-1} c_N z^N$$

Multipliquemos (3.7) por $\sum_{N=p-1}^{(d+1)p-1} N!\, c_N$

$$r_o \sum_{N=p-1}^{(d+1)p-1} N!\, c_N + r_1 e \sum_{N=p-1}^{(d+1)p-1} N!\, c_N + \dots + r_d e^d \sum_{N=p-1}^{(d+1)p-1} N!\, c_N = 0$$

(3.8) $r_o \sum_{N=p-1}^{(d+1)p-1} N!\, c_N + r_1 e^1 \sum_{N=p-1}^{(d+1)p-1} N!\, c_N + \dots + r_d e^d \sum_{N=p-1}^{(d+1)p-1} N!\, c_N = 0$

Para $1 \leq t \leq d$

$$e^t \sum_{N=p-1}^{(d+1)p-1} N!\, c_N = \sum_{N=p-1}^{(d+1)p-1} \left(N!\, c_N \sum_{n=0}^{N-p} \frac{t^n}{n!} \right) + \sum_{N=p-1}^{(d+1)p-1} \left(N!\, c_N \sum_{n=N-p+1}^{N-1} \frac{t^n}{n!} \right)$$

$$+ \sum_{N=p-1}^{(d+1)p-1} \left(N!\, c_N \sum_{n=N}^{\infty} \frac{t^n}{n!} \right)$$

Por el lema 2.1

$$\sum_{n=1}^{p-1} f^n(z) = \sum_{N=p-1}^{(d+1)p-1} \left(N!\, c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right)$$

De nuevo por la observación 2.1, para $t = 1,2,3,\ldots,d$; el término medio se anula. Por lo tanto:

$$e^t \sum_{N=p-1}^{(d+1)p-1} N!\,c_N = \sum_{N=p-1}^{(d+1)p-1}\left(N!\,c_N \sum_{n=0}^{N-p}\frac{t^n}{n!}\right) + \sum_{N=p-1}^{(d+1)p-1}\left(N!\,c_N \sum_{n=N}^{\infty}\frac{t^n}{n!}\right)$$

$$= \mathcal{P}_p(t) + \mathcal{T}_p(t)$$

Donde

$\mathcal{P}_p(z) = \sum_{N=p-1}^{(d+1)p-1}\left(N!\,c_N \sum_{n=0}^{N-p}\frac{z^n}{n!}\right)$, Polinomio de aproximación

$\mathcal{T}_p(z) = \sum_{N=p-1}^{(d+1)p-1}\left(N!\,c_N \sum_{n=N}^{\infty}\frac{z^n}{n!}\right)$, Cola de la serie

Reescribiendo (3.8)

$$r_o \sum_{N=p-1}^{(d+1)p-1} N!\,c_N + r_1(\mathcal{P}_p(1) + \mathcal{T}_p(1)) + \cdots + r_d(\mathcal{P}_p(d) + \mathcal{T}_p(d)) = 0$$

$$r_o \sum_{N=p-1}^{(d+1)p-1} N!\,c_N + r_1\mathcal{P}_p(1) + \cdots + r_d\mathcal{P}_p(d) = -r_1\mathcal{T}_p(1) - \cdots - r_d\mathcal{T}_p(d)$$

(3.9) $$r_o \sum_{N=p-1}^{(d+1)p-1} N!\,c_N + \sum_{t=1}^{d} r_t\mathcal{P}_p(t) = -\sum_{t=1}^{d} r_t\mathcal{T}_p(t)$$

Procediendo como lo hicimos en (3.3), se demuestra que el lado izquierdo de (3.9) es un entero que tiene como factor a $(p-1)!$, así que al dividir entre este factor y tomar valor absoluto a ambos miembros de la igualdad, (3.9) se reescribe como:

$$\left|\frac{r_0}{(p-1)!}\sum_{N=p-1}^{(d+1)p-1} N!\,c_N + \sum_{t=1}^{d}\frac{r_t}{(p-1)!}\mathcal{T}_p(t)\right| = \left|\sum_{t=1}^{d}\frac{r_t}{(p-1)!}\mathcal{T}_p(t)\right|$$

Tal como lo hicimos para obtener una cota superior para $\mathcal{T}_p(a)$ en la demostración del teorema 3.1, para $t = 1,2,3,\dots,d$ se tiene que

(3.10) $$|\mathcal{T}_p(t)| \le e^t t^{(d+1)p-1} \sum_{N=p-1}^{(d+1)p-1} |c_N|$$

Por definición

$$f(z) = z^{p-1}(z-1)^p(z-2)^p \dots (z-d)^p$$

$$= z^{p-1}\prod_{t=1}^{d}(z-t)^p$$

$$= \sum_{N=p-1}^{(d+1)p-1} c_N z^N$$

Por el Lema 2.5.

$$|c_N| \le \prod_{t=1}^{d}(2t)^p \le [(2d)^d]^p$$

Ahora podemos seguir acotando $|\mathcal{T}_p(t)|$

$$|\mathcal{T}_p(t)| \le e^t t^{(d+1)p-1} \sum_{N=p-1}^{(d+1)p-1} |c_N|$$

$$\le e^t t^{(d+1)p-1}(dp+1)[(2d)^d]^p$$

$$\le e^t t^{(d+1)p-1} d^p [(2d)^d]^p$$

Así para $1 \le t \le d$

$$|\mathcal{T}_p(t)| \leq e^d d^{(d+1)p-1} d^p [(2d)^d]^p$$

$$= e^d d^{-1} d^{(d+2)p} [(2d)^d]^p$$

$$= \frac{e^d}{d} (d^d d^2)^p [(2d)^d]^p$$

$$= \frac{e^d}{d} [d^2 2^d d^{2d}]^p$$

$$= \frac{e^d}{d} [d^2 (2d^2)^d]^p$$

$$= K_1 {K_2}^p \qquad\qquad K_1 = \frac{e^d}{d} \text{ y } K_2 = d^2(2d^2)^d$$

Luego,

(3.11) $$\left|\frac{r_0}{(p-1)!}\sum_{N=p-1}^{(d+1)p-1} N!\, c_N + \sum_{t=1}^{d} \frac{r_t}{(p-1)!} \mathcal{P}_p(t)\right| = \left|\sum_{t=1}^{d} \frac{r_t}{(p-1)!} \mathcal{T}_p(t)\right|$$

$$\leq K_1 \left(\sum_{t=1}^{d} |r_t| \frac{{K_2}^p}{(p-1)!}\right)$$

Para $p > max\{r_0, 1, 2, \ldots, d\}$

(3.12) $$\frac{r_0}{(p-1)!}\sum_{N=p-1}^{(d+1)p-1} N!\, c_N \not\equiv o \bmod p$$

En efecto, como $p > r_0$

Si $$p/\left(\frac{\sum_{N=p-1}^{(d+1)p-1} N!\, c_N}{(p-1)!}\right)$$

$$p/\left[c_{p-1} + pc_p + \cdots + \{(d+1)p-1\} \ldots pc_{(d+1)p-1}\right]$$

Se tiene que,

$$p/c_{p-1}$$

Y en vista de que

$$|c_{p-1}| = |1^p 2^p \dots d^p| = \prod_{t=1}^{d} t^p$$

Se concluye que

$$p/t^p$$

Para algún $t = 1,2,\dots,d$

Entonces,

$$p/t$$

Lo cual es imposible, pues $p > t$. Así completamos la prueba de (3.12)

Por otro lado

$$p/\left(\sum_{t=1}^{d} \frac{r_t}{(p-1)!} \mathcal{P}_p(t)\right)$$

Por lo tanto;

$$\frac{r_0}{(p-1)!} \sum_{N=p-1}^{(d+1)p-1} N!\, c_N + \sum_{t=1}^{d} \frac{r_t}{(p-1)!} \mathcal{P}_p(t)$$

Es un entero distinto de cero

Como p es arbitrario, al escoger un p relativamente grande, es decir $p \to \infty$, se tendría en vista de que K_1 y K_2 no dependen de p y de (3.11) que:

$$0 < \left| \frac{r_0}{(p-1)!} \sum_{N=p-1}^{(d+1)p-1} N! c_N + \sum_{t=1}^{d} \frac{r_t}{(p-1)!} \mathcal{P}_p(t) \right| < 1$$

Lo cual es imposible□

Teorema 3.3. Para todo número racional $\frac{a}{b}$ distinto de cero, $e^{\sqrt{\frac{a}{b}}}$ es irracional.

La demostración es análoga a la del Teorema 3.1, por lo cual no seremos tan detallistas en la prueba.

Prueba:

Sea $\frac{a}{b} \in \mathbb{Q} - \{0\}$ y $\alpha = \sqrt{\frac{a}{b}}$.

Supongamos que $e^{\alpha} = \frac{r}{s} \in \mathbb{Q}$. Entonces,

$$r - se^{\alpha} = 0$$

Multiplicando por $r - se^{-\alpha}$ se tiene que

$$(r - se^{\alpha})(r - se^{-\alpha}) = 0$$

$$s^2 + r^2 - rse^{\alpha} - rse^{-\alpha} = 0$$

$$(s^2 + r^2) - rse^{\alpha} - rse^{-\alpha} = 0 \tag{3.13}$$

Sea

$$f(z) = b^p z^{p-1}(z - \alpha)^p (z + \alpha)^p$$

$$f(z) = z^{p-1}[b(z^2 - \alpha^2)]^p$$

$$= z^{p-1}\left[b\left(z^2 - \frac{a}{b}\right)\right]^p$$

(3.14) $$f(z) = z^{p-1}[bz^2 - a]^p$$

$$= z^{p-1}\sum_{n=0}^{p}\binom{p}{n}(bz^2)^{p-n}(-a)^n$$

$$= z^{p-1}\left[\binom{p}{0}(bz^2)^p + \binom{p}{1}(bz^2)^{p-1}(-a)^1 + \cdots + \binom{p}{p}(-a)^p\right]$$

$$= \binom{p}{0}b^p z^{3p-1} + \binom{p}{1}b^{p-1}(-a)z^{3p-3} + \cdots + \binom{p}{p}(-a)^p z^{p-1}$$

(3.15) $$f(z) = \binom{p}{o}(-a)^p z^{p-1} + \binom{p}{1}(-a)^{p-1}bz^{p+1} + \binom{p}{2}(-a)^{p-2}b^2z^{p+3} + \cdots$$

$$+\binom{p}{p}b^p z^{3p-1}$$

Así,

$$f(z) = \sum_{N=p-1}^{3p-1} c_N z^N \in \mathbb{Z}[z]$$

Multiplicando (3.13) por $\sum_{N=p-1}^{3p-1} N!\, c_N$

(3.16) $$(s^2 + r^2)\sum_{N=p-1}^{3p-1} N!\, c_N - rse^{\alpha}\sum_{N=p-1}^{3p-1} N!\, c_N - rse^{-\alpha}\sum_{N=p-1}^{3p-1} N!\, c_N = 0$$

Para $t = \alpha, -\alpha$

$$e^t \sum_{N=p-1}^{3p-1} N!\, c_N = \sum_{N=p-1}^{3p-1}\left(N!\, c_N \sum_{n=0}^{N-p}\frac{t^n}{n!}\right) + \sum_{N=p-1}^{3p-1}\left(N!\, c_N \sum_{n=N-p+1}^{N-1}\frac{t^n}{n!}\right)$$

$$+\sum_{N=p-1}^{3p-1}\left(N!\, c_N \sum_{n=N}^{\infty}\frac{t^n}{n!}\right)$$

Por el Lema 2.1

$$\sum_{n=1}^{p-1} f^n(z) = \sum_{N=p-1}^{3p-1}\left(N!\,c_N \sum_{n=N-p+1}^{N-1}\frac{z^n}{n!}\right) \tag{3.17}$$

Para $t = \alpha, -\alpha$; por el Lema 2.2

$$\sum_{n=1}^{p-1} f^n(t) = f^1(t) + f^2(t) + \cdots f^{p-1}(t)$$

$$= (p-1)t^{p-2}\left[b\left(t^2 - \frac{a}{b}\right)\right]^p + 2bpz^p\left[b\left(t^2 - \frac{a}{b}\right)\right]^{p-1}$$

$$+\sum_{k=0}^{2}\binom{2}{k}[t^{p-1}]^{(2-k)}\left[\left\{b\left(t^2 - \frac{a}{b}\right)\right\}^p\right]^{(k)} + \ldots$$

$$+\sum_{k=0}^{p-1}\binom{p-1}{k}[t^{p-1}]^{(p-1-k)}\left[\left\{b\left(t^2 - \frac{a}{b}\right)\right\}^p\right]^{(k)}$$

De donde

$$\sum_{n=1}^{p-1} f^n(t) = 0 \qquad \text{para} \qquad t = \alpha, -\alpha \tag{3.18}$$

Por lo tanto,

$$e^t \sum_{N=p-1}^{3p-1} N!\,c_N = \sum_{N=p-1}^{3p-1}\left(N!\,c_N \sum_{n=0}^{N-p}\frac{t^n}{n!}\right) + \sum_{N=p-1}^{3p-1}\left(N!\,c_N \sum_{n=N}^{\infty}\frac{t^n}{n!}\right)$$

$$= \mathcal{P}_p(t) + \mathcal{T}_p(t)$$

Reescribiendo (3.13)

$$(s^2 + r^2)\sum_{N=p-1}^{3p-1} N!\,c_N - rs\left(\mathcal{P}_p(\alpha) + \mathcal{T}_p(\alpha)\right) - rs\left(\mathcal{P}_p(-\alpha) + \mathcal{T}_p(-\alpha)\right) = 0$$

$$(s^2+r^2)\sum_{N=p-1}^{3p-1} N!\, c_N - rs\left(\mathcal{P}_p(\alpha)+\mathcal{P}_p(-\alpha)\right) = rs\left(\mathcal{T}_p(\alpha)+\mathcal{T}_p(-\alpha)\right)$$

Acotemos $\left|\mathcal{T}_p(\alpha)+\mathcal{T}_p(-\alpha)\right|$

Procediendo como lo hicimos para acotar $\mathcal{T}_p(\alpha)$

$$\left|\mathcal{T}_p(\alpha)+\mathcal{T}_p(-\alpha)\right| \leq \left|\mathcal{T}_p(\alpha)\right| + \left|\mathcal{T}_p(-\alpha)\right|$$

$$\leq e^{\alpha}\alpha^{3p-1}\sum_{N=p-1}^{3p-1}|c_N| + e^{-\alpha}\alpha^{3p-1}\sum_{N=p-1}^{3p-1}|c_N|$$

$$= e^{\alpha}\alpha^{3p-1}|a+b|^p + e^{-\alpha}\alpha^{3p-1}|a+b|^p \text{ por (3.15)}$$

$$= \alpha^{3p-1}|a+b|^p(e^{\alpha}+e^{-\alpha})$$

Igual que en el teorema 3.1, se demuestra que

$$\frac{1}{(p-1)!}\mathcal{P}_p(z) \in \mathbb{Z}[z]$$

Sea $\quad N = \left|\frac{b^{3p-1}(s^2+r^2)}{(p-1)!}\sum_{N=p-1}^{3p-1} N!\, c_N - \frac{b^{3p-1}rs}{(p-1)!}\left(\mathcal{P}_p(\alpha)+\mathcal{P}_p(-\alpha)\right)\right|$

$$0 < N = \left|\frac{b^{3p-1}rs}{(p-1)!}\left(\mathcal{T}_p(\alpha)+\mathcal{T}_p(-\alpha)\right)\right|$$

$$\leq \frac{|b^{3p-1}rs|}{(p-1)!}\alpha^{3p-1}|a+b|^p(e^{\alpha}+e^{-\alpha})$$

$$= \frac{|b^{3p}rs|}{b(p-1)!}\left[\left(\frac{a}{b}\right)^{\frac{1}{2}(3p-1)}\right]|a+b|^p\left(e^{\sqrt{\frac{a}{b}}}+e^{-\sqrt{\frac{a}{b}}}\right)$$

$$= \frac{|rs|\left(e^{\sqrt{\frac{a}{b}}}+e^{-\sqrt{\frac{a}{b}}}\right)}{b\left(\sqrt{\frac{a}{b}}\right)}\frac{(b^3)^p\left[\left(\frac{a}{b}\right)^{\frac{3}{1}}\right]^p|a+b|^p}{(p-1)!}$$

$$0 < N \leq K_1 \frac{K_2^p}{(p-1)!} \tag{3.19}$$

Por el Lema 2.6, N es un entero, así que al escoger un p relativamente grande, es decir $p \to \infty$, se tendría en vista de que K_1 y K_2 no dependen de p y de (3.19) que:

$$0 < N < 1$$

Lo cual es, nuevamente, imposible□

Corolario 3.2. El número π es irracional.

Prueba: Supongamos que π es racional, es decir $\pi = \frac{p}{q}$. Por el Teorema 3.3. $e^{\sqrt{-\frac{p^2}{q^2}}}$ es irracional; pero,

$$e^{\sqrt{-\frac{p^2}{q^2}}} = e^{(\sqrt{-1})\left(\frac{p}{q}\right)} = e^{i\pi} = -1$$

Luego nuestra suposición es falsa y π es irracional□

3.2. El teorema de Lindemann-Weierstrass.

Teorema 3.4. (Caso especial del Teorema de Lindemann-Weierstrass)

Sean $\alpha_1, \alpha_2, \dots, \alpha_M$ números algebraicos no nulos y distintos, donde $\{\alpha_1, \alpha_2, \dots, \alpha_M\}$ es un conjunto completo de conjugados. Supongamos que $\beta_0, \beta_1, \dots, \beta_M$ son enteros no nulos tal que si α_i y α_j son conjugados, se tiene que $\beta_i = \beta_j$. Entonces

$$\beta_0 + \sum_{m=1}^{M} \beta_m e^{\alpha_m} \neq 0 \tag{3.20}$$

Prueba:

Supongamos que

$$\beta_0 + \sum_{m=1}^{M} \beta_m e^{\alpha_m} = 0$$

Como $\{\alpha_1, \alpha_2, \dots, \alpha_M\}$ es un conjunto completo de conjugados, introduzcamos un cambio de variable para agrupar conjuntos de conjugados.

$$\alpha_{11}, \alpha_{12}, \dots, \alpha_{1M_1}$$

$$\alpha_{21}, \alpha_{22}, \dots, \alpha_{2M_2}$$

$$\alpha_{L1}, \alpha_{L2}, \dots, \alpha_{LM_L}$$

Donde $\{\alpha_{l1}, \alpha_{l2}, \dots, \alpha_{lM_l}\}$ es un conjunto de conjugados, $l = 1,2, \dots, L$.

De acuerdo con nuestro reordenamiento β_l denota los coeficientes

$$\beta_{l1} = \beta_{l2} = \cdots = \beta_{lM_l}$$

Así se tiene que

$$\beta_0 + \sum_{l=1}^{L} \beta_l \left(\sum_{m=1}^{M_l} e^{\alpha_{lm}}\right) = 0 \tag{3.21}$$

Sea

(3.22) $$f_l(z) = (z - \alpha_{l1})(z - \alpha_{l2}) \dots (z - \alpha_{lM_l})$$

Ya que $\{\alpha_{l1}, \alpha_{l2}, \dots, \alpha_{lM_l}\}$ es un conjunto completo de conjugados, por el Lema 2.8.

(3.23) $$f_l(z) \in \mathbb{Q}[z]$$

Entonces existe $d_l \in \mathbb{Z}$ tal que:

(3.24) $$d_l f_l(z) \in \mathbb{Z}[z]$$

Definamos el polinomio auxiliar

$$f(z) = (d_1 d_2 \dots d_L)^p z^{p-1} [f_1(z)]^p [f_2(z)]^p \dots [f_L(z)]^p \in \mathbb{Z}[z]$$

$$= \sum_{N=p-1}^{(M+1)p-1} c_N z^N \qquad \text{Ver observación 2.1}$$

Es claro que

$$c_{p-1} = \pm(d_1 d_2 \dots d_L \alpha_1 \alpha_2 \dots \alpha_M)^p \qquad \text{y}$$

$c_{p-1} \neq 0$, porque los α_m son distintos de cero, $m = 1, \dots, M$

Por el Lema 2.1

(3.25) $$\sum_{n=1}^{p-1} f^n(z) = \sum_{N=p-1}^{(M+1)p-1} \left(N!\, c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right)$$

Aplicando, reiteradamente, el Lema 2.2; se tiene que para $\alpha \in \{\alpha_1, \alpha_2, \dots, \alpha_M\}$

(3.26) $$\sum_{n=1}^{p-1} f^n(\alpha) = 0$$

Multiplicando (3.21) por $\frac{\sum_{N=p-1}^{(M+1)p-1} N!c_N}{(p-1)!}$, se tiene que:

$$\frac{\sum_{N=p-1}^{(M+1)p-1} N!\,c_N}{(p-1)!}\beta_0+\frac{\sum_{N=p-1}^{(M+1)p-1} N!\,c_N}{(p-1)!}\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}e^{\alpha_{lm}}\right)=0$$

(3.27) $\frac{\beta_0}{(p-1)!}\sum_{N=p-1}^{(M+1)p-1} N!\,c_N+\frac{1}{(p-1)!}\sum_{l=1}^{L}\beta_l\left(\sum_{N=p-1}^{(M+1)p-1} N!\,c_N\right)\left(\sum_{m=1}^{M_l}e^{\alpha_{lm}}\right)=0$

Ahora para cada $\alpha\in\{\alpha_1,\alpha_2,\dots,\alpha_M\}=\{\alpha_{11},\dots,\alpha_{1M_1},\dots,\alpha_{L1},\dots,\alpha_{LM_L}\}$

$$e^{\alpha}\sum_{N=p-1}^{(M+1)p-1} N!\,c_N=\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{\alpha^n}{n!}\right)+\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=N-p+1}^{N-1}\frac{\alpha^n}{n!}\right)$$

$$+\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=N}^{\infty}\frac{\alpha^n}{n!}\right)$$

Por (3.25) y (3.26)

$$e^{\alpha}\sum_{N=p-1}^{(M+1)p-1} N!\,c_N=\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{\alpha^n}{n!}\right)+\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=N}^{\infty}\frac{\alpha^n}{n!}\right)$$

$$=\mathcal{P}_p(\alpha)+\mathcal{T}_p(\alpha)$$

Donde

$\mathcal{P}_p(z)=\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{z^n}{n!}\right)$, Polinomio de aproximación

$\mathcal{T}_p(z)=\sum_{N=p-1}^{(M+1)p-1}\left(N!\,c_N\sum_{n=N}^{\infty}\frac{z^n}{n!}\right)$, Cola de la serie

Reescribiendo (3.27)

$$\frac{\beta_0}{(p-1)!}\sum_{N=p-1}^{(M+1)p-1} N!\,c_N+\frac{1}{(p-1)!}\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\left(\mathcal{P}_p(\alpha_{lm})+\mathcal{T}_p(\alpha_{lm})\right)\right)=0$$

Luego

(3.28) $\beta_0\sum_{N=p-1}^{(M+1)p-1}\frac{N!c_N}{(p-1)!}+\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\frac{\mathcal{P}_p(\alpha_{lm})}{(p-1)!}\right)=-\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right)$

Para $N=p-1$, la suma interior en $\mathcal{P}_p(z)$ es vacía y por lo tanto es igual a cero; lo que implica que

$$\mathcal{P}_p(z)=\sum_{N=p}^{(M+1)p-1}\left(N!\,c_N\sum_{n=0}^{N-p}\frac{z^n}{n!}\right)=p!\,c_p+(p+1)!\,c_{p+1}(1+z)$$

$$+(p+2)!\,c_{p+2}\left(1+z+\frac{z^2}{2!}\right)+\cdots\in\mathbb{Z}[z]$$

De donde

(3.29) $$\frac{1}{p!}\mathcal{P}_p(z),\frac{1}{(p-1)!}\mathcal{P}_p[z]\in\mathbb{Z}[z]$$

Como $gr(\mathcal{P}_p)=Mp-1$ y $\alpha_{l1},\alpha_{l2},\dots,\alpha_{lM_l}$ son los ceros de $f_l(z)\in\mathbb{Q}[z]$; por Lema 2.12 y (3.29)

$$\sum_{m=1}^{M_l}\frac{\mathcal{P}_p(\alpha_{lm})}{(p-1)!}=\frac{a_l}{d_l^{\,Mp-1}}\in\mathbb{Q}$$

Reescribiendo (3.28)

(3.30) $$\beta_0\sum_{N=p-1}^{(M+1)p-1}\frac{N!c_N}{(p-1)!}+\sum_{l=1}^{L}\frac{a_l\beta_l}{d_l^{\,Mp-1}}=-\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right)$$

Multiplicando (3.30) por $D^{Mp}=(d_1d_2\dots d_L)^{Mp}\in\mathbb{Z}$

$$\beta_0 D^{Mp} \sum_{N=p-1}^{(M+1)p-1} \frac{N!\, c_N}{(p-1)!} + \sum_{l=1}^{L} a_l \beta_l d_l \left(\frac{D}{d_l}\right)^{Mp} = -\sum_{l=1}^{L} \beta_l D^{Mp} \left(\sum_{m=1}^{M_l} \frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right)$$

Ya que $\frac{D}{d_l} \in \mathbb{Z}$, se tiene que

(3.31) $$N = \beta_0 D^{Mp} \sum_{N=p-1}^{(M+1)p-1} \frac{N! c_N}{(p-1)!} + \sum_{l=1}^{L} a_l \beta_l d_l \left(\frac{D}{d_l}\right)^{Mp} \in \mathbb{Z}$$

Reescribiendo (3.31)

(3.32) $$N = \beta_0 D^{Mp} c_{p-1} + \left(\beta_0 D^{Mp} \sum_{N=p}^{(M+1)p-1} \frac{N! c_N}{(p-1)!} + \sum_{l=1}^{L} a_l \beta_l d_l \left(\frac{D}{d_l}\right)^{Mp}\right)$$

Como p/a_l para cada l , entonces p divide al entero contenido en el paréntesis de (3.32)

Por hipótesis $\beta_0 \neq 0$, luego si escogemos $p > máx\{|\beta_0|, D, |c_{p-1}|\}$ se tiene que $\beta_0 D^{Mp} c_{p-1}$ es un entero distinto de cero y no divisible entre p; por lo tanto p no divide a N. Ahora podemos seguir reescribiendo (3.31) como sigue.

$$N = -\sum_{l=1}^{L} \beta_l D^{Mp} \left(\sum_{m=1}^{M_l} \frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right)$$

Luego

$$|N| = \left|\sum_{l=1}^{L} \beta_l D^{Mp} \left(\sum_{m=1}^{M_l} \frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right)\right|$$

Por la desigualdad triangular y en vista de que N es distinto de cero.

(3.33) $$0 < N \leq \sum_{l=1}^{L} \left(\sum_{m=1}^{M_l} \frac{|\beta_l D^{Mp} \mathcal{T}_p(\alpha_{lm})|}{(p-1)!}\right)$$

Empleando los mismos argumentos para acotar $\mathcal{T}_p(\alpha)$ en el teorema 3.1; obtenemos que

(3.34) $$|\mathcal{T}_p(\alpha)| \leq e^{\alpha}|\alpha|^{(M+1)p-1}\sum_{N=p-1}^{(M+1)p-1}|c_N|$$

Para todo $\alpha \in \{\alpha_1, \alpha_2, \dots, \alpha_M\}$

Modificando, ligeramente, los argumentos de la prueba del Lema 2.5

$$\max_{n=0,1,\dots,p}\left\{\left|\binom{p}{n}(-\alpha_l)^{p-n}\right|\right\} \leq |\alpha_l|^p\sum_{n=0}^{p}\binom{p}{n} = |2\alpha_l|^p$$

Y, en vista de que

$$f(z) = D^p z^{p-1}\prod_{l=1}^{M}(z-\alpha_l)^p = \sum_{N=p-1}^{(M+1)p-1} c_N z^N$$

Obtenemos

$$|c_N| \leq D^p\prod_{l=1}^{M}|2\alpha_l|^p \leq D^p((2\lambda)^M)^p$$

Donde $\lambda = máx\{|\alpha_1|, \dots, |\alpha_M|\}$

Ahora podemos seguir acotando $|\mathcal{T}_p(\alpha)|$, para todo $\alpha \in \{\alpha_1, \alpha_2, \dots, \alpha_M\}$. De (3.34).

$$|\mathcal{T}_p(\alpha)| \leq e^{\lambda}\lambda^{(M+1)p-1}(Mp+1)D^p((2\lambda)^M)^p$$

$$= e^{\lambda}\lambda^{(M+1)p-1}M^pD^p((2\lambda)^M)^p\ , \qquad Mp+1 \leq M^p$$

$$|\mathcal{T}_p(\alpha)| = \frac{e^{\lambda}}{\lambda}\lambda^{Mp}\lambda^p M^p D^p((2\lambda)^M)^p$$

$$= \frac{e^{\lambda}}{\lambda}(2^{M}\lambda^{2M})^{p}(\lambda MD)^{p}$$

$$= \frac{e^{\lambda}}{\lambda}((2\lambda^{2})^{M})^{p}(\lambda MD)^{p}$$

$$= K_1 {K_2}^{p}$$

Donde $K_1 = \frac{e^{\lambda}}{\lambda}$ y $K_2 = \lambda MD(2\lambda^2)^M$

Sea $B = máx\{|\beta_1|, |\beta_2|, \dots, |\beta_L|\}$, entonces de (3.33):

$$0 < N \leq \sum_{l=1}^{L}\left(\sum_{m=1}^{M_l}\frac{|\beta_l D^{Mp} T_p(\alpha_{lm})|}{(p-1)!}\right) \leq BMK_1 \frac{(D^M K_2)^p}{(p-1)!}$$

Como BMK_1 y $D^M K_2$ son constantes independientes de p, concluimos que para un p suficientemente grande

$$0 < |N| < 1$$

Lo cual es imposible, por lo tanto:

$$\beta_0 + \sum_{m=1}^{M} \beta_m e^{\alpha_m} \neq 0 \square$$

Teorema 3.5. (Lindemann-Weierstrass)

Sean $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_M$ $M+1$ números algebraicos distintos. Entonces,

$$e^{\alpha_0}, e^{\alpha_1}, \dots, e^{\alpha_M}$$

Son linealmente independientes sobre los números algebraicos, esto es, si $\beta_0, \beta_1, \dots, \beta_M$ son números algebraicos no todos nulos, entonces;

$$\textstyle\sum_{m=0}^{M} \beta_m e^{\alpha_m} \neq 0$$

Antes de presentar la prueba, un ejemplo sencillo nos puede ilustrar los detalles de la misma.

Ejemplo3.1:

Consideremos los números algebraicos $\alpha_0 = \sqrt{2}, \alpha_1 = \sqrt{3}, \beta_0 = \sqrt{5}, \beta_1 = -\sqrt{7}$.

El Teorema de Lindemann-Weiestrass nos garantiza que

$$\sqrt{5}e^{\sqrt{2}} - \sqrt{7}e^{\sqrt{3}} \neq 0 \tag{3.35}$$

Vamos a emplear el Teorema 3.4, para verificar (3.5).

Supongamos que

$$\sqrt{5}e^{\sqrt{2}} - \sqrt{7}e^{\sqrt{3}} = 0 \tag{3.36}$$

Multipliquemos (3.36) por expresiones análogas, reemplazando α_0 y α_1 por sus conjugados en todas las posibles combinaciones.

$$\left(\sqrt{5}e^{\sqrt{2}} - \sqrt{7}e^{\sqrt{3}}\right)\left(\sqrt{5}e^{-\sqrt{2}} - \sqrt{7}e^{\sqrt{3}}\right)\left(\sqrt{5}e^{\sqrt{2}} - \sqrt{7}e^{-\sqrt{3}}\right)\left(\sqrt{5}e^{-\sqrt{2}} - \sqrt{7}e^{-\sqrt{3}}\right) = 0$$

Luego

$$\begin{gathered}144 + 35e^{-2\sqrt{2}} + 35e^{2\sqrt{2}} + 35e^{-2\sqrt{3}} + 35e^{2\sqrt{3}} - 12\sqrt{35}e^{-\sqrt{2}-\sqrt{3}} \\ -12\sqrt{35}e^{\sqrt{2}-\sqrt{3}} - 12\sqrt{35}e^{-\sqrt{2}+\sqrt{3}} - 12\sqrt{35}e^{\sqrt{2}+\sqrt{3}} = 0\end{gathered}$$

Factorizando

$$\begin{gathered}144 + 35\left(e^{-2\sqrt{2}} + e^{2\sqrt{2}} + e^{-2\sqrt{3}} + e^{2\sqrt{3}}\right) \\ -12\sqrt{35}\left(e^{-\sqrt{2}-\sqrt{3}} + e^{\sqrt{2}-\sqrt{3}} + e^{-\sqrt{2}+\sqrt{3}} + e^{\sqrt{2}+\sqrt{3}}\right) = 0\end{gathered} \tag{3.37}$$

Si no fuese por el coeficiente irracional $-12\sqrt{35}$, aplicaríamos el Teorema 3.4 y la igualdad anterior no podría darse; por ende (3.35) quedaría verificado.

Observemos que

$$e^{-2\sqrt{2}}+e^{2\sqrt{2}}+e^{-2\sqrt{3}}+e^{2\sqrt{3}},\quad e^{-\sqrt{2}-\sqrt{3}}+e^{\sqrt{2}-\sqrt{3}}+e^{-\sqrt{2}+\sqrt{3}}+e^{\sqrt{2}+\sqrt{3}}$$

Son sumas exponenciales conjugadas completas

Multipliquemos (3.37) por una expresión análoga, reemplazando $-12\sqrt{35}$ por su conjugado $12\sqrt{35}$

$$\begin{aligned}\Big[144+35\left(e^{-2\sqrt{2}}+e^{2\sqrt{2}}+e^{-2\sqrt{3}}+e^{2\sqrt{3}}\right)&\\ -12\sqrt{35}\left(e^{-\sqrt{2}-\sqrt{3}}+e^{\sqrt{2}-\sqrt{3}}+e^{-\sqrt{2}+\sqrt{3}}+e^{\sqrt{2}+\sqrt{3}}\right)\Big]\Big[144&\\ +35\left(e^{-2\sqrt{2}}+e^{2\sqrt{2}}+e^{-2\sqrt{3}}+e^{2\sqrt{3}}\right)&\\ +12\sqrt{35}\left(e^{-\sqrt{2}-\sqrt{3}}+e^{\sqrt{2}-\sqrt{3}}+e^{-\sqrt{2}+\sqrt{3}}+e^{\sqrt{2}+\sqrt{3}}\right)\Big]&=0\end{aligned}$$

Luego

$$\begin{aligned}5476+1225e^{-4\sqrt{2}}+1225e^{4\sqrt{2}}+1225e^{-4\sqrt{3}}+1225e^{4\sqrt{3}}&\\ -2590e^{-2\sqrt{2}-2\sqrt{3}}-2590e^{2\sqrt{2}-2\sqrt{3}}-2590e^{-2\sqrt{2}+2\sqrt{3}}&\\ -2590e^{2\sqrt{2}+2\sqrt{3}}&=0\end{aligned}$$

Factorizando

$$5476 + 1225\left(e^{-4\sqrt{2}} + e^{4\sqrt{2}} + e^{-4\sqrt{3}} + e^{4\sqrt{3}}\right)$$

$$-2590\left(e^{-2\sqrt{2}-2\sqrt{3}} + e^{2\sqrt{2}-2\sqrt{3}} + e^{-2\sqrt{2}+2\sqrt{3}} + e^{2\sqrt{2}+2\sqrt{3}}\right) = 0$$

Por el Teorema 3.4, la igualdad anterior no puede darse; por lo tanto (3.35) queda verificado

Prueba del Teorema de Lindemann-Weierstrass.

Supongamos que existen números algebraicos no todos nulos, tales que:

(3.38) $$\sum_{m=0}^{M} \beta_m e^{\alpha_m} = 0$$

Multiplicando (3.38) por expresiones análogas, reemplazando cada α_m por sus conjugados en todas las posibles combinaciones.

$$\prod_{\substack{\rho_m \text{ conjugado de } \alpha_m \\ m=0,1,\ldots,M}} \left(\beta_0 e^{\rho_0} + \beta_1 e^{\rho_1} + \cdots + \beta_M e^{\rho_M}\right) = 0$$

Si cada α_m tiene grado n_m, el producto en (3.38) está compuesto de $\prod_{m=0}^{M} n_m$ factores.

En vista de la simetría con respecto a los conjugados, después de multiplicar y factorizar los coeficientes comunes se llega a:

(3.39) $$k_0E_0 + k_1E_1 + \cdots + k_LE_L = 0$$

Donde los $k_l$son combinaciones lineales enteras de productos de los β_m y E_l son sumas exponenciales conjugadas completas; para $0 \leq l \leq L$ y $0 \leq m \leq M$.

Por el Lema 2.7 No todos los k_l son nulos. Sin pérdida de generalidades, asumamos que todos los k_l son distintos de cero.

Ahora transformamos los coeficientes en enteros, multiplicando (3.39) por expresiones análogas, reemplazando cada k_l por sus conjugados en todas las posibles combinaciones.

$$\prod_{\substack{\gamma_l \text{conjugado de } k_l \\ l=0,1,\ldots L}} (\gamma_0 E_0 + \gamma_1 E_1 + \cdots + \gamma_L E_L) = 0$$

Al expandir este producto y factorizar coeficientes comunes, obtenemos:

(3.40) $$\delta_0 \varepsilon_0 + \delta_1 \varepsilon_1 + \cdots + \delta_J \varepsilon_J = 0$$

Donde los δ_j son polinomios simétricos en los β_m y sus conjugados, con coeficientes enteros; además los ε_k son productos de los E_l. Por el Lema 2.13 los δ_j son números racionales y por el Lema 2.7 no todos se anulan.

Sin pérdida de generalidades podemos asumir que todos los δ_j son enteros distintos de cero, en caso contrario se eliminan los términos nulos y se multiplica por el mínimo común múltiplo de los denominadores de los δ_j.

Por el Lema 2.15 ε_j son sumas exponenciales conjugadas completas, de tal manera que en los exponentes se puede tomar conjugados dos a dos y llevar (3.40) a las condiciones del segundo término del lado izquierdo de (3.20).

Para que (3.40) reúna todas las condiciones de (3.20) es necesario que para algún k, $\varepsilon_k = e^0 = 1$. Supongamos que $\varepsilon_k \neq 1, \forall k$.

Consideremos $\varepsilon_0 = e^{v_1} + e^{v_2} + \cdots + e^{v_J}$, donde $v_1, v_2, \ldots, v_J$ son números algebraicos no nulos y constituyen un conjunto de conjugados.

Sea $\varepsilon_0' = e^{-v_1} + e^{-v_2} + \cdots + e^{-v_J}$. Es claro que ε_0' es una suma exponencial conjugada completa.

Por el Lema 2.15, $\varepsilon_0'\varepsilon_0$ también es una suma exponencial conjugada completa. Esta suma contiene al menos J veces e^0, por ende:

$$\varepsilon_0'\varepsilon_0 = J + \varepsilon_0''$$

donde ε_0'' es alguna suma exponencial conjugada completa.

Como para cada $k_1 \neq k_2$, los exponentes que aparecen en ε_{k_1} son distintos de los que aparecen en ε_{k_2}; se tiene que para $k \neq 0$, $\varepsilon_0'\varepsilon_k$ no contiene ningún término e^0. Multiplicando (3.40) por ε_0', obtenemos

$$J\delta_0 + \delta_0\varepsilon_0'' + \delta_1\varepsilon_1'' + \delta_2\varepsilon_2'' + \cdots + \delta_k\varepsilon_k'' = 0 \tag{3.41}$$

Donde los $\delta_k$son enteros no nulos y cada ε_k'' es una suma exponencial conjugada completa sin término e^o, por ende $J\delta_0$ es el único termino libre de factores exponenciales.

Por el Teorema 3.4, (3.41) es distinto de cero y por lo tanto (3.38) también□

Corolario 3.3: (Teorema de Hermite-Lindemann)

El número e^α es trascendente para cualquier número algebraico α distinto de cero.

Prueba:

Sea $\alpha \in \overline{\mathbb{Q}} - \{0\}$, y supongamos que e^α es algebraico; es decir,

$$e^{\alpha} = \beta$$

Para algún número algebraico β, obviamente distinto de cero.

Si $\beta_1 \in \overline{\mathbb{Q}} - \{0\}$, entonces

$$\beta_1 e^{\alpha} = \beta_1 \beta$$

$$-\beta_1 \beta + \beta_1 e^{\alpha} = 0$$

$$\beta_0 e^{0} + \beta_1 e^{\alpha} = 0$$

Lo cual contradice el Teorema 3.5, pues $0, \alpha$ son números algebraicos distintos y $\beta_0 = -\beta_1 \beta, \beta_1$ son no nulos. Luego e^{α} es trascendente□

Corolario 3.4: El número π es trascendente.

Prueba.

Supongamos que π es algebraico. Como el producto de dos números algebraicos es algebraico, se tiene que

$$i\pi \in \overline{\mathbb{Q}} - \{0\}$$

En vista del corolario 3.3:

$$e^{i\pi} = -1$$

es trascendente, lo cual es totalmente falso; por lo tanto π es trascendente.

Corolario 3.5: Si $\alpha \in \overline{\mathbb{Q}} - \{0,1\}$, entonces $log\alpha$ es trascendente.

Prueba:

Supongamos que $log\alpha$ es algebraico. Como $log\alpha \neq 0$, pues $\alpha \neq 1$; por el corolario 3.3 $e^{log\alpha} = \alpha$ es trascendente, lo que nos lleva a una contradicción. Luego nuestra suposición es falsa y $log\alpha$ es trascendente.□

El siguiente corolario nos permite generar números trascendentes, tanto como lo deseemos.

Corolario 3.6: Se $\alpha_0, \alpha_1, \ldots, \alpha_M$ $M+1$ números algebraicos distintos y no nulos. Entonces para números algebraicos no nulos $\beta_0, \beta_1, \ldots, \beta_M$; el número

$$\sum_{m=0}^{M} \beta_m e^{\alpha_m}$$

es trascendente.

Prueba:

Supongamos lo contrario, es decir,

$$\sum_{m=0}^{M} \beta_m e^{\alpha_m} = -\beta_{M+1} \in \overline{\mathbb{Q}} - \{0\}$$

Entonces,

$$\sum_{m=0}^{M+1} \beta_m e^{\alpha_m} = 0$$

Donde $\alpha_{M+1} = 0$ y por lo tanto, $\alpha_0, \alpha_1, \ldots, \alpha_M, \alpha_{M+1}$ son números algebraicos distintos y $e^{\alpha_0}, e^{\alpha_1}, \ldots, e^{\alpha_M}$ no son linealmente independientes sobre $\overline{\mathbb{Q}}$; lo que contradice el Teorema 3.5. Luego nuestra suposición es falsa y

$$\sum_{m=0}^{M} \beta_m e^{\alpha_m}$$

es trascendente□

3.3. Irracionalidad de e^π

Teorema 3.6: e^π es irracional

Prueba:

Supongamos que

$$e^\pi = \frac{r}{s} \in \mathbb{Q}$$

Como $e^\pi > 1$, se tiene que $s < r$

Sea

(3.41) $$D = 2\sqrt{KT} \in \mathbb{Z}\,, \text{ donde } T > r^{(16K)^8}$$

Consideremos el polinomio no nulo

$$p(x,y) = \sum_{m=0}^{D-1} \sum_{m=0}^{D-1} a_{mn} x^m y^n \in \mathbb{Z}[x,y]$$

Donde a_{mn} son las soluciones enteras no nulas que garantiza el Lema de Siegel en del sistema del ejemplo 2.7 del Capítulo N°2.

Para $$0 \le m \le D-1, 0 \le n \le D-1$$

Sabemos que

$$|a_{mn}| < 1 + (D^2(T+1)(2D)^{2T} r^{KD})^{\frac{2KT}{D^2-2KT}},$$

Y por (3.41) $$\frac{2KT}{D^2-2KT} = 1$$

Luego

$$|a_{mn}| < 1 + (D^2(T+1)(2D)^{2T} r^{KD})$$

Como $|a_{mn}|, (D^2(T+1)(2D)^{2T} r^{KD}) \in \mathbb{Z}^+$; se tiene que

$$|a_{mn}| \leq (D^2(T+1)(2D)^{2T}r^{KD})$$

$$\leq 4KT(T+1)\left[2\left(2\sqrt{KT}\right)\right]^{2T} r^{2K\sqrt{KT}}$$

$$\leq 4KT(T+1)(16KT)^T r^{2K^{\frac{3}{2}}T^{\frac{1}{2}}}$$

$$\leq (4KT)(4KT)(16KT)^T \left(r^{2K^{\frac{3}{2}}}\right)^{T^{\frac{1}{2}}}$$

$$\leq (4KT)^2(16KT)^T \left(r^{2K^{\frac{3}{2}}}\right)^{T}$$

$$\leq (4KT)^2 16^T K^T \left(r^{2K^{\frac{3}{2}}}\right)^{T} T^T$$

Por la propiedad 2.3.

$$|a_{mn}| < T^{\frac{T}{8}} T^{\frac{T}{8}} T^{\frac{T}{8}} T^{\frac{T}{8}} T^T$$

De donde

(3.42) $$máx\{|a_{mn}|\} < T^{1.5T}$$

Sea $f(z) = p\left(e^z, e^{iz}\right)$. Entonces

$$f(z) = \sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}(e^z)^m\left(e^{iz}\right)^n$$

(3.43) $$f(z) = \sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}e^{(m+ni)z}$$

Luego,

(3.44) $$f^t(z) = \sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}(m+ni)^t e^{(m+ni)z} \qquad 0 \leq t \leq T-1$$

Ahora si evaluamos las derivadas de f en $z = k\pi$, $k = 1,2,\dots,K$; y en vista de que $e^{k\pi} = \left(\frac{r}{s}\right)^k$ y $e^{ik\pi} = (-1)^k$, obtenemos que

(3.45) $$f^t(k\pi) = \sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}(m+ni)^t\left(\frac{r}{s}\right)^{km}(-1)^{kn} = \rho_{t,k}$$

Para $\quad 1 \le k \le K, \quad 0 \le t \le T-1$

Multiplicando (3.45) por $s^{k(D-1)}$, llegamos a la siguiente igualdad

(3.46) $$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1}(m+ni)^t r^{km} s^{k(D-1-m)}(-1)^{kn} a_{mn} = s^{k(D-1)}\rho_{t,k}$$

Para $\quad 1 \le k \le K, \quad 0 \le t \le T-1$

En vista de que en las KT ecuaciones en (3.46) aparecen involucrados números complejos, obtenemos las siguientes $2KT$ ecuaciones

$$Re\left(\sum_{m=0}^{D-1}\sum_{n=0}^{D-1}(m+ni)^t r^{km} s^{k(D-1-m)}(-1)^{kn} a_{mn}\right) = Re\left(s^{k(D-1)}\rho_{t,k}\right), \text{ y}$$

$$Im\left(\sum_{m=0}^{D-1}\sum_{n=0}^{D-1}(m+ni)^t r^{km} s^{k(D-1-m)}(-1)^{kn} a_{mn}\right) = Im\left(s^{k(D-1)}\rho_{t,k}\right)$$

Lo que equivale a

$$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} Re[(m+ni)^t] r^{km} s^{k(D-1-m)}(-1)^{kn} a_{mn} = s^{k(D-1)}\mathrm{Re}(\rho_{t,k})$$

$$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} Im[(m+ni)^t] r^{km} s^{k(D-1-m)}(-1)^{kn} a_{mn} = s^{k(D-1)}\mathrm{Im}(\rho_{t,k})$$

Para $\quad 1 \le k \le K, \quad 0 \le t \le T-1$

En virtud del ejemplo 2.7.

$$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} Re[(m+ni)^t] r^{km} s^{k(D-1-m)}(-1)^{kn} a_{mn} = 0$$

$$\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} Im[(m+ni)^t]r^{km}s^{k(D-1-m)}(-1)^{kn}a_{mn}=0$$

Luego $f(z)=p(e^z,e^{iz})$, satisface la siguiente condición

$$f^t(k\pi)=0 \qquad k=1,2,\dots.K \qquad t=0,1,2,\dots.,T-1$$

Ya que $p(x,y)\neq 0, f(z)\neq 0$. Luego la serie de potencia para $f(z)$ centrada en $z=k\pi$ tiene al menos un coeficiente no nulo. Sea M el entero más pequeño tal que

$$f^M(k_0\pi)\neq 0 \qquad\qquad 1\leq k_0\leq K$$

Así, Mdepende del parámetro K y $M\geq T$

De (3.44)

$$f^M(z)=\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}(m+ni)^M e^{(m+ni)z}$$

Al evaluar f^M en $k_0\pi$ se tiene que

$$f^M(k_0\pi)=\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}(m+ni)^M\left(\frac{r}{s}\right)^{k_0m}(-1)^{k_0n}$$

Multiplicando la previa identidad por $s^{k_0(D-1)}$ se tiene que,

$$s^{k_0(D-1)}f^M(k_0\pi)=\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}(m+ni)^M(r)^{k_0m}s^{k_0(D-1-m)}(-1)^{k_0n}$$

$$=\sum_{m=0}^{D-1}\sum_{n=0}^{D-1} a_{mn}\left[\sum_{l=0}^{M}\binom{M}{l}m^M(ni)^{M-l}\right]r^{k_0m}s^{k_0(D-1-m)}(-1)^{k_0n}$$

$$=A_{k_0}+iB_{k_0}$$

De donde

(3.47) $$s^{k_0(D-1)} f^M(k_0\pi) = A_{k_0} + iB_{k_0} \in \mathbb{Z}(i)$$

Por el Lema 2.29, podemos considerar la función analítica

(3.48) $$G(z) = \frac{f(z)}{(z-\pi)^M(z-2\pi)^M \dots (z-k\pi)^M}$$

Como f es analítica, podemos expresarla como una serie de potencia centrada en $z = k_0\pi$, es decir,

$$f(z) = \sum_{n=0}^{\infty} \frac{f^n(k_0\pi)}{n!}(z-k_0\pi)^n$$

$$= \sum_{n=M}^{\infty} \frac{f^n(k_0\pi)}{n!}(z-k_0\pi)^n$$

$$= (z-k_0\pi)^M \sum_{n=M}^{\infty} \frac{f^n(k_0\pi)}{n!}(z-k_0\pi)^{n-M}$$

De donde

$$\frac{f(z)}{(z-k_0\pi)^M} = \sum_{n=M}^{\infty} \frac{f^n(k_0\pi)}{n!}(z-k_0\pi)^{n-M}$$

$$= \frac{f^M(k_0\pi)}{M!} + \frac{f^{M+1}(k_0\pi)}{(M+1)!}(z-k_0\pi)^1 + \frac{f^{M+2}(k_0\pi)}{(M+2)!}(z-k_0\pi)^2 + \cdots$$

Luego por (3.48)

$$G(z) \prod_{\substack{1\le k\le K \\ k\ne k_0}} (z-k\pi)^M = \frac{f^M(k_0\pi)}{M!} + \frac{f^{M+1}(k_0\pi)}{(M+1)!}(z-k_0\pi)^1$$

$$+ \frac{f^{M+2}(k_0\pi)}{(M+2)!}(z-k_0\pi)^2 + \cdots$$

En particular para $z = k_0\pi$ se tiene que

$$G(k_0\pi)\prod_{\substack{1\le k\le K\\ k\neq k_0}}(k_0\pi-k\pi)^M=\frac{f^M(k_0\pi)}{M!}+\frac{f^{M+1}(k_0\pi)}{(M+1)!}(k_0\pi-k_0\pi)^1$$

$$+\frac{f^{M+2}(k_0\pi)}{(M+2)!}(k_0\pi-k_0\pi)^2+\cdots$$

Luego

$$f^M(k_0\pi)=M!\,G(k_0\pi)\prod_{\substack{1\le k\le K\\ k\neq k_0}}(k_0\pi-k\pi)^M$$

Por (3.47)

$$\left|s^{k_0(D-1)}f^M(k_0\pi)\right|^2=\left|s^{k_0(D-1)}M!\,G(k_0\pi)\prod_{\substack{1\le k\le K\\ k\neq k_0}}(k_0\pi-k\pi)^M\right|$$

Es un entero positivo.

Ahora si $0.1R>K\pi$, entonces $0.9R<R-K\pi$ y, por el Principio del Módulo Máximo

$$|G(k_0\pi)|\le\underbrace{max}_{|z|\le R}(|G(z)|)=max|G(z)|_R\le\frac{|f(z)|_R}{\underbrace{min}_{1\le k\le K}(|R-k\pi|)^{KM}}$$

$$=\frac{|f(z)|_R}{|R-K\pi|^{KM}}$$

$$<\frac{|f(z)|_R}{(0.9R)^{KM}}$$

Para seguir acotando el lado derecho de la desigualdad anterior, haremos uso de (3.43), el grado del polinomio y el valor de R.

En vista de que

$$\left|e^{(m+ni)R}\right| = e^{mR} < e^{(D-1)R} < e^{2DR}$$

Por (3.43)

$$|f(z)|_R \leq D^2 max\{|a_{mn}|\}e^{2DR}$$

$$< (4KT)T^{1.5T}e^{4R\sqrt{KT}} \qquad \text{Por (3.42)}$$

$$< T^{\frac{T}{16}}\, T^{1.5T}e^{4R\sqrt{KT}} \qquad \text{Por la propiedad 2.3}$$

$$T^{\frac{T}{16}}\, T^{1.5T}e^{4R\sqrt{KT}} < T^{1.5625T}e^{4R\sqrt{KT}}$$

$$< T^{1.6T}e^{4R\sqrt{KT}}$$

$$= e^{1.6T.logT}e^{4R\sqrt{KT}}$$

Así,

(3.49) $$|f(z)|_R < e^{1.6TlogT}e^{4R\sqrt{KT}}$$

Como $|\mathcal{A}| = \left|s^{K(D-1)}f^M(k_0\pi)\right|^2$ es un entero positivo, pues $k_0 \leq K$; se tiene que:

$$log|\mathcal{A}| = log\left|s^{K(D-1)}f^M(k_0\pi)\right|^2$$

$$= 2log\left|s^{K(D-1)}f^M(k_0\pi)\right|$$

$$= 2log\left|s^{K(D-1)}M!\,G(k_0\pi)\prod_{\substack{1\leq k\leq K\\ k\neq k_0}}(k_0\pi - k\pi)^M\right|$$

$$\leq 2\left[logs^{K(D-1)} + logM^M + log|G(k_0\pi)| + log\prod_{\substack{1\leq k\leq K\\ k\neq k_0}}|\pi(k-k_0)|^M\right]$$

$$< 2\left[logs^{K(D-1)} + logM^M + log|G(k_0\pi)| + Klog(K\pi)^M\right]$$

$$< 2\left[K(D-1)logs + MlogM + log\left(\frac{|f(z)|_R}{(0.9R)^{KM}}\right) + MKlog(K\pi)\right]$$

$$log|\mathcal{A}| < 2[K(D-1)logs + MlogM + log|f(z)|_R - KMlog(0.9R)$$
$$+KMlog(K\pi)]$$

Ahora por (3.49)

$$log|\mathcal{A}| < 2[K(D-1)logs + MlogM + log\left(e^{1.6TlogT}e^{4R\sqrt{KT}}\right)$$
$$-KMlog(0.9R) + KMlog(K\pi)]$$

(3.50) $$log|\mathcal{A}| < 2[K(D-1)logs + MlogM + 1.6TlogT + 4R\sqrt{KT}$$
$$-KMlog(0.9R) + KMlog(K\pi)]$$

Si tomamos $R = \frac{10}{9}\sqrt{M}, K = 24$ y $T > máx\left\{r^{((16)(24))^8}, (24)^3s^2,\ (24\pi)^{12}\right\}$

se tiene que

$$\begin{aligned} K(D-1)logs &= 24\left(2\sqrt{24T}-1\right)logs \\ &< 24\left(2\sqrt{24T}\right)logT \\ &< 2(24)^{\frac{3}{2}}T^{\frac{1}{2}}logM \\ &= 2[(24)^3]^{\frac{1}{2}}T^{\frac{1}{2}}logM \\ &< 2T^{\frac{1}{2}}T^{\frac{1}{2}}logM \\ &< 2M^{\frac{1}{2}}M^{\frac{1}{2}}logM \\ &= 2MlogM \end{aligned}$$

De donde

(3.51) $$K(D-1)logs < 2MlogM$$

Por otro lado

$$(3.52) \qquad KMlog(K\pi) = 24Mlog(24\pi)$$
$$= 2(12)Mlog(24\pi)$$
$$= 2Mlog(24\pi)^{12}$$
$$< 2MlogM$$

y

$$(3.53) \qquad 4R\sqrt{KT} = 4\frac{10}{9}\sqrt{M}\sqrt{24T}$$
$$\leq 4\left(\frac{10}{9}\right)(24)^{\frac{1}{2}}\sqrt{M}\sqrt{M}$$
$$= 2M\left[\left(\frac{20}{9}\right)(24)^{\frac{1}{2}}\right]$$
$$< 2M(12)$$
$$< 2Mlog(24\pi)^{12}$$
$$< 2MlogM$$

Además, es claro que

$$(3.54) \qquad MlogM < 2MlogM$$

$$(3.55) \qquad 1.6TlogT < 2MlogM$$

Ahora por (3.51), (3.52), (3.53), (3.54) y (3.55),

$$log|\mathcal{A}| < 2[2MlogM + 2MlogM + 2MlogM + 2MlogM$$
$$+2MlogM - 24Mlog\left((0.9)\left(\frac{10}{9}\right)\sqrt{M}\right)]$$

$$log|\mathcal{A}| < 2[2MlogM + 2MlogM + 2MlogM + 2MlogM$$
$$+2MlogM - 24Mlog\left(M^{\frac{1}{2}}\right)]$$

$$log|\mathcal{A}| < 2[10MlogM - 12MlogM]$$

(3.56) $$log|\mathcal{A}| < -4MlogM$$

Así si se cumplen las condiciones impuestas a R, K, T y $D = 2\sqrt{24T}$ es un entero; por (3.56)

$$log|\mathcal{A}| < -4MlogM$$
$$< -4TlogT < 0$$

Luego

$$0 < |\mathcal{A}| < 1$$

Lo cual es imposible y; por lo tanto nuestra suposición es falsa y así

es irracional.□

CAPITULO N° 4

PRUEBAS DEL TEOREMA DE GELFOND-SCHNEIDER

El presente capítulo presenta las soluciones dadas, independientemente, por Gelfond y Schneider en 1934 del séptimo problema planteado por Hilbert, en el Segundo Congreso Internacional de Matemáticos de 1900. Primeramente formulémoslo como se conoce en la actualidad.

4.1. Teorema de Gelfond-Schneider.

Damos dos formulaciones equivalentes al teorema que resuelve el séptimo problema de Hilbert.

Teorema 4.1. Si α y β son números algebraicos con $\alpha \neq 0, \alpha \neq 1$, y si $\beta \notin \mathbb{Q}$, entonces algún valor de α^{β} es trascendente.

Teorema 4.2. Si α y γ son números algebraicos no nulos y si $\alpha \neq 1$, entonces $\frac{\log\gamma}{\log\alpha}$ es racional o trascendente.

Prueba de la equivalencia.

<u>El Teorema 4.1 implica el Teorema 4.2</u>.

Supongamos que $\beta = \frac{\log\gamma}{\log\alpha}$ es irracional algebraico, entonces $\gamma = \alpha^{\beta}$ es trascendente por el Teorema 4.1; contradiciendo la hipótesis del Teorema 4.2.

El Teorema 4.2 implica el Teorema 4.1

Supongamos que $\gamma = \alpha^{\beta}$ es un número algebraico distinto de cero, entonces β es racional o trascendente por el Teorema 4.2, contradiciendo la hipótesis del teorema 4.1.□

4.2. Prueba de Gelfond

Sea $\alpha, \beta \in \tilde{\mathbb{Q}}$; con $\alpha \neq 0,1$ y $\beta \notin \mathbb{Q}$.

Supongamos que $\gamma = \alpha^{\beta} = e^{\beta(\log\alpha)} \in \tilde{\mathbb{Q}}$ y $\theta \in \tilde{\mathbb{Q}}$ tal que:

$$\alpha, \beta, \gamma \in \mathbb{Q}(\theta) \text{ con } [\mathbb{Q}(\theta):\mathbb{Q}] = h$$

Sea $m = 2h + 3$. Escojamos $q > 4m^2$ de tal forma que q^2 sea múltiplo de $2m$, $n = \frac{q^2}{2m}$ y q un cuadrado perfecto. Entonces, es claro que $n > q$ y $mn < q^2 = t$.

Sea

$$p(x,y) = \sum_{i=1}^{q} \sum_{j=1}^{q} \xi_{ij} x^i y^j$$

Donde los ξ_{ij} son enteros algebraicos en el cuerpo $\mathbb{Q}(\theta)$ que se obtienen de la solución del sistema (2.25) del ejemplo 2.8.

Definamos la función entera,

$$f(z) = p(e^z, e^{\beta z}) \tag{4.1}$$

$$= \sum_{i=1}^{q} \sum_{j=1}^{q} \xi_{ij} (e^z)^i (e^{\beta z})^j$$

$$= \sum_{i=1}^{q} \sum_{j=1}^{q} \xi_{ij} e^{(i+\beta j)z}$$

La $a - esíma$ derivada de f viene dada por,

$$f^{a}(z) = \sum_{i=1}^{q} \sum_{j=1}^{q} \xi_{ij} (i + \beta j)^a e^{(i+\beta j)z} \tag{4.2}$$

Del ejemplo 2.8, sabemos que

$$(4.3) \qquad \|\xi_{ij}\| < c + c\left[c(2mn)c_3^n n^{\frac{n}{2}}\right]^{\frac{mn}{2mn-mn}}$$

$$= c + 2c^2mnc_3^n n^{\frac{n}{2}}$$

$$< 3c^2mnc_3^n n^{\frac{n}{2}}$$

$$< 3c^2 4^n c_3^n n^{\frac{n}{2}}$$

$$< 3^n (c^2)^n 4^n c_3^n n^{\frac{n}{2}}$$

$$= c_4^n n^{\frac{n}{2}}$$

Donde c es la constante del Lema 2.24, y

$$(4.4) \quad c_4 = 12c^2c_3, \qquad c_3 = (c_1c_2)^{2m+1}\sqrt{2m}, \quad c_2 = max\{\|\alpha\|, \|\gamma\|, 1 + \|\beta\|)$$

$$(4.5) \qquad f^a(b(log\alpha)) = 0 \qquad a = 0,1,\dots, n-1; b = 1,2,\dots, m$$

Ahora bien, $f^a(b(log\alpha))$ no se anula para todos los valores de $a = 0,1,\dots,t-1; b = 1,2,\dots,m$. Para demostrar esta afirmación podemos, sin pérdida de generalidades, fijar $b = 1$ y suponer lo contrario, es decir:

$$f^a(log\alpha) = 0 \qquad a = 0,1,2,\dots,t-1$$

Luego

$$\sum_{i=1}^{q}\sum_{j=1}^{q} \xi_{ij}(i + \beta j)^a e^{(i+\beta j)log\alpha} = 0$$

Como los ξ_{ij} no son todos nulos y en vista de que tenemos t ecuaciones en t incógnitas, por el lema 2.16,

$$D = det\left|(i + \beta j)^a e^{(i+\beta j)log\alpha}\right| = 0$$

Donde

$$D = \begin{vmatrix} e^{(1+\beta)\log\alpha} & e^{(1+2\beta)\log\alpha} & \dots & e^{(q+q\beta)\log\alpha} \\ (1+\beta)e^{(1+\beta)\log\alpha} & (1+2\beta)e^{(1+2\beta)\log\alpha} & \dots & (q+q\beta)e^{(q+q\beta)\log\alpha} \\ & \vdots & & \\ (1+\beta)^{t-1}e^{(1+\beta)\log\alpha} & (1+2\beta)^{t-1}e^{(1+2\beta)\log\alpha} & \dots & (q+q\beta)^{t-1}e^{(q+q\beta)\log\alpha} \end{vmatrix}$$

$$= det|(i+j\beta)^{a}| \prod_{\substack{1\le i\le q \\ 1\le j\le q}} e^{(i+j\beta)\log\alpha}$$

En vista de que $e^{(i+j\beta)\log\alpha} \neq 0, \forall i,j$; se tiene que

$$det|(i+j\beta)^{a}| = 0$$

Pero esta última expresión es el determinante de Vandermonde y por el Lema 2.17, se anula si

$$i + j\beta = i' + j'\beta$$

para algunos i,j,i',j' distintos; lo cual es imposible pues β sería racional, contradiciendo la hipótesis; por lo tanto, existe un entero $p \geq n$ y B, con $1 \leq B \leq m$; tal que

(4.6) $\qquad f^{a}(b(\log\alpha)) = 0 \qquad$ y $\qquad \mu = f^{p}(B(\log\alpha)) \neq 0$

Para $a = 0,1,\dots,p-1$; $b = 1,2,3,\dots,m$

De paso (4.6) revela que $f(z)$ no es idénticamente nula.

Por el Lema 2.20, existe un entero c_1 tal que

$$c_1\alpha, \quad c_1\beta, \quad c_1\gamma$$

son enteros algebraicos en $\mathbb{Q}(\theta)$, y en vista de que los ξ_{ij} también están en $\mathbb{Q}(\theta)$, procediendo como en el ejemplo 2.8, llegamos a que

$$c_1^{p+2mq}\mu$$

es un entero algebraico en $\mathbb{Q}(\theta)$.

Como $q < n \leq p$,se tiene que

$$c_1^{p+2mq} < c_1^{p+2mp} = (c_1^{1+2m})^p = c_5^p$$

Donde $c_5 = c_1^{1+2m}$ y c_1 , m son independientes de p y n.

Es claro que $c_5^p\mu$ también es un entero algebraico en $\mathbb{Q}(\theta)$, luego por el lema 2.24

$$1 \leq |N_{\mathbb{Q}(\theta)}(c_5^p\mu)| = \left|\left(N_{\mathbb{Q}(\theta)}(c_5^p)\right)\left(N_{\mathbb{Q}(\theta)}(\mu)\right)\right| = c_5^{ph}|N_{\mathbb{Q}(\theta)}(\mu)|$$

De donde

(4.7) $$|N_{\mathbb{Q}(\theta)}(\mu)| \geq \left(c_5^h\right)^{-p}$$ y

es claro que h es independiente de n y p.

Por (4.6)

$$\mu = f^p\big(B(log\alpha)\big) = \sum_{i=1}^{q}\sum_{j=1}^{q}\xi_{ij}(l + j\beta)^p\alpha^{iB}\gamma^{jB} \neq 0$$

Luego, de (4.3) y (4.4)

(4.8) $$\|\mu\| \leq q^2 \max_{\substack{1\leq i\leq q\\ 1\leq j\leq q}}\{\|\xi_{ij}\|, \|i + j\beta\|^p, \|\alpha\|^{iB}, \|\gamma\|^{jB}\}$$

Como $q < n \leq p$ y $q^2 = t = 2mn < 2^n$, para n suficientemente grande; se tiene que:

$$\|\mu\| < 2^n c_4^n n^{\frac{n}{2}}(qc_2)^p c_2^{mq} c_2^{mq}$$

$$\leq (2c_4 c_2^{1+2m})^p n^{\frac{n}{2}} q^p$$

En vista de que $q^2 = 2mn$, $q^p = \left(\sqrt{2mn}\right)^p = \left(\sqrt{2m}\right)^p n^{\frac{p}{2}} \leq \left(\sqrt{2m}\right)^p p^{\frac{p}{2}}$; se sigue que

$$\|\mu\| < \left(2c_4c_2^{1+2m}\sqrt{2m}\right)^p p^{\frac{p}{2}}p^{\frac{p}{2}}$$

$$= \left(2c_4c_2^{1+2m}\sqrt{2m}\right)^p p^p$$

(4.9) $$\|\mu\| = c_6^p p^p \qquad\qquad c_6 = 2c_4c_2^{1+2m}\sqrt{2m}$$

Por (4.6), la función entera $f(z) = p\left(e^z, e^{\beta z}\right)$ tiene ceros de orden al menos p en los puntos $z = b(log\alpha)$, para $b = 1,2,\dots,m$; luego por el lema 2.29, existe una función G analítica y no nula en dichos puntos tal que,

(4.10) $$G(z) = \frac{f(z)}{(z-log\alpha)^p(z-2log\alpha)^p\dots(z-mlog\alpha)^p}$$

Además, por ser f entera

$$f(z) = \sum_{a=0}^{\infty}\frac{f^a(B(log\alpha))}{a!}(z - Blog\alpha)^a$$

$$= \sum_{a=p}^{\infty}\frac{f^a(Blog\alpha)}{a!}(z - Blog\alpha)^a$$

$$= (z - Blog\alpha)^p\sum_{a=p}^{\infty}\frac{f^a(Blog\alpha)}{a!}(z - Blog\alpha)^{a-p}$$

$$\frac{f(z)}{(z-Blog\alpha)^p} = \sum_{a=p}^{\infty}\frac{f^a(Blog\alpha)}{a!}(z - Blog\alpha)^{a-p}$$

$$G(Blog\alpha) = \frac{f^p(Blog\alpha)}{p!\prod_{\substack{1\le b\le m\\ b\ne B}}(Blog\alpha - blog\alpha)^p}$$

$$f^p(Blog\alpha) = p!\,G(Blog\alpha)\prod_{\substack{1\le b\le m\\ b\ne B}}\left((B-b)log\alpha\right)^p$$

Entonces

(4.11) $$\mu = p!\,G(Blog\alpha)\prod_{\substack{1\le b\le m\\ b\ne B}}\left((B-b)log\alpha\right)^p$$

Si escogemos $R = \frac{p}{q}|log\alpha|$, entonces (para n suficientemente grande):

$$\frac{p}{q}|log\alpha| \geq \frac{p}{2q}|log\alpha| \geq \frac{n}{2q}|log\alpha|$$

$$= \frac{q^2}{(2m)(2q)}|log\alpha|$$

$$= \frac{q}{4m}|log\alpha|$$

$$> m|log\alpha|$$

$$> B|log\alpha|$$

Luego, por el Principio del Módulo Máximo, para $R = \frac{p}{q}|log\alpha|$,

$$|G(Blog\alpha)| \leq \max_{|z|\leq R}\{|G(z)|\} = |G(z)|_R \leq \frac{|f(z)|_R}{\min\limits_{1\leq b\leq m}\left\{\left|\frac{p}{q}|log\alpha| - b(log\alpha)\right|\right\}^{mp}}$$

$$= \frac{|f(z)|_R}{\left|\frac{p}{q}|log\alpha| - m(log\alpha)\right|^{mp}}$$

$$\leq \frac{|f(z)|_R}{\left|\left|\frac{p}{q}|log\alpha|\right| - |m(log\alpha)|\right|^{mp}}$$

$$= \frac{|f(z)|_R}{\left|\frac{p}{q}|log\alpha| - m|log\alpha|\right|^{mp}}$$

$$= \frac{|f(z)|_R}{|log\alpha|^{mp}\left|\frac{p}{q} - m\right|^{mp}}$$

De donde

(4.12) $$|G(z)|_R \leq \frac{|f(z)|_R}{|log\alpha|^{mp}\left|\frac{p}{q} - m\right|^{mp}}$$

Por otro lado,

$$\left|exp\big(z(i + j\beta)\big)\right| \leq exp|z(i + j\beta)|$$

$$\leq exp\left\{\frac{p}{q}|log\alpha|(q + q|\beta|)\right\}$$

$$= exp\{p(1 + |\beta|)|log\alpha|\}$$

$$exp\{p(1+|\beta|)|log\alpha|\} = e^{p(1+|\beta|)|log\alpha|}$$

$$= \left(e^{(1+|\beta|)|log\alpha|}\right)^p$$

$$= c_7^p \qquad\qquad c_7 = e^{(1+|\beta|)|log\alpha|}$$

De (4.1) y la desigualdad anterior

$$|f(z)|_R \leq q^2 c_4^n n^{\frac{n}{2}} c_7^p$$

$$< 2^n c_4^n c_7^p n^{\frac{n}{2}} \qquad\qquad q^2 = 2mn < 2^n, n \text{ grande}$$

$$< 2^p c_4^p c_7^p n^{\frac{n}{2}}$$

$$= c_8^p n^{\frac{n}{2}} \qquad\qquad c_8 = 2c_4c_7$$

Ahora podemos seguir acotando (4.12),

$$|G(z)|_R \leq \frac{|f(z)|_R}{|log\alpha|^{mp}\left|\frac{p}{q}-m\right|^{mp}}$$

$$\leq \frac{c_8^p p^{\frac{p}{2}}}{\left(\frac{p}{q}-m\right)^{mp}|log\alpha|^{mp}}$$

$$\leq \frac{c_8^p p^{\frac{p}{2}}}{\left(\frac{p}{2q}\right)^{mp}|log\alpha|^{mp}} \qquad\qquad \frac{p}{q}-m \geq \frac{p}{2q}, \text{ pues } p > n$$

$$= \frac{c_8^p p^{\frac{p}{2}}\left(\frac{2q}{p}\right)^{mp}}{|log\alpha|^{mp}}$$

Ahora de (4.11),

$$|\mu| = p!\,|G(Blog\alpha)|\left|\prod_{\substack{1\leq b\leq m\\ b\neq B}}\left((B-b)log\alpha\right)^p\right|$$

$$\leq \frac{p!c_8^p p^{\frac{p}{2}}\left(\frac{2q}{p}\right)^{mp}}{|log\alpha|^{mp}}\left(\prod_{\substack{b=1\\ b\neq B}}^{m}|B-b|^p\right)\left(\prod_{\substack{b=1\\ b\neq B}}^{m}|log\alpha|^p\right)$$

$$< p!\,c_8^p p^{\frac{p}{2}}\left(\frac{2q}{p}\right)^{mp}\left(\prod_{\substack{b=1\\ b\neq B}}^{m}|B-b|^p\right)$$

$$|\mu| < \left(c_8 2^m (2m)^{\frac{m}{2}} \left(\prod_{\substack{b=1\\b\neq B}}^{m} |B-b|\right)\right)^p p!\, p^{\frac{p}{2}} \left(\frac{\sqrt{n}}{p}\right)^{mp}$$

$$= c_9^p\, p!\, p^{\frac{p}{2}} \left(\frac{\sqrt{n}}{p}\right)^{mp}$$

$$< c_9^p p^p p^{\frac{p}{2}} \left(\frac{1}{\sqrt{p}}\right)^{mp}$$

$$= c_9^p p^p p^{\frac{p}{2}} p^{-\frac{mp}{2}}$$

$$= c_9^p p^{p+\frac{p}{2}-\frac{mp}{2}}$$

$$= c_9^p p^{\frac{2p+p-mp}{2}}$$

$$= c_9^p p^{\frac{3p-mp}{2}}$$

$$= c_9^p p^{\frac{p(3-m)}{2}}$$

Donde $c_9 = c_8 2^m (2m)^{\frac{m}{2}} \left(\prod_{\substack{b=1\\b\neq B}}^{m} |B-b|\right)$ y claramente es independiente de n y p.

Luego, de la desigualdad anterior y (4.9),

$$\left|N_{\mathbb{Q}(\theta)}(\mu)\right| < c_9^p p^{\frac{p(3-m)}{2}} \left(c_6^p p^p\right)^{h-1}$$

$$= \left(c_9 c_6^{h-1}\right)^p p^{\frac{p(3-m)}{2}} p^{ph-p}$$

$$= c_{10}^p p^{\frac{p(3-m)}{2}} p^{ph-p}$$

$$= c_{10}^p p^{p(3-2h-3)} p^{ph-p}$$

$$= c_{10}^p p^{-ph+ph-p}$$

(4.13) $$\left|N_{\mathbb{Q}(\theta)}(\mu)\right| = c_{10}^p p^{-p}$$

Donde $c_{10} = c_9 c_6^{h-1}$ y claramente es independiente de n y p.

Ahora de (4.7) y (4.13),

$$\left(c_5^h\right)^{-p} \leq \left|N_{\mathbb{Q}(\theta)}(\mu)\right| < c_{10}^p p^{-p}$$

De donde

$$c_{10}^{p}p^{-p} > \left(c_5^{h}\right)^{-p}$$

$$c_{10}^{p}\left(c_5^{h}\right)^{p} > p^{p}$$

$$\left(c_{10}c_5^{h}\right)^{p} > p^{p}$$

$$c_{10}c_5^{h} > p$$

En vista de que c_{10}, c_5, h son independientes de n y p, la última desigualdad contradice el hecho de que $p \geq n$ y n lo podemos escoger arbitrariamente grande; por lo tanto nuestra suposición es falsa y algún valor de α^{β} debe ser trascendente.□

4.3. Prueba de Schneider

Sea $\alpha, \beta \in \widetilde{\mathbb{Q}}$; con $\alpha \neq 0,1$ y $\beta \notin \mathbb{Q}$.

Supongamos que $\gamma = \alpha^{\beta} = e^{\beta(\log\alpha)} \in \widetilde{\mathbb{Q}}$ y $\theta \in \widetilde{\mathbb{Q}}$ tal que:

$$\alpha, \beta, \gamma \in \mathbb{Q}(\theta) \text{ con } [\mathbb{Q}(\theta):\mathbb{Q}] = h$$

Escojamos un entero positivo q tal que

$$D_1 = \sqrt{2h}q^{\frac{3}{2}} \text{ y } D_2 = \sqrt{2h}q^{\frac{1}{2}}$$

son enteros (basta tomar $q = 2hp^2$)

Sea

$$p(x,y) = \sum_{m=0}^{D_1-1}\sum_{n=0}^{D_2-1}\xi_{mn}x^{m}y^{n}$$

Donde $\xi_{mn} \in \mathbb{Z}$

Definamos la función entera

(4.14) $$f(z) = p\left(z, e^{(\log\alpha)z}\right)$$

Tal que

(4.15) $$f(a + b\beta) = 0 \qquad 0 \leq a, b < q$$

Veamos que tal función está bien definida y cumple (4.15); lo que se reduce a encontrar los enteros apropiados ξ_{mn}. En efecto,

$$f(a + b\beta) = p\left(a + b\beta, e^{(\log\alpha)(a+b\beta)}\right)$$

$$= \sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \xi_{mn}(a + b\beta)^m e^{\log\alpha(a+b\beta)n}$$

$$= \sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \xi_{mn}(a + b\beta)^m \alpha^{na}\left(\alpha^{\beta}\right)^{nb}$$

Para que se dé (4.15), se tendría que:

(4.16) $$\sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \underbrace{(a + b\beta)^m \alpha^{na} \gamma^{nb}}_{coeficientes} \underbrace{\xi_{mn}}_{incógnitas} = 0 \qquad \text{para } 0 \leq a, b < q$$

Tenemos q^2 ecuaciones lineales en $D_1 D_2$ incógnitas con coeficientes algebraicos. En vista de que $\alpha, \beta, \gamma \in \mathbb{Q}(\theta)$, los podemos representar como sigue:

$$\alpha = p_\alpha(\theta) = \sum_{i=0}^{h-1} c_i \theta^i \qquad \text{donde } c_i \in \mathbb{Q}$$

$$\beta = p_\beta(\theta) = \sum_{i=0}^{h-1} b_i \theta^i \qquad \text{donde } b_i \in \mathbb{Q}$$

$$\gamma = p_\gamma(\theta) = \sum_{i=0}^{h-1} \omega_i \theta^i \qquad \text{donde } \omega_i \in \mathbb{Q}$$

Es claro que para $0 \leq a, b < q$, $f(a + b\beta) \in \mathbb{Q}(\theta)$; por lo tanto

(4.17) $$f(a + b\beta) = E_1 + E_2\theta + \cdots + E_h\theta^{h-1}$$

Donde $E_1, E_2, \ldots, E_h$ dependen del par (a, b)

Ahora (4.16) lo podemos reescribir como sigue

(4.18) $$\sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \left(a + bp_\beta(\theta)\right)^m \left(p_\alpha(\theta)\right)^{na} \left(p_\gamma(\theta)\right)^{nb} \xi_{mn} = 0$$

Al desarrollar esta última expresión y emplear el Lema 2.25, observamos que

$$E_j = E_j(a,b) = \sum_{m=0}^{D_1-1}\sum_{n=0}^{D_2-1} w_j(m,n,a,b)\,\xi_{mn}$$

Donde cada coeficiente $w_j(m,n,a,b)$ es la suma de D_1D_2 términos racionales de la forma $r_j(m,n,a,b)$.

En vista de que $1,\theta,\theta^2,\dots,\theta^{h-1}$ son $\mathbb{Q}$ –linealmente independientes; para cada par (a,b) tal que $0 \leq a,b < q$

$$f(a+b\beta)=0 \;\Leftrightarrow\; E_1 = E_2 = \cdots = E_h = 0$$

De donde obtenemos un sistema homogéneo de hq^2 ecuaciones lineales en D_1D_2 incógnitas tal que $D_1D_2 = 2hq^2 > hq^2$.

Vamos a encontrar una cota para los coeficientes $w_j(m,n,a,b)$. Para tal efecto, consideremos los coeficientes en (4.18), es decir, para cada par (a,b) vamos a considerar:

(4.19) $$\left(a+bp_\beta(\theta)\right)^m \left(p_\alpha(\theta)\right)^{na} \left(p_\gamma(\theta)\right)^{nb}$$

Con $\quad 0 \leq m \leq D_1 - 1, \quad 0 \leq n \leq D_2 - 1, \quad 0 \leq a,b < q$

Aplicando el Lema 2.26 a (4.19), se tiene que si

$$\beta_1 = \beta_2 = \cdots = \beta_m = a + b\left(p_\beta(\theta)\right)$$

$$\beta_{m+1} = \beta_{m+2} = \cdots = \beta_{m+n} = \left(p_\alpha(\theta)\right)^a$$

$$\beta_{m+n+1} = \beta_{m+n+2} = \cdots = \beta_{m+2n} = \left(p_\gamma(\theta)\right)^b$$

Entonces, para $l = 1,2,\dots,m$

$$a+b\left(p_\beta(\theta)\right) = a + b\sum_{i=0}^{h-1} b_i\theta^i = (a+bb_0) + bb_1\theta + bb_2\theta^2 + \cdots + bb_{h-1}\theta^{h-1}$$

Como

$$a + bb_0 < q + q\varkappa(p_\beta) < 2q\varkappa(p_\beta) \quad \text{y} \qquad bb_i < q\varkappa(p_\beta), 1 \le i \le h-1$$

Podemos tomar $\qquad B_l = 2q\varkappa(p_\beta),\ l = 1,2,\dots,m$

Para $l = m+1, m+2, \dots, m+n$; en vista de que $\quad \alpha = p_\alpha(\theta) = \sum_{i=0}^{h-1} c_i\theta^i$

Podemos tomar $B_l = h^q(\varkappa(p_\alpha))^q(2\varkappa(\theta))^{hq}$ pues $|c_i| \le \varkappa(p_\alpha)$

De manera análoga, para $l = m+n+1, m+n+2, \dots, m+2n$; podemos tomar

$$B_l = h^q\left(\varkappa(p_\gamma)\right)^q(2\varkappa(\theta))^{hq}$$

Ahora, en vista de que para cada

$$0 \le m \le D_1 - 1, 0 \le n \le D_2 - 1, 0 \le a, b < q;$$

$$\left(a + bp_\beta(\theta)\right)^m (p_\alpha(\theta))^{na}\left(p_\gamma(\theta)\right)^{nb} = r_1 + r_2\theta + \dots + r_h\theta^{h-1}$$

Con $r_j = r_j(m,n,a,b)$. De nuevo por el Lema 2.26

$$\max_{1\le j\le h}\{|r_j|\} \le h^{m+2n}\left(2q\varkappa(p_\beta)\right)^m\left(h^q(\varkappa(p_\alpha))^q(2\varkappa(\theta))^{hq}\ \right)^n$$

$$\left(h^q\left(\varkappa(p_\gamma)\right)^q(2\varkappa(\theta))^{hq}\ \right)^n(2\varkappa(\theta))^{h(m+2n)}$$

De donde

$$\max_{1\le j\le h}(|r_j|) \le h^{D_1+2D_2+2qD_2}(2q)^{D_1}\left(\varkappa(p_\beta)\right)^{D_1}(\varkappa(p_\alpha))^{qD_2}\left(\varkappa(p_\gamma)\right)^{qD_2}(2\varkappa(\theta))^{h(D_1+2D_2+2qD_2)}$$

Ahora (4.18) puede tomar la forma

$$f(a+b\beta) = \sum_{m=0}^{D_1-1}\sum_{n=0}^{D_2-1}(r_1 + r_2\theta + \dots + r_h\theta^{h-1})\xi_{mn} = 0$$

Con

$$\max_{1\le j\le h}\{|r_j|\} \le q^{D_1}\left[2h\varkappa(p_\beta)(2\varkappa(\theta))^h\right]^{D_1}\left[h^2(2\varkappa(\theta))^{2h}\right]^{D_2}\left[h^2\varkappa(p_\alpha)\varkappa(p_\gamma)(2\varkappa(\theta))^{2h}\right]^{qD_2}$$

$$= c_1^{D_1}c_2^{D_2}q^{D_1}c_3^{D_2 q}$$

Donde

$$c_1 = 2h\varkappa(p_\beta)(2\varkappa(\theta))^h, c_2 = h^2(2\varkappa(\theta))^{2h}, c_3 = h^2\varkappa(p_\alpha)\varkappa(p_\gamma)(2\varkappa(\theta))^{2h}$$

Reescribiendo q como e^{logq}

$$\max_{1\le j\le h}\{|r_j(m,n,a,b)|\} \le c_1^{D_1}c_2^{D_2}(e^{logq})^{D_1}c_3^{qD_2}$$

$$\le c_1^{logqD_1}(e^{logq})^{D_1}c_2^{qD_2}c_3^{qD_2}$$

$$= c_4^{(logq)D_1}c_5^{qD_2} \qquad c_4 = c_1 e, \quad c_5 = c_2 c_3$$

Así,

$$\max_{1\le j\le h}\{|r_j(m,n,a,b)|\} \le c_6^{D_1(logq)+qD_2} \qquad c_6 = máx\{c_4, c_5\} \tag{4.20}$$

Al multiplicar (4.17) por

$$\delta = M.C.M.\left\{Den\left(p_\beta(\theta)\right)^{D_1}\right\}M.C.M.\left\{Den(p_\alpha(\theta))^{qD_2}\right\}M.C.M.\left\{Den\left(p_\gamma(\theta)\right)^{qD_2}\right\}$$

Donde la abreviatura *Den* significa denominadores de, obtenemos:

$$\delta f(a+b\beta) = A_1 + A_2\theta + \cdots + A_h\theta^{h-1} \tag{4.21}$$

es un entero algebraico en $\mathbf{Q}(\theta)$ y como en (4.17), al compararlo con (4.18),

$$A_j = A_j(a,b) = \sum_{m=0}^{D_1-1}\sum_{n=0}^{D_2-1} t_j(m,n,a,b)\xi_{mn}$$

Donde cada coeficiente $t_j(m,n,a,b)$ es un entero que resulta de la suma de D_1D_2 términos de la forma $\delta r_j(m,n,a,b)$

Por (4.20), se tiene que

$$\left|t_j(m,n,a,b)\right| \leq D_1D_2\delta c_6^{D_2(\log q)+qD_2} \tag{4.22}$$

$$< D_1D_2\delta^{D_2(\log q)+qD_2}c_6^{D_1(\log q)+qD_2}$$

$$= D_1D_2c_7^{D_2(\log q)+qD_2}$$

Ahora, para cada par (a,b), igualamos los $A_1, A_2, \dots, A_d$ a cero, es decir:

$$A_j(a,b) = \sum_{m=0}^{D_1-1}\sum_{n=0}^{D_2-1} t_j(m,n,a,b)\xi_{mn} = 0 \qquad \text{y}$$

obtenemos un sistema homogéneo de hq^2 ecuaciones lineales con coeficientes enteros en D_1D_2 incógnitas con

$$D_1D_2 > hq^2 \qquad \text{y} \qquad \left|t_j(m,n,a,b)\right| < D_1D_2c_7^{D_2(\log q)+qD_2}$$

Por el lema de Siegel existe una solución no nula de enteros ξ_{mn} tal que

$$|\xi_{mn}| < 1 + \left[(D_1D_2)^2c_7^{D_2(\log q)+qD_2}\right]^{\frac{hq^2}{2hq^2-hq^2}} = 1 + (D_1D_2)^2c_7^{D_2(\log q)+qD_2} \tag{4.23}$$

Como q es relativamente grande, podemos sin pérdida de generalidades reescribir (4.23) como sigue

$$|\xi_{mn}| < 1 + (D_1D_2)^2c_7^{D_2(\log q)+qD_2}$$

$$= 1 + 4h^2q^4c_7^{D_2(\log q)}c_7^{qD_2}$$

$$= 1 + 4h^2e^{4\log q}\left(c_7^{\sqrt{2h}}\right)^{q^{\frac{3}{2}}\log q}\left(c_7^{\sqrt{2h}}\right)^{q^{\frac{3}{2}}}$$

$$\leq (4h^2)^{q^{\frac{3}{2}}\log q}(e^4)^{q^{\frac{3}{2}}\log q}\left(c_7^{\sqrt{2h}}\right)^{q^{\frac{3}{2}}\log q}\left(c_7^{\sqrt{2h}}\right)^{q^{\frac{3}{2}}\log q}$$

Así,

(4.24) $$|\xi_{mn}| \leq c_8^{q^{\frac{3}{2}}log q}$$

Por lo anterior, tenemos que

$$p(x,y) = \sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \xi_{mn} x^m y^n$$ y,

$$f(z) = p\left(z, e^{(log\alpha)z}\right)$$

Están bien definidos, además:

$$f(a + b\beta) = 0 \qquad 1 \leq a, b < q$$

Para seguir trabajando, debemos asegurarnos de que f no es idénticamente nula. Para tal efecto, vamos a demostrar que si: $\rho \in \mathbb{C} - \{0\}$; entonces $f(z, e^{\rho z}) \not\equiv 0$ para todo polinomio no nulo $p(x, y) \in \mathbb{Z}[x, y]$.

Prueba: Sea

(4.25) $$p(x,y) = \sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \xi_{mn} x^m y^n \in \mathbb{Z}[x, y]$$

no nulo, y supongamos que

(4.26) $$f(z, e^{\rho z}) = 0, \quad \forall z \in \mathbb{C}$$

Reescribiendo (4.25)

$$p(x,y) = \sum_{m=0}^{D_1-1} p_m(y)\, x^m \quad \text{donde} \quad p_m(y) = \sum_{n=0}^{D_2-1} \xi_{mn}\, y^n \in \mathbb{Z}[y]$$

Así

$$p(x,y) = p_0(y) + p_1(y)x + \cdots + p_{D_1-1}(y)x^{D_1-1}$$ y

$$p_0(y) = \xi_{00} + \xi_{01}y + \cdots + \xi_{oD_2-1}y^{D_2-1}$$

$$p_1(y) = \xi_{10} + \xi_{11}y + \cdots + \xi_{1D_2-1}y^{D_2-1}$$

$$p_{D_1-1}(y) = \xi_{(D_1-1)0} + \xi_{(D_1-1)1}y + \cdots + \xi_{(D_1-1)(D_2-1)}y^{D_2-1}$$

Luego hay un número finito de valores y_0, $(D_2-1)(D_1-1)$, para los cuales la función

$$g(x) = p(x, y_0) \equiv 0$$

Los y_0 tal que $p_m(y_0) \equiv 0$; $m = 1,2,\dots,D_1-1$

Sea y_0 tal que $p_m(y_0) \neq 0$; $m = 1,2,\dots,D_1-1$. Entonces $p(x,y_0) \in \mathbb{Z}[x]$.

En vista de que $\rho \neq 0$, si $z_0 = \frac{1}{\rho}$

$$\begin{aligned} G(z) &= p(z, e^{\rho z_0}) = p(z,e) \\ &= \textstyle\sum_{m=0}^{D_1-1}\sum_{n=0}^{D_2-1}\xi_{mn}z^m e^n \\ &= p_0(e) + p_1(e)z + p_2(z)z^2 + \cdots + p_{D_1-1}(e)z^{D_1-1} \end{aligned}$$

Es no nula, pues de lo contrario,

$$p_m(e) = 0 \qquad\qquad m = 0,1,\dots,D_1-1$$

Lo que es imposible, pues e es trascendente; por lo tanto

(4.27) $$G(z) = p(z, e^{\rho z_0}) \in \mathbb{C}[z]$$ no es nulo.

Ahora, para cada entero k;

$$\begin{aligned} G\left(z_0 + \frac{2\pi i k}{\rho}\right) &= p\left(z_0 + \frac{2\pi i k}{\rho}, e^{\rho z_0}\right) \\ &= p\left(z_0 + \frac{2\pi i k}{\rho}, e^{\rho z_0 + 2\pi i k}\right) \\ &= p\left(z_0 + \frac{2\pi i k}{\rho}, e^{\rho\left(z_0 + \frac{2\pi i k}{\rho}\right)}\right) \\ &= 0 \end{aligned}$$

Luego el polinomio G tiene infinitos ceros, lo que contradice (4.27); por lo tanto, nuestra suposición es falsa y $f(z, e^{\rho z}) \neq 0$.

Al igual que en la prueba de Gelfond, se necesita un valor no nulo que dependa de la función f que nos lleve a una contradicción. Para encontrar tal valor fijemos q en (4.15) y apliquemos el lema 2.30 a la función auxiliar f definida por Schneider en (4.14).

Por el Principio del Módulo Máximo y la desigualdad triangular

$$|f|_R = \max_{|z|=R}\{D_1 D_2 max\{|\xi_{mn}|\}|z|^{D_1} e^{D_2|log\alpha||z|}\}$$

$$\leq D_1 D_2 c_8^{q^{\frac{3}{2}}logq} R^{D_1} e^{D_2|log\alpha|R}$$

$$\leq D_1 D_2 c_8^{q^{\frac{3}{2}}logq} e^{D_1 logR} e^{D_2|log\alpha|R}$$

$$\leq e^{R^k}$$

Donde la desigualdad anterior es válida para $k > 1$ y R suficientemente grande, ya que $D_1, D_2, c_8^{q^{\frac{3}{2}}logq}$ no dependen de R.

En vista de que f no es idénticamente nula, el lema 2.30 implica que para una escogencia de $\epsilon > 0$ y todo número real $R > q$ relativamente grande; f no puede tener más que $R^{k+\epsilon}$ ceros en $Z(F, R)$. Más concretamente, si tomamos $k = \frac{5}{4}$ y $\epsilon = \frac{1}{4}$

(4.28) $$card\big(Z(F, R)\big) \leq R^{\frac{3}{2}}$$

Ahora, si f se anula en todos los puntos $z = a + b\beta$, donde a, b son enteros positivos; podemos, en vista de que $1 + |\beta| > 1$ es fijo, tomar un $R > q$ relativamente grande tal que

$$R(1 + |\beta|) \approx R$$

Y en donde

$$card\big(Z(f, R)\big) \geq R^2 \qquad\qquad \text{pues } \beta \notin \mathbf{Q}$$

Lo que contradice (4.28); por lo tanto muestra suposición en falsa y existen enteros positivos a^*, b^* tal que $f(a^* + b^*\beta) \neq 0$.

Ahora, si escogemos $Q = min\{a^*, b^*\}$ se tiene que

$$f(a + b\beta) = 0 \qquad 0 \leq a < Q, \quad 0 \leq b < Q$$

Mientras que existe un par de enteros (a^*, b^*), satisfaciendo $0 \leq a^* \leq Q$, $0 \leq b^* \leq Q$; donde a^* o b^* es igual a Q, tal que

$$f(a^* + b^*\beta) \neq 0$$

Tal como se hizo para llegar a (4.21),

$$\mu = \delta^* f(a^* + b^*\beta) = A_1^* + A_2^*\theta + \cdots + A_h^*\theta^{h-1} \tag{4.29}$$

Es un entero algebraico en $\mathbf{Q}(\theta)$ y;

$$\max_{1 \leq j \leq h}\{|A_j^*|\} \leq D_1 D_2 \delta^* max\{|\xi_{mn}|\} max\{|t_j(m, n, a^*, b^*)|\}$$

$$\leq D_1^2 D_2^2 (\delta^*)^{D_1 logQ + D_2 Q} C_8^{q^{\frac{3}{2}} logq} C_7^{D_1(logQ) + QD_2}$$

$$\leq D_1^2 D_2^2 (\delta^*)^{D_1 logQ + D_2 Q} C_8^{Q^{\frac{3}{2}} logQ} C_7^{D_1(logQ) + QD_2}$$

Procediendo como lo hicimos para llegar a (4.24), obtenemos que

(4.30) $$\max_{1\le j\le h}\{|A_j^*|\} \le c_9^{Q^{\frac{3}{2}}\log Q}$$

Sea $\theta_1 = \theta, \theta_2, \dots, \theta_h$ los conjugados de θ; entonces por el lema 2.23

(4.31) $$N_{\mathbb{Q}(\theta)}(\mu) = \prod_{i=1}^{h}\left(A_1^* + A_2^*\theta_i + \cdots + A_h^*\theta_i^{h-1}\right) \in \mathbb{Z} - \{0\}$$

Finalmente, vamos a probar que $\left| N_{\mathbb{Q}(\theta)}(\mu)\right|$ nos lleva a la contradicción esperada.

En efecto,

$$\left|N_{\mathbb{Q}(\theta)}(\mu)\right| = |A_1^* + A_2^*\theta + \cdots + A_h^*\theta^{h-1}| \prod_{i=2}^{h}\left|A_1^* + A_2^*\theta_i + \cdots + A_h^*\theta_i^{h-1}\right|$$

(4.32) $$\left|N_{\mathbb{Q}(\theta)}(\mu)\right| = |\delta^* f(a^* + b^*\xi)| \prod_{i=2}^{h}\left|A_1^* + A_2^*\theta_i + \cdots + A_h^*\theta_i^{h-1}\right|$$

Ahora, para $2 \le i \le d$; por la desigualdad triangular y (4.30)

$$\left|A_1^* + A_2^*\theta_i + \cdots + A_h^*\theta_i^{h-1}\right| \le h \max_{1\le j\le h}\{|A^*_j|\}\, max\{1, |\theta_1|, \dots, |\theta_h|\}^{h-1}$$

$$\le c_{10}^{Q^{\frac{3}{2}}\log Q}$$

Por lo tanto,

(4.33) $$\prod_{i=2}^{h}\left|A_1^* + A_2^*\theta_i + \cdots + A_h^*\theta_i^{h-1}\right| \le \left(c_{10}^{Q^{\frac{3}{2}}\log Q}\right)^{h-1} \le c_{11}^{Q^{\frac{3}{2}}\log Q}$$

Para acotar el otro factor de (4.32), definamos la función entera

$$G(z) = \frac{\delta^* f(z)}{\prod_{a=0}^{Q-1}\prod_{b=0}^{Q-1}\left(z - (a + b\beta)\right)}$$

Luego,

$$|\delta^* f(a^* + b^*\beta)| = |G(a^* + b^*\beta)| \prod_{a=0}^{Q-1}\prod_{b=0}^{Q-1}|(a^* - a) + (b^* - b)\beta|$$

Dado que $a < Q$ y $b < Q$, para $R > Q(1+|\beta|)$, $|a^* + b^*\beta| < R$ y; por el Principio del Módulo Máximo

$$|\delta^* f(a^* + b^*\beta)| \leq |G|_R \prod_{a=0}^{Q-1} \prod_{b=0}^{Q-1} |(a^* - a) + (b^* - b)\beta|$$

$$\leq \frac{|\delta^* f|_R}{\left|\prod_{a=0}^{Q-1} \prod_{b=0}^{Q-1} (z - (a + b\beta))\right|_R} \prod_{a=0}^{Q-1} \prod_{b=0}^{Q-1} |(a^* - a) + (b^* - b)\beta|$$

Ahora,

$$|\delta^* f|_R = \left|\delta^* \sum_{m=0}^{D_1-1} \sum_{n=0}^{D_2-1} \xi_{mn}\, z^m \left(e^{(\log\alpha)z}\right)^n\right|$$

$$\leq \delta^* D_1 D_2 c_8^{q^{\frac{3}{2}}\log q} |z|_R^{D_1} \left|e^{(\log\alpha)z}\right|_R^{D_2}$$

$$\leq \delta^* D_1 D_2 c_8^{q^{\frac{3}{2}}\log q} R^{D_1} \left(e^{|Re(\log\alpha)|R}\right)^{D_2}$$

De nuevo, procediendo como lo hicimos para llegar a (4.24) y en vista de que $R > Q > q$ se llega a

$$|\delta^* f|_R < c_{12}^{q^{\frac{3}{2}}\log R + q^{\frac{1}{2}} R} \tag{4.34}$$

Por otro lado, es claro que

$$\prod_{a=0}^{Q-1} \prod_{b=0}^{Q-1} |(a^* - a) + (b^* - b)\beta| \leq \left(Q(1+|\beta|)\right)^{Q^2} \tag{4.35}$$

Además, ya que $R > Q(1+|\beta|)$ y $|a + b\beta| \leq Q(1+|\beta|)$; para $z = R$, se sigue que

$$\left|\prod_{a=0}^{Q-1} \prod_{b=0}^{Q-1} (z - (a + b\beta))\right|_R \geq \left|\prod_{a=0}^{Q-1} \prod_{b=0}^{Q-1} (R - (a + b\beta))\right|_R \tag{4.36}$$

$$\geq \left(R - Q(1+|\beta|)\right)^{Q^2}$$

Ahora, si tomamos $R = Q^{1+\epsilon} + Q(1+|\beta|)$ se tiene por (4.35) y (4.36) que:

$$\frac{\prod_{a=0}^{Q-1}\prod_{b=0}^{Q-1}|(a^*-a)+(b^*-b)\beta|}{\left|\prod_{a=0}^{Q-1}\prod_{b=0}^{Q-1}(z-(a+b\beta))\right|_R} \leq \left((1+|\beta|)Q^{-\epsilon}\right)^{Q^2}$$

$$= \left((1+|\beta|)e^{-\varepsilon logQ}\right)^{Q^2}$$

Luego, para una constante apropiada c_{13},

$$\text{(4.37)} \qquad \frac{\prod_{a=0}^{Q-1}\prod_{b=0}^{Q-1}|(a^*-a)+(b^*-b)\beta|}{\left|\prod_{a=0}^{Q-1}\prod_{b=0}^{Q-1}(z-(a+b\beta))\right|_R} \leq c_{13}^{-\varepsilon Q^2 logQ}$$

Así, por (4.34) y (4.37) se tiene que

$$\text{(4.38)} \qquad |\delta^* f(a^* + b^*\beta)| < c_{12}^{q^{\frac{3}{2}}logR+q^{\frac{1}{2}}R} c_{13}^{-\varepsilon Q^1 logQ}$$

Si escogemos q, e indirectamente Q lo suficientemente grande se tendrá que $Q^{1+\epsilon} > Q(1+|\beta|)$, lo cual implica que $R < 2Q^{1+\epsilon}$ y; la desigualdad (4.38) la podemos reescribir como sigue,

$$|\delta^* f(a^* + b^*\beta)| < c_{12}^{q^{\frac{3}{2}}log(2Q^{1+\varepsilon})+q^{\frac{1}{2}}(2Q^{1+\varepsilon})} c_{13}^{-\varepsilon Q^2 logQ}$$

$$\leq c_{14}^{(1+\varepsilon)Q^{\frac{3}{2}}logQ+Q^{\frac{3}{2}+\varepsilon}-\varepsilon Q^2 logQ}$$

Si fijamos $\varepsilon = \frac{1}{2}$ y combinamos (4.33) con la desigualdad previa, se tiene por (4.32) que:

$$\text{(4.39)} \qquad \left|N_{\mathbf{Q}(\theta)}(\mu)\right| < c_{11}^{Q^{\frac{3}{2}}logQ} c_{14}^{\frac{3}{2}Q^{\frac{3}{2}}logQ+Q^2-\frac{1}{2}Q^2 logQ}$$

En vista de que podemos tomar c_{14} lo suficientemente grande, (4.39) lo podemos reescribir como sigue:

$$|N_{\mathbb{Q}(\theta)}(\mu)| < c_{15}^{Q^{\frac{3}{2}}logQ+Q^2-\frac{1}{2}Q^2logQ} \tag{4.40}$$

Como escogimos q y Q lo suficientemente grande, el término negativo $-\frac{1}{2}Q^2logQ$ domina el crecimiento lento del término positivo $Q^{\frac{3}{2}}logQ + Q^2$; por lo tanto, para una selección de q lo suficientemente grande,

$$0 < |N_{\mathbb{Q}(\theta)}(\mu)| < 1$$

Obteniendo la contradicción esperada□

4.4. Corolarios del Teorema de Gelfond-Schneider.

Corolario 4.1. (Teorema de Gelfond-1929) e^{π} es trascendente.

Prueba:

Supongamos que $\alpha = e^{\pi}$ es algebraico, y tomemos $\beta = i$. Es claro que β es algebraico y además no es racional; luego por el Teorema de Gelfond-Schneider (Teorema 4.1)

$$\alpha^{\beta} = (e^{\pi})^{i} = e^{i\pi} = -1$$

es trascendente, lo cual es obviamente falso. Por lo tanto nuestra suposición es falsa y e^{π} es trascendente.□

Corolario 4.2. (Teorema de Kuzmin-1930) $2^{\sqrt{2}}$ es trascendente

Prueba:

Supongamos que $\gamma = 2^{\sqrt{2}}$ es algebraico y, tomemos $\alpha = 2$. Ya que

$$\frac{log2^{\sqrt{2}}}{log2} = \sqrt{2}$$

es irracional; por el Teorema de Gelfond-Schneider (Teorema 4.2) $\sqrt{2}$ es trascendente, lo cual es falso. Se sigue, por lo tanto, que $2^{\sqrt{2}}$ es trascendente.□

Por el teorema de Gelfond-Schneider podemos seguir obteniendo más números trascendentes como: $\frac{log r}{log 10}$ (para cualquier número racional positivo r que no sea una potencia de 10), $\sqrt{3}^{\sqrt{2}}$, i^{i}, ...

4.5. Diferencias y similitudes en las soluciones del séptimo problema de Hilbert

Los métodos empleados por Gelfond y Schneider tienen mucho en común, a saber:

1. Asumen que α^{β} es algebraico.
2. Construyen una función auxiliar, empleando el lema de Siegel, con un gran número de ceros en cierto disco.
3. Prueban que existe un número algebraico no nulo que dependen de la función y; que el mismo nos lleva a una contradicción al emplear, principalmente, el principio del módulo máximo.

La diferencia de las pruebas estriba, en las técnicas empleadas para recorrer los pasos descritos en el párrafo anterior. Mientras Gelfond construye la función auxiliar $f(z) = p(e^{z}, e^{\beta z})$, la cual tiene ceros de multiplicidad relativamente grande y dependen de un solo parámetro (múltiplos enteros de $log\alpha$); Schneider construye la función $f(z) = p(z, e^{(log\alpha)z})$ con ceros de multiplicidad uno y los mismos dependen de dos parámetros enteros $(a + b\beta)$. En la prueba de Gelfond la función auxiliar se garantiza más expeditamente que en la de Schneider. Otra diferencia notable está en la obtención del número algebraico $\mu \neq 0$, el cual como apreciamos es más complejo de deducir en la prueba de Schneider.

Es importante señalar, que la prueba que presentamos de Gelfond es una síntesis de las pruebas presentadas por Niven (1985), Siegel (1949) y Gelfond (1960); mientras que para la prueba de Schneider, decidimos seguir la ofrecida por Burger y Tubbs (2010), misma que se deduce de la prueba del Teorema de Michel Waldschmidt.

Para terminar, resaltamos que las diferencias, técnicas, de las pruebas que presentamos se mantienen en la versión de Fel'dman y Nesterenko (1998), Siegel (1949) y Hilbert's Seventh Problem: Solutions and extensions; mientras que las dos últimas emplean el determinante de Vandermonde, en ambas pruebas, en la técnica empleada para encontrar el número algebraico distinto de cero.

CONCLUSIONES

Los problemas planteados por Hilbert, en el segundo Congreso celebrado en Paris, motivaron que un sinnúmero de matemáticos dedicarán sus esfuerzos a resolverlos; a tal punto que aquel que resolviese uno de estos problemas entraba a lo que se denominó: "la clase de honor de la comunidad matemática". La historia de estos problemas y su solución trae consigo el desarrollo de la Matemática del siglo XX; ya que su proponente recoge en ellos, prácticamente, la totalidad de la matemática de aquel entonces. La mayoría fueron resueltos, pero tal como se lo propuso Hilbert; el área en los cuales se encuadran sigue lleno de vida y reflejan las insospechadas relaciones entre las ramas de la Matemática. Así, por ejemplo, vimos que la solución del séptimo problema establece la relación entre la teoría de número algebraica, el álgebra lineal, la teoría de polinomios, el análisis complejo y claro está la teoría de números trascendentes. Podemos decir que se cumplió la profecía de Minkowski en su carta a Hilbert.

La Teoría de Números Trascendentes florece a partir de fuentes diversas y algunas de estas de tiempos antiguos; sin embargo, es a partir del Teorema de Liouville (1844) que se logra obtener el primer número trascendente concreto. Posteriormente, Hermite (1873) y Lindemann (1882) demuestran, respectivamente, la trascendencia de e y π. Seguidamente el teorema de Hermite-Lindemann y su generalización, Teorema de Lindemann-Weierstrass (1884), permitió generar más y más números trascendentes. Esta generación de números trascendentes continúo con las soluciones del séptimo problema de Hilbert en 1934.

Las soluciones del séptimo problema de Hilbert tienen mucho en común en sus métodos, pero las técnicas empleadas para recorrerlo son diferentes; por ende, podemos concluir que este problema fue solucionado, de forma independiente, por Gelfond (Rusia) y Schneider (Alemania) y de aquí que se conozca como Teorema de Gelfond-Schneide.

RECOMENDACIONES

Entre las principales recomendaciones tenemos:

- Realizar con mayor detenimiento, una investigación de cada uno de los problemas planteados por Hilbert y las soluciones dadas a estos.
- Presentar y comparar diferentes pruebas de algunos teoremas presentados en esta investigación; por ejemplo, del Teorema de Lindemann-Weiestrass.
- Estudiar a profundidad el desarrollo histórico-matemático de la Teoría de Números Trascendentes.
- Ahondar en el Teorema de Michel Waldschmidt y en el trabajo de Alan Baker de 1966; de los cuales se puede obtener, como corolario, el Teorema de Gelfond-Schneider.

REFERENCIAS BIBLIOGRÁFICAS

Baker, A. (1975). *Transcendental Number Theory.* Cambridge: Cambridge University Press.

Boyer, C. (1986). *Historia de la Matemática.* Madrid: Alianza Editorial

Brown, J. & Churchill, R. (2004). *Variables Complejas y Aplicaciones.* Madrid: McGrawHill.

Burger, E. & Tubbs, R. (2010).*Making Transcendence Transparent: An intuitive approach to classical transcendental number theory.* New York: Springer.

Burgos, J. (2006). *Algebra Lineal y Geometría Cartesiana.* Madrid: McGrawHill.

Butler, L. ( ). *Transcendence and Irrationality Proofs.* Disponible en: www.math.bris.ac.uk/~malab/PDF/MA469.pdf [Consultado el 8 de diciembre de 2012]

Chadid, I.(2005). *Temas de Teoría de Cuerpos, Teoría de Anillos y Números Algebraicos.* Vol I. Bogotá: Universidad Nacional de Colombia.

Chudnovsky, G. (1984). *Contributions to the Theory of transcendental Numbers.* E.E.U.U.: American Mathematical Society

Conrad, K. *Symmetric Polynomials.* Disponible en: www.math.uconn.edu/.../Symmfuction.pdf. [Consultado el 16 de noviembre de 2012]

Corry, L. (1998). *Los 23 Problemas de Hilbert y su Trasfondo Histórico.* Boletín de la Asociación Matemática Venezolana Vol. V, Nº 2. Disponible en: www.emis.ams.org/journals/BAMV/conten/vol5/v5n2p117.pdf. [Consultado el 6 de diciembre de 2012]

Courant, R. & Robbins, H. (1971). *¿Qué es la Matemática?* Madrid: Aguilar

Dorronsoro, J. & Hernández, E. (1996). *Números, grupos y anillos.* Madrid: Addison-Wesley Iberoamericana España.

Eves, H. (1968). *Funciones de Variables Compleja.* Tomo I. México: C.E.C.S.A.

Fel'dman, N.I. & Nesterenko, Y. V. (1998). *Trascendental Numbers.* En:Encyclopaedia of Mathematical Sciences (vol. 44). New York: Springer.

Fel'dman, N.I. & Shidlovskii, A.B. (1967). *The Development and Present State of The Theory of Transcendental Numbers.* IOPscience. Disponible en: http://iopscience.iop.org/0036-0279/22/3/R01. [Consultado el 4 de agosto de 2011]

Fischler, S. *Algebraic and Transcendental* Numbers. Disponible en: www.math.u-psud.fr/~fischler/inde/inde_fischlerpondichery.pdf. [Consultado el 8 de diciembre de 2012]

Gelfond, A. (1960). *Transcendental and Algebraic Numbers.* New York: Dover Publications.

Gray, J. (2003). *El reto de Hilbert: Los 23 problemas que desafiaron a la matemática.* Barcelona: Crítica.

Guedes, D. (2002). *Números Irracionales e transcendentes.* Brasil: S.B.M.

Haristoy, J. & Oudet, E. *Autour du septième problème de Hilbert: une excursión en transcendance.* Disponible en: ireme.u-strasbg.fr/php/articles/107_Haristoy_Oudet.pdf.

Herstein, I. N. (1990). *Álgebra Moderna: Grupos, Anillos, Campos, Teoría de Galois.* México: Ed. Trillas

Hoffman, K. & Kunze, R. (1973). *Álgebra Lineal.* Barcelona: Prentice-Hall

Ivorra, C. *Teoría de Números.* Disponible en: www.uv.es/ivorra/Libros/Numeros.pdf. [Colsultado el 5 de marzo de 2011]

Niven, I. (1985). *Irrational Numbers.* Estados Unidos de América: The Mathematical Association of America.

Patterson, E. & Shchogolev, V. (2001). *Summer Number Theory Seminar 2001: Algebraic and Transcendental Numbers.* Disponible en: www.math.columbia.educ/~ums/pdf/algtrans.pdf. [Consultado el 23 de noviembre de 2012]

Pickover, C.A. (2011). *El Libro de las Matemáticas: De Pitágoras a la 57° dimensión, 250 hitos de la historia de las matemáticas.* Madrid: Librero.

Pollard, H. & Diamond, H. (1998). *The Theory of Algebraic Numbers*. New York: Dover Publications.

Rosales, A. (2010). *Números Trascendentes: Desarrollo Histórico*. Revista digital Matemática, Educación e Internet. Disponible en: www.tec-digital.itcr.ac.cr/revistmatematica/ARTICULOS_V10_N2_2010/A_Rosales_Numero_Trascendentes. [Consultado el 6 de diciembre de 2012]

Siegel, C. (1949). *Transcendental Numbers*. Estados Unidos de América: Princeton University Press.

S. Daoub, H. (2012). *The Fundamental Theorem on Symmetric Polynomial*. The Teaching of Mathematics, Vol. XV. Disponible en: http://elib.mi.sanu.ac.rs/files/journals/tm/28/tm1515.pdf. [Consultado el 16 de noviembre de 2012]

Toenniessen, F. (2010). *Das Geheimnis der Transzendenten Zahlen: Eine etwas andere Einfuhrung indie Mathematik*. Heidelberg: Spektrum Akadenischer Verlag.

Tubbs, R. *Hilbert's Seventh Problem: Solutions and extensions*. Disponible en: euclid.colorado.edu/~tubbs/course/course.html [Consultado el 1 de nov. de 2012]

Yandell, B.H. (2002). *The Honors Class: Hilbert's Problems and Their Solvers*. Natick: A K Peters.